

No. 17-16107

**In the United States Court of Appeals
for the Ninth Circuit**

WILEY GILL; JAMES PRIGOFF; TARIQ RAZAK; KHALED IBRAHIM;
AARON CONKLIN,

Plaintiffs-Appellants,

v.

DEPARTMENT OF JUSTICE; JEFF SESSIONS, Attorney General; PROGRAM
MANAGER – INFORMATION SHARING ENVIRONMENT; KSHEMENDRA
PAUL, in his official capacity as Program Manager of the Information Sharing
Environment,

Defendants-Appellees.

**EXCERPTS OF RECORD
Volume 1 of 4 – Pages 1 to 10**

On Appeal from the United States District Court
for the Northern District of California
No. 3:14-cv-03120-RS
The Honorable Richard Seeborg, District Judge

Stephen Scotch-Marmo
stephen.scotch-
marmo@morganlewis.com
Michael James Ableson
michael.ableson@morganlewis.com
MORGAN, LEWIS & BOCKIUS LLP
101 Park Avenue
New York, NY 10178
T. 212.309.6000
F. 212.309.6001

Linda Lye
llye@aclunc.org
Julia Harumi Mass
jmass@aclunc.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN
CALIFORNIA, INC.
39 Drumm Street
San Francisco, CA 94111
T. 415.921.2493
F. 415.255.8437

*Attorneys for Appellants
Wiley Gill, James Prigoff, Tariq Razak, Khaled Ibrahim, and Aaron Conklin*

(Additional Counsel on Inside Cover)

Mitra Ebadolahi
mebadolahi@aclusandiego.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF SAN DIEGO AND
IMPERIAL COUNTIES
P.O. Box 87131
San Diego, CA 92138
T. 619.232.2121
F. 619.232.0036

Peter Bibring
pbibring@aclusocal.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF SOUTHERN
CALIFORNIA
1313 West 8th Street
Los Angeles, CA 90017
T. 213.977.9500
F. 213.977.5299

Hugh Handeyside
hhandeyside@aclu.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
T. 212.549.2500
F. 212.549.2654

Jeffrey S. Raskin
jeffrey.raskin@morganlewis.com
Phillip J. Wiese
phillip.wiese@morganlewis.com
MORGAN LEWIS & BOCKIUS LLP
One Market, Spear Street Tower
San Francisco, CA 94105
T. 415.442.1000
F. 415.442.1001

Christina Sinha
christinas@advancingjustice-alc.org
ASIAN AMERICANS ADVANCING
JUSTICE – ASIAN LAW CAUCUS
55 Columbus Avenue
San Francisco, CA 94111
T. 415.848.7711
F. 415.896.1703

Attorneys for Appellants

Wiley Gill, James Prigoff, Tariq Razak, Khaled Ibrahim, and Aaron Conklin

INDEX

Docket No.	Description	Date	Page No.
Volume 1 of 4 – Pages 1 to 10			
134	Order On Cross Motions For Summary Judgment	03/27/17	1
Volume 2 of 4 – Pages 11 to 252			
136	Notice Of Appeal To The United States Court Of Appeals For The Ninth Circuit	05/28/17	11
135	Judgment	03/29/17	16
127	Declaration Of Wiley Gill In Support Of Plaintiffs' Motion For Summary Judgment	11/03/16	17
	Exhibit 1: Letter, Dated January 3, 2014		25
	Exhibit 2: Letter, Dated June 23, 2014		28
	Exhibit 3: Letter, Dated February 29, 2016		48
124	Defendants' Reply In Support Of Motion For Summary Judgment, Opposition To Plaintiffs' Motion For Summary Judgment, And Opposition To Plaintiffs' Motion To Strike Defendants' Declarations And To Supplement The Record With Plaintiffs' Declarations	10/20/16	68
121	Plaintiffs' Motion To Strike Defendants' Declarations And To Supplement The Record With Plaintiffs' Declarations; Memorandum Of Points And Authorities In Support	09/22/16	73
120	Declaration Of Aaron Conklin In Support Of Plaintiffs' Motion For Summary Judgment And Plaintiffs' Opposition To Defendants' Motion For Summary Judgment	09/22/16	88

INDEX
(continued)

Docket No.	Description	Date	Page No.
119	Declaration Of Khaled Ibrahim In Support Of Plaintiffs' Motion For Summary Judgment	09/22/16	94
	Exhibit 1: Suspicious Activity Report		100
118	Declaration Of Tariq Razak In Support Of Plaintiffs' Motion For Summary Judgment	09/22/16	104
	Exhibit 1: Suspicious Activity Report		111
	Exhibit 2: Letter, Dated February 13, 2015		115
	Exhibit 3: Letter, Dated April 9, 2015		132
	Exhibit 4: Letter, Dated May 21, 2015		136
	Exhibit 5: Letter, Dated June 25, 2014		139
117	Declaration Of James Prigoff In Support Of Plaintiffs' Motion For Summary Judgment And Plaintiffs' Opposition To Defendants' Motion For Summary Judgment	09/22/16	143
	Exhibit 1: Business Card With Note, Dated August 19, 2004		153
	Exhibit 2: Suspicious Activity Report On James Burt Prigoff, Dated June 21, 2004		156
	Exhibit 3: Suspicious Activity Report On James Burt Prigoff, Dated October 18, 2004		160
	Exhibit 4: Suspicious Activity Report On James Burt Prigoff, Dated November 8, 2004		165

INDEX
(continued)

Docket No.	Description	Date	Page No.
	Exhibit 5: Letter, Dated March 24, 2015		168
	Exhibit 6: Letter, Dated May 19, 2015		172
	Exhibit 7: Letter, Dated January 27, 2016		176
	Exhibit 8: Letter, Dated January 8, 2015		179
	Exhibit 9: Letter, Dated September 15, 2015		181
	Exhibit 10: ISE-SAR Criteria Guidance		186
	Exhibit 11: Potential Indicators of Terrorist Activities Related to the General Public		201
116	Declaration Of Linda Lye In Support Of Plaintiffs' Opposition To Defendants' Motion For Summary Judgment And Cross-Motion For Summary Judgment	09/22/16	204
	Exhibit 1: Letter, Dated July 12, 2013		209
	Exhibit 2: Emails, Dated July 22, 2013, July 23, 2013 and August 2, 2013		212
	Exhibit 3: Letter, Dated March 7, 2016		217
	Exhibit 4: Letter, Dated March 21, 2016		220
	Exhibit 5: Regional Information Sharing Systems (RISS)		238
	Exhibit 6: 28 CFR Part 23 Frequently Asked Questions		241

INDEX
(continued)

Docket No.	Description	Date	Page No.
113	Defendants' Notice Of Motion For Summary Judgment And Memorandum In Support	08/18/16	243
Volume 3 of 4 – Pages 253 to 375			
107	Defendants' Notice Of Filing Of Supplemental Administrative Record	05/10/16	253
	Amended Certification Of Administrative Record And Supplemental Administrative Record		255
	Document 1: ISE Privacy Guidelines (December 4, 2006)		265
	Document 3: National Strategy for Information Sharing (October 2007)		268
	Document 5: Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project (October 1, 2008)		272
	Document 6: ISE Suspicious Activity Reporting Evaluation Environment Segment Architecture (December 2008)		290
	Document 7: ISE SAR Evaluation Environment Implementation Guide, Version 1.0 (January 9, 2009)		293
	Document 8: Final Report: Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Evaluation Environment (January 2010)		296

INDEX
(continued)

Docket No.	Description	Date	Page No.
	Document 9: Review of Advocate Websites for Concerns and Issues on ISE-Related Activities (2012)		306
94	Notice Of Motion And Memorandum Of Law In Support Of Defendants' Motion For Relief From Nondispositive Pretrial Order Of Magistrate Judge	01/15/16	310
79	Defendants' Opposition To Plaintiffs' Motion To Complete The Administrative Record	10/22/15	322
56	Defendants' Opposition To Plaintiffs' Special Motion To Establish Right To Discovery On The Department Of Justice's Standard For Suspicious Activity Reporting	07/10/15	374
Volume 4 of 4 – Pages 376 to 656			
52	Defendants' Notice Of Filing Of Administrative Record	06/16/15	376
	Certification of Administrative Record		380
53	Administrative Record	06/16/15	—
	Exhibit 1: White House Memorandum on Guidelines and Requirements in Support of the Information Sharing Environment (December 16, 2005) (wh121605- memo .pdf)		390

INDEX
(continued)

Docket No.	Description	Date	Page No.
	Exhibit 3: The Information Sharing Environment Suspicious Activity Reporting (SAR) Working Group's Business Process Analysis (February 13, 2007) (SAR_BusinessAnalysis_final20070215.doc)		395
	Exhibit 6: PM-ISE Memorandum, Release of the Information Sharing Environment (ISE) Functional Standard for Suspicious Activity Reporting (SAR) Version 1.0 (ISE-FS-200) (January 25, 2008) (Transmittal_Memorandum_ISE-FS-200.pdf)		397
	Exhibit 7: Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.0 ISE-FS-200 (January 25, 2008) (Functional Standard_Issuance_Version_1.0_Final_Signed).pdf)		401
	Exhibit 15: Information Sharing Environment – Suspicious Activity Reporting Functional Standard And Evaluation Environment Initial Privacy and Civil Liberties Analysis September 2008— Version 1 (September 2008) (ISE-SAR FS and EE Initial Privacy and Civil Liberties Analysis_090508.pdf)		433

INDEX
(continued)

Docket No.	Description	Date	Page No.
	Exhibit 20: Feedback Session with Privacy and Civil Liberties Advocates: Suspicious Activity Reporting (SAR) Line-Officer Training and the ISE-SAR Functional Standard—Agenda (February 13, 2009) (Agenda February 18, 2009 - SAR Feedback Session.doc)		447
	Exhibit 26: Memorandum for Release of the Information Sharing Environment (ISE) Functional Standard for Suspicious Activity Reporting, Version 1.5 (May 21, 2009) (ISE-SAR Functional Standard V1.5 Cover Letter.pdf)		448
	Exhibit 28: Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) version 1.5 (May 21, 2009) (ISE-FS-200_ ISESAR_ Functional_ Standard_ V1.5_ Issued.pdf)		450
	Exhibit 30: NSI Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations report issued by PMISE on privacy compliance outcomes of the ISE SAR Evaluation Environment and providing recommendations for additional privacy protections during nationwide expansion of the NSI (July 2010) (NSI_PCRCL_ Analysis_July2010_final.pdf)		486

INDEX
(continued)

Docket No.	Description	Date	Page No.
	Exhibit 40: ISE-SAR Functional Standard Version 1.5.5 Executive Summary (February 17, 2015) (FS v1_5_5 Executive Summary PM_ISE 21715 Comprehensive)		493
	Exhibit 41: Final and signed version of the ISE-SAR Functional Standard version 1.5.5 issued by the PM-ISE. (February 23, 2015) (SAR_FS_1.5.5_IssuedFeb2015.pdf)		501
46-1	Defendants' Answer To Complaint	04/24/15	561
40	Joint Case Management Statement & [Proposed] Order	03/05/15	566
38	Order Denying Motion To Dismiss	02/20/15	569
36	Joint Case Management Statement & [Proposed] Order	12/31/14	581
21	Notice Of Motion And Memorandum Of Law In Support Of Defendants' Motion To Dismiss	10/16/14	586
—	District Court Docket	—	632

United States District Court
Northern District of California

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

WILEY GILL, et al.,

Plaintiffs,

v.

DEPARTMENT OF JUSTICE, et al.,

Defendants.

Case No. [14-cv-03120-RS](#)

**ORDER ON CROSS MOTIONS FOR
SUMMARY JUDGMENT**

I. INTRODUCTION

This is a challenge brought under the Administrative Procedures Act (“APA”), to certain aspects of the National Suspicious Activity Reporting Initiative (“NSI”), a nationwide program that collects, vets, and disseminates intelligence with a possible nexus to terrorism. Plaintiffs contend defendant Program Manager-Information Sharing Environment (“PM-ISE”) has adopted a so-called “Functional Standard” that utilizes overly broad criteria to define the types of activities deemed as having a potential nexus to terrorism. As a result, plaintiffs allege, state and local law enforcement authorities submit “Suspicious Activity Reports” (“SARs”) to the federal government even if unsupported by reasonable suspicion of criminal activity, and innocent Americans are “wrongly branded as potential terrorists.”

Plaintiffs contend the Functional Standard conflicts with a duly-promulgated DOJ regulation, 28 C.F.R. Part 23 (hereafter “Part 23”), which they assert was adopted to protect

United States District Court
Northern District of California

1 constitutional and privacy rights by prohibiting the collection of “criminal intelligence” unless
2 supported by “reasonable suspicion.” The Functional Standard, in contrast, calls for sharing of
3 SARs whenever they reflect “observed behavior” that is “reasonably indicative of pre-operational
4 planning associated with terrorism or other criminal activity.” The crux of the controversy,
5 therefore, lies in the distinction between the “reasonably indicative” standard, and the “reasonable
6 suspicion” standard. Both sides agree that “reasonably indicative” is a lesser standard which calls
7 for dissemination of SARs even in the absence of “reasonable suspicion.” The question is whether
8 defendants failed to comply with the APA in adopting the “reasonably indicative” standard.

9 Plaintiffs contend defendants violated the APA in two ways. First, plaintiffs insist the
10 Functional Standard was adopted without complying with the APA’s requirement that the public
11 be provided a notice and comment period prior to adoption of “legislative rules.” While
12 defendants acknowledge no such notice and comment procedure was utilized, they argue that the
13 Functional Standard is not a “legislative rule” subject to the requirement, or that even if it were,
14 the violation was harmless because the Functional Standard was adopted through a collaborative
15 process that included public input. Second, plaintiffs contend adoption of the Functional Standard
16 was “arbitrary and capricious” because of the alleged conflict with Part 23. Defendants argue
17 there is no conflict that renders adoption of the Functional Standard improper.

18 The parties have brought cross-motions for summary judgment. Because defendants have
19 shown that adoption of the Functional Standard did not violate the APA, their motion will be
20 granted and plaintiffs’ motion will be denied.

21
22 **II. BACKGROUND**

23 As plaintiffs describe it, the NSI was created to facilitate the nationwide sharing of
24 information potentially related to terrorism. It is premised on the notion that while state, local, and
25 tribal law enforcement agents – so called “front line” personnel – are well situated to gather that
26 type of information, their reports should be vetted under uniform standards. DOJ and PM-ISE
27 have issued protocols relating to SAR reporting designed to provide such standards for evaluating

United States District Court
Northern District of California

1 information collected by front line personnel before it is disseminated nationally. At the time of a
2 prior motion to dismiss in this action, the parties were disputing whether DOJ’s protocols and the
3 PM-ISE protocols were separate or not. Now, the parties appear to be in agreement that only the
4 one “Functional Standard” is at issue—and that it was first adopted in 2009, and revised in 2015.

5 The SAR process proceeds in three stages: collection of information by front line
6 personnel, vetting by trained analysts at “fusion centers,” and dissemination to law enforcement
7 nationwide. Front line personnel are allegedly trained in the Functional Standard, collect
8 information about people engaged in activities that purportedly have a potential nexus to terrorism,
9 and submit such information in the form of SARs, either directly to the Federal Bureau of
10 Investigation or to a fusion center.

11 Fusion centers, which are federally funded, gather, receive, store, analyze, and share
12 intelligence, including SARs, related to terrorism and other threats. Although the local collecting
13 agencies perform some vetting, the primary responsibility for doing so rests with fusion centers,
14 whose staff are trained in the Functional Standard and review SARs for compliance with that
15 standard. SARs meeting the standard are then disseminated both regionally through the fusion
16 center’s database, and nationally through a data base known as “eGuardian.”¹ The FBI oversees
17 eGuardian, which allows law enforcement personnel across the country to access SARs that have
18 been uploaded to it. Plaintiffs allege that the federal government maintains SARs sent to
19 eGuardian for 30 years, even when the FBI has determined that a particular SAR has no nexus to
20 terrorism.²

21
22
23
24 _____
¹ There is some indication certain other databases may have been used in the past.

25
26 ² From materials attached as exhibits to the complaint, however, it appears that where no nexus to
27 potential terrorism can be validated, the SAR will not be made accessible through the ISE. Also,
the protocols appear to include some measures to address removing unfounded information. See
Complaint Exh. D, pp. 61-63; Exh. E, p. 93.

United States District Court
Northern District of California

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

III. LEGAL STANDARD

Although the parties characterize their briefing as constituting cross-motions for “summary judgment,” they recognize this is not an inquiry under Rule 56 of the Federal Rules of Civil Procedure as to whether there are disputed factual issues for trial. Rather, this is the review on the merits under the APA of the validity of the adoption of the Functional Standard. *See, Klamath Siskiyou Wildlands Ctr.*, 962 F. Supp. 2d at 1233; *see also Sierra Club v. Mainella*, 459 F. Supp. 2d 76, 89 (D.D.C. 2006) (“[T]he standard set forth in Rule 56(c) does not apply [in an APA case] because of the limited role of a court in reviewing the administrative record.”); *McCrary v. Gutierrez*, 495 F. Supp. 2d 1038, 1041 (N.D. Cal. 2007) (judicial review of agency action under the APA limited to the administrative record).

“Under the APA, it is the role of the agency to resolve factual issues to arrive at a decision that is supported by the administrative record, whereas ‘the function of the district court is to determine whether or not as a matter of law the evidence in the administrative record permitted the agency to make the decision it did.’” *Sierra Club*, 459 F.Supp. 2d at 90 (quoting *Occidental Eng’g Co. v. INS*, 753 F.2d 766, 769–70 (9th Cir. 1985)). In other words, “the district court acts like an appellate court, and the ‘entire case’ is ‘a question of law.’” *Nat’l Law Ctr. on Homelessness & Poverty v. U.S. Dep’t of Veterans Affairs*, 842 F. Supp. 2d 127, 130 (D.D.C. 2012) (quoting *Amer. Bioscience, Inc. v. Thompson*, 269 F.3d 1077, 1083 (D.C. Cir. 2001)). “Summary judgment thus serves as the mechanism for deciding, as a matter of law, whether the agency action is supported by the administrative record and otherwise consistent with the APA standard of review.” *Stuttering Found. of Am. v. Springer*, 498 F. Supp. 2d 203, 207 (D.D.C. 2007).

IV. DISCUSSION

A. Notice and Comment

An agency may lawfully issue a so-called “legislative rule” only by using the notice and comment procedure described in the APA, unless it publishes a specific finding of good cause documenting why such procedures “are impracticable, unnecessary, or contrary to the public

United States District Court
Northern District of California

1 interest.” 5 U.S.C. § 553(b), (b)(B). In contrast, an agency need not follow the notice and
2 comment procedure to issue an “interpretive rule.” § 553(b)(A). See *Hemp Indus. Ass’n v. Drug*
3 *Enforcement Admin.*, 333 F.3d 1082, 1087 (9th Cir. 2003). Here, there is no dispute that the
4 Functional Standard was adopted without notice and comment, or a specific finding of good cause
5 that none was appropriate.

Courts have struggled with identifying the difference between
legislative rules and interpretive rules. In general terms, interpretive
rules merely explain, but do not add to, the substantive law that
already exists in the form of a statute or legislative rule. *Yesler*
Terrace Community Council v. Cisneros, 37 F.3d 442, 449 (9th
Cir.1994). Legislative rules, on the other hand, create rights, impose
obligations, or effect a change in existing law pursuant to authority
delegated by Congress. *Id.*

11
12 *Hemp Indus.*, 333 F.3d at 1087.

13 Plaintiffs argue the Functional Standard is “legislative” because, they contend, no statute
14 sets forth a self-executing substantive standard governing the type of information that can be
15 collected, maintained, or disseminated. Plaintiffs explain the statutes operate instead to delegate
16 the authority for the promulgation of such standards to defendants, and that they have done so in
17 the Functional Standard. Defendants, in turn, point to the voluntary nature of the system as a
18 whole to argue the standard is not legislative in nature.

19 The Functional Standard does not fit neatly into *either* side of the dichotomy described in
20 *Hemp Industries*, above. It is not inarguably merely an “explanation” of other substantive law that
21 already existed “in the form of a statute or legislative rule.” Nor, however, is it plainly a rule that
22 “create[s] rights, impose[s] obligations, or effect[s] a change in existing law pursuant to authority
23 delegated by Congress.”

24 Rather, as defendants argue, it primarily describes an operating procedure—a policy, a
25 plan, a strategy—allowing cooperation and communication among various governmental actors.
26 At the motion to dismiss stage, defendants argued this “guidance” aspect of the standard meant it
27 was not a “final agency action” subject to judicial review. See *Bennett v. Spear*, 520 U.S. 154

United States District Court
Northern District of California

1 (1997) (“First, the action must mark the ‘consummation’ of the agency’s decisionmaking
 2 process—it must not be of a merely tentative or interlocutory nature. And second, the action must
 3 be one by which ‘rights or obligations have been determined,’ or from which ‘legal consequences
 4 will flow.’”) While there was and is no dispute that the Functional Standard was neither tentative
 5 nor interlocutory, it far less clearly constitutes a rule determining legal rights and obligations.
 6 Even though the order on the motion to dismiss called that question in plaintiff’s favor at the
 7 pleading stage, there is good reason to treat the Functional Standard as not constituting a final
 8 agency action within the meaning of *Bennet v. Spear*.

9 Even assuming, however, there was “final agency action,” it was fundamentally a policy
 10 guidance statement not subject to a notice-and-comment requirement.

11
 12 When a federal agency issues a directive concerning the future
 13 exercise of its discretionary power, for purposes of APA section
 14 553, its directive will constitute either a substantive rule, for which
 notice-and-comment procedures are required, or a general statement
 of policy, for which they are not

15 To the extent that the directive merely provides guidance to agency
 16 officials in exercising their discretionary powers while preserving
 17 their flexibility and their opportunity to make “individualized
 determination [s],” it constitutes a general statement of policy. . . .

18 *Mada-Luna v. Fitzpatrick*, 813 F.2d 1006, 1013–14 (9th Cir. 1987).

19
 20 Accordingly, defendants are entitled to summary judgment that adoption of the Functional
 21 Standard without a notice-and-comment period did not violate the APA.³

22
 23
 24
 25 ³ As noted above, defendants also argue any failure to follow the notice and comment procedures
 26 of the APA was harmless in light of how the Functional Standard was adopted. Defendants insist
 27 it was a collaborative process that included public input. It is subject to question, however,
 whether an agency could avoid any statutory notice and comment process by undertaking a more
 informal procedure.

United States District Court
Northern District of California

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

B. Arbitrary and capricious

Plaintiffs also seek to set aside the Functional Standard as arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law.

The scope of review under the “arbitrary and capricious” standard is narrow and a court is not to substitute its judgment for that of the agency. Nevertheless, the agency must examine the relevant data and articulate a satisfactory explanation for its action including a rational connection between the facts found and the choice made In reviewing that explanation, [the court] must consider whether the decision was based on a consideration of the relevant factors and whether there has been a clear error of judgment

Motor Vehicle Mfrs. Ass’n v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 43 (1983) (citations omitted).

As the *Motor Vehicles* court further explained:

Normally, an agency rule would be arbitrary and capricious if the agency has relied on factors which Congress has not intended it to consider, entirely failed to consider an important aspect of the problem, offered an explanation for its decision that runs counter to the evidence before the agency, or is so implausible that it could not be ascribed to a difference in view or the product of agency expertise.

Id.

Here, plaintiffs’ theory is that because the Functional Standard does not require SARs to be based on a “reasonable suspicion,” it conflicts with Part 23’s requirement that criminal intelligence not be collected or maintained unless supported by “reasonable suspicion.” The rules in Section 23 proceed from an “[o]perating principle[]” that a “project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.” 28 C.F.R. § 23.20(a). There is no dispute that the Functional Standard allows for collection and dissemination of SARs not meeting that test.

Defendants insist there is no conflict between the Functional Standard and Part 23 because,

United States District Court
Northern District of California

1 they contend, the NSI is not a system for collecting “criminal intelligence.” They argue that the
 2 Functional Standard and 28 C.F.R. Part 23 were issued pursuant to distinct statutory authorities for
 3 application to different information gathering programs. Compare 42 U.S.C. § 3789g(c)
 4 (authorizing OJP to issue policy standards for criminal intelligence systems funded under the
 5 Omnibus Crime Control and Safe Streets Act of 1968 Pub. L. 90-351, 82 Stat. 197, codified at 42
 6 U.S.C. §3711 *et seq.* (“Omnibus Act”) with 6 U.S.C. § 485(f)(2)(A)(iii) (authorizing the Program
 7 Manager to issue functional standards for the ISE). Defendants note that the operating principles
 8 of Part 23 are expressly linked to federal funding of criminal intelligence systems under the
 9 Omnibus Act. *See* 42 U.S.C. § 3789g(c); 28 C.F.R. § 23.1; 28 C.F.R. § 23.3; 28 C.F.R. § 23.30; 28
 10 C.F.R. § 23.40.

11 Plaintiffs correctly observe that the arguments defendants now make about the claimed
 12 lack of Omnibus Act funding were not the basis on which the agency decided to adopt the
 13 “reasonably indicative” standard in lieu of a “reasonable suspicion” standard. Plaintiffs also
 14 rightly note that, generally, “an agency’s action must be upheld, if at all, on the basis articulated
 15 by the agency itself,” *Motor Vehicle*, 463 U.S. at 50.

16 Nevertheless, plaintiffs have not shown that it was arbitrary and capricious for the
 17 Functional Standard to depart from the “reasonable suspicion” standard of Part 23. The
 18 administrative record includes the following description of why the “reasonably indicative”
 19 standard was adopted:

20 The use of the “reasonably indicative” determination process allows
 21 supervisors at source agencies and trained analysts and investigators
 22 at fusion centers and other agencies to have a uniform process that
 23 will result in better quality SARs and the posting of more reliable
 24 ISE-SARs to the ISE Shared Spaces, while at the same time
 25 enhancing privacy, civil rights, and civil liberties protections.
 26 Furthermore, this revision improves mission effectiveness and
 27 enables NSI participating agency personnel to identify and address,
 28 in a more efficient manner, potential criminal and terrorism threats
 by using more narrowly targeted language. Finally, better quality
 SARS should result in a sufficiently high quality of information
 enabling agencies and analysts to “connect the dots” while not
 producing so much information as to overwhelm agency analytical
 capacity. In addition, the “reasonably indicative” determination is an
 essential privacy, civil rights, and civil liberties protection because it

United States District Court
Northern District of California

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

emphasizes a behavior-focused approach to identifying suspicious activity and mitigates the risk of profiling based upon race, ethnicity, national origin, or religious affiliation or activity.

Plaintiffs insist the record also shows defendants were “aware of the need” to address Part 23, because it was raised during discussion of the Functional Standard. Plaintiffs’ argument, however, presupposes that SARs are “criminal intelligence” governed under Part 23. Defendants have shown that to the contrary, the Functional Standard was developed to address data collection and dissemination issues not already within the scope of Part 23. While they certainly could have adopted the same standard, the record reveals no “clear error of judgment” or “failure to consider an important aspect of the problem” or such a counter-factual or implausible explanation as to permit the court to substitute its judgment of what a better rule might be.⁴ Accordingly, defendants are entitled to summary judgment that adoption of the Functional Standard did not violate the APA as arbitrary and capricious.

C. Motion to strike

In connection with their argument that Part 23 applies only to systems funded under the Omnibus Act, defendants have offered a declaration of Marilyn B. Atsatt to show that the FBI eGuardian and the “NSI SAR Data Repository” are not funded under the Omnibus Act. Defendants also proffer a declaration from Basil N. Harris describing the adoption and amendment of the Functional Standard, including the public input that allegedly was solicited and considered.

Defendants have consistently sought to enforce the principle that, with narrow exceptions, APA actions are decided on the administrative record and nothing more. In extended proceedings before the assigned magistrate judge, and in objections to her rulings, defendants resisted attempts to expand that record. Defendants also successfully resisted plaintiffs’ requests to be allowed discovery. In light of that discovery history, plaintiffs’ motion to strike these declarations is

⁴ Plaintiffs have offered policy arguments as to why, in their view, the “reasonably indicative” standard draws a poor balance between individual rights and public safety. In an action under the APA, however, something more must be shown.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

granted.⁵

V. CONCLUSION

Defendants’ motion is granted, and plaintiffs’ motion is denied. A separate judgment will issue.

IT IS SO ORDERED.

Dated: March 27, 2017



RICHARD SEEBORG
United States District Judge

United States District Court
Northern District of California

⁵ Plaintiffs’ motion to supplement the record under the exception for extra-record evidence related to standing is denied as moot. Defendants’ challenge to plaintiffs’ standing was rejected at the motion to dismiss stage, and was not renewed on summary judgment.

No. 17-16107

**In the United States Court of Appeals
for the Ninth Circuit**

WILEY GILL; JAMES PRIGOFF; TARIQ RAZAK; KHALED IBRAHIM;
AARON CONKLIN,

Plaintiffs-Appellants,

v.

DEPARTMENT OF JUSTICE; JEFF SESSIONS, Attorney General; PROGRAM
MANAGER – INFORMATION SHARING ENVIRONMENT; KSHEMENDRA
PAUL, in his official capacity as Program Manager of the Information Sharing
Environment,

Defendants-Appellees.

**EXCERPTS OF RECORD
Volume 2 of 4 – Pages 11 to 252**

On Appeal from the United States District Court
for the Northern District of California
No. 3:14-cv-03120-RS
The Honorable Richard Seeborg, District Judge

Stephen Scotch-Marmo
stephen.scotch-
marmo@morganlewis.com
Michael James Ableson
michael.ableson@morganlewis.com
MORGAN, LEWIS & BOCKIUS LLP
101 Park Avenue
New York, NY 10178
T. 212.309.6000
F. 212.309.6001

Linda Lye
llye@aclunc.org
Julia Harumi Mass
jmass@aclunc.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN
CALIFORNIA, INC.
39 Drumm Street
San Francisco, CA 94111
T. 415.921.2493
F. 415.255.8437

*Attorneys for Appellants
Wiley Gill, James Prigoff, Tariq Razak, Khaled Ibrahim, and Aaron Conklin*

(Additional Counsel on Inside Cover)

Mitra Ebadolahi
mebadolahi@aclusandiego.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF SAN DIEGO AND
IMPERIAL COUNTIES
P.O. Box 87131
San Diego, CA 92138
T. 619.232.2121
F. 619.232.0036

Peter Bibring
pbibring@aclusocal.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF SOUTHERN
CALIFORNIA
1313 West 8th Street
Los Angeles, CA 90017
T. 213.977.9500
F. 213.977.5299

Hugh Handeyside
hhandeyside@aclu.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
T. 212.549.2500
F. 212.549.2654

Jeffrey S. Raskin
jeffrey.raskin@morganlewis.com
Phillip J. Wiese
phillip.wiese@morganlewis.com
MORGAN LEWIS & BOCKIUS LLP
One Market, Spear Street Tower
San Francisco, CA 94105
T. 415.442.1000
F. 415.442.1001

Christina Sinha
christinas@advancingjustice-alc.org
ASIAN AMERICANS ADVANCING
JUSTICE – ASIAN LAW CAUCUS
55 Columbus Avenue
San Francisco, CA 94111
T. 415.848.7711
F. 415.896.1703

Attorneys for Appellants
Wiley Gill, James Prigoff, Tariq Razak, Khaled Ibrahim, and Aaron Conklin

INDEX

Docket No.	Description	Date	Page No.
Volume 1 of 4 – Pages 1 to 10			
134	Order On Cross Motions For Summary Judgment	03/27/17	1
Volume 2 of 4 – Pages 11 to 252			
136	Notice Of Appeal To The United States Court Of Appeals For The Ninth Circuit	05/28/17	11
135	Judgment	03/29/17	16
127	Declaration Of Wiley Gill In Support Of Plaintiffs' Motion For Summary Judgment	11/03/16	17
	Exhibit 1: Letter, Dated January 3, 2014		25
	Exhibit 2: Letter, Dated June 23, 2014		28
	Exhibit 3: Letter, Dated February 29, 2016		48
124	Defendants' Reply In Support Of Motion For Summary Judgment, Opposition To Plaintiffs' Motion For Summary Judgment, And Opposition To Plaintiffs' Motion To Strike Defendants' Declarations And To Supplement The Record With Plaintiffs' Declarations	10/20/16	68
121	Plaintiffs' Motion To Strike Defendants' Declarations And To Supplement The Record With Plaintiffs' Declarations; Memorandum Of Points And Authorities In Support	09/22/16	73
120	Declaration Of Aaron Conklin In Support Of Plaintiffs' Motion For Summary Judgment And Plaintiffs' Opposition To Defendants' Motion For Summary Judgment	09/22/16	88

INDEX
(continued)

Docket No.	Description	Date	Page No.
119	Declaration Of Khaled Ibrahim In Support Of Plaintiffs' Motion For Summary Judgment	09/22/16	94
	Exhibit 1: Suspicious Activity Report		100
118	Declaration Of Tariq Razak In Support Of Plaintiffs' Motion For Summary Judgment	09/22/16	104
	Exhibit 1: Suspicious Activity Report		111
	Exhibit 2: Letter, Dated February 13, 2015		115
	Exhibit 3: Letter, Dated April 9, 2015		132
	Exhibit 4: Letter, Dated May 21, 2015		136
	Exhibit 5: Letter, Dated June 25, 2014		139
117	Declaration Of James Prigoff In Support Of Plaintiffs' Motion For Summary Judgment And Plaintiffs' Opposition To Defendants' Motion For Summary Judgment	09/22/16	143
	Exhibit 1: Business Card With Note, Dated August 19, 2004		153
	Exhibit 2: Suspicious Activity Report On James Burt Prigoff, Dated June 21, 2004		156
	Exhibit 3: Suspicious Activity Report On James Burt Prigoff, Dated October 18, 2004		160
	Exhibit 4: Suspicious Activity Report On James Burt Prigoff, Dated November 8, 2004		165

INDEX
(continued)

Docket No.	Description	Date	Page No.
	Exhibit 5: Letter, Dated March 24, 2015		168
	Exhibit 6: Letter, Dated May 19, 2015		172
	Exhibit 7: Letter, Dated January 27, 2016		176
	Exhibit 8: Letter, Dated January 8, 2015		179
	Exhibit 9: Letter, Dated September 15, 2015		181
	Exhibit 10: ISE-SAR Criteria Guidance		186
	Exhibit 11: Potential Indicators of Terrorist Activities Related to the General Public		201
116	Declaration Of Linda Lye In Support Of Plaintiffs' Opposition To Defendants' Motion For Summary Judgment And Cross-Motion For Summary Judgment	09/22/16	204
	Exhibit 1: Letter, Dated July 12, 2013		209
	Exhibit 2: Emails, Dated July 22, 2013, July 23, 2013 and August 2, 2013		212
	Exhibit 3: Letter, Dated March 7, 2016		217
	Exhibit 4: Letter, Dated March 21, 2016		220
	Exhibit 5: Regional Information Sharing Systems (RISS)		238
	Exhibit 6: 28 CFR Part 23 Frequently Asked Questions		241

INDEX
(continued)

Docket No.	Description	Date	Page No.
113	Defendants' Notice Of Motion For Summary Judgment And Memorandum In Support	08/18/16	243
Volume 3 of 4 – Pages 253 to 375			
107	Defendants' Notice Of Filing Of Supplemental Administrative Record	05/10/16	253
	Amended Certification Of Administrative Record And Supplemental Administrative Record		255
	Document 1: ISE Privacy Guidelines (December 4, 2006)		265
	Document 3: National Strategy for Information Sharing (October 2007)		268
	Document 5: Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project (October 1, 2008)		272
	Document 6: ISE Suspicious Activity Reporting Evaluation Environment Segment Architecture (December 2008)		290
	Document 7: ISE SAR Evaluation Environment Implementation Guide, Version 1.0 (January 9, 2009)		293
	Document 8: Final Report: Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Evaluation Environment (January 2010)		296

INDEX
(continued)

Docket No.	Description	Date	Page No.
	Document 9: Review of Advocate Websites for Concerns and Issues on ISE-Related Activities (2012)		306
94	Notice Of Motion And Memorandum Of Law In Support Of Defendants' Motion For Relief From Nondispositive Pretrial Order Of Magistrate Judge	01/15/16	310
79	Defendants' Opposition To Plaintiffs' Motion To Complete The Administrative Record	10/22/15	322
56	Defendants' Opposition To Plaintiffs' Special Motion To Establish Right To Discovery On The Department Of Justice's Standard For Suspicious Activity Reporting	07/10/15	374
Volume 4 of 4 – Pages 376 to 656			
52	Defendants' Notice Of Filing Of Administrative Record	06/16/15	376
	Certification of Administrative Record		380
53	Administrative Record	06/16/15	—
	Exhibit 1: White House Memorandum on Guidelines and Requirements in Support of the Information Sharing Environment (December 16, 2005) (wh121605- memo .pdf)		390

INDEX
(continued)

Docket No.	Description	Date	Page No.
	Exhibit 3: The Information Sharing Environment Suspicious Activity Reporting (SAR) Working Group's Business Process Analysis (February 13, 2007) (SAR_BusinessAnalysis_final20070215.doc)		395
	Exhibit 6: PM-ISE Memorandum, Release of the Information Sharing Environment (ISE) Functional Standard for Suspicious Activity Reporting (SAR) Version 1.0 (ISE-FS-200) (January 25, 2008) (Transmittal_Memorandum_ISE-FS-200.pdf)		397
	Exhibit 7: Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.0 ISE-FS-200 (January 25, 2008) (Functional Standard_Issuance_Version_1.0_Final_Signed).pdf)		401
	Exhibit 15: Information Sharing Environment – Suspicious Activity Reporting Functional Standard And Evaluation Environment Initial Privacy and Civil Liberties Analysis September 2008— Version 1 (September 2008) (ISE-SAR FS and EE Initial Privacy and Civil Liberties Analysis_090508.pdf)		433

INDEX
(continued)

Docket No.	Description	Date	Page No.
	Exhibit 20: Feedback Session with Privacy and Civil Liberties Advocates: Suspicious Activity Reporting (SAR) Line-Officer Training and the ISE-SAR Functional Standard—Agenda (February 13, 2009) (Agenda February 18, 2009 - SAR Feedback Session.doc)		447
	Exhibit 26: Memorandum for Release of the Information Sharing Environment (ISE) Functional Standard for Suspicious Activity Reporting, Version 1.5 (May 21, 2009) (ISE-SAR Functional Standard V1.5 Cover Letter.pdf)		448
	Exhibit 28: Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) version 1.5 (May 21, 2009) (ISE-FS-200_ ISESAR_ Functional_ Standard_ V1.5_ Issued.pdf)		450
	Exhibit 30: NSI Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations report issued by PMISE on privacy compliance outcomes of the ISE SAR Evaluation Environment and providing recommendations for additional privacy protections during nationwide expansion of the NSI (July 2010) (NSI_PCRCL_ Analysis_July2010_final.pdf)		486

INDEX
(continued)

Docket No.	Description	Date	Page No.
	Exhibit 40: ISE-SAR Functional Standard Version 1.5.5 Executive Summary (February 17, 2015) (FS v1_5_5 Executive Summary PM_ISE 21715 Comprehensive)		493
	Exhibit 41: Final and signed version of the ISE-SAR Functional Standard version 1.5.5 issued by the PM-ISE. (February 23, 2015) (SAR_FS_1.5.5_IssuedFeb2015.pdf)		501
46-1	Defendants' Answer To Complaint	04/24/15	561
40	Joint Case Management Statement & [Proposed] Order	03/05/15	566
38	Order Denying Motion To Dismiss	02/20/15	569
36	Joint Case Management Statement & [Proposed] Order	12/31/14	581
21	Notice Of Motion And Memorandum Of Law In Support Of Defendants' Motion To Dismiss	10/16/14	586
—	District Court Docket	—	632

1 MORGAN, LEWIS & BOCKIUS LLP
 2 Stephen Scotch-Marmo (admitted *pro hac vice*)
 3 Stephen.scotch-marmo@morganlewis.com
 4 Michael James Ableson (admitted *pro hac vice*)
 5 michael.ableson@morganlewis.com
 6 101 Park Avenue
 7 New York, NY 10178
 8 Telephone: (212) 309-6000; Facsimile: (212) 309-6001

9 AMERICAN CIVIL LIBERTIES UNION
 10 FOUNDATION OF NORTHERN CALIFORNIA
 11 Linda Lye (SBN 215584), llye@aclunc.org
 12 Julia Harumi Mass (SBN: 18649), jmass@aclunc.org
 13 39 Drumm Street
 14 San Francisco, CA 94111
 15 Telephone: (415) 621-2493; Facsimile: (415) 255-8437

16 ASIAN AMERICANS ADVANCING
 17 JUSTICE – ASIAN LAW CAUCUS
 18 Christina Sinha (SBN 278893), christinas@advancingjustice-alc.org
 19 55 Columbus Avenue
 20 San Francisco, CA 94111
 21 Telephone: (415) 848-7711; Facsimile: (415) 896-1703

22 *Attorneys for Plaintiffs*
 23 Additional counsel listed on signature page

24 UNITED STATES DISTRICT COURT
 25 NORTHERN DISTRICT OF CALIFORNIA
 26 SAN FRANCISCO DIVISION

27 WILEY GILL; JAMES PRIGOFF; TARIQ
 28 RZAK; KHALID IBRAHIM; AND AARON
 CONKLIN,

Plaintiffs,

v.

DEPARTMENT OF JUSTICE, et al.,

Defendants.

Case No. 3:14-CV-03120-RS-KAW

**NOTICE OF APPEAL TO THE
 UNITED STATES COURT OF
 APPEALS FOR THE NINTH CIRCUIT**

Honorable Richard Seeborg

1 Notice is hereby given that all plaintiffs in the above-captioned action hereby appeal to the
 2 United States Court of Appeals for the Ninth Circuit from the district court's March 29, 2017
 3 Judgment entered in favor of defendants and against plaintiffs.

4
5 Dated: May 28, 2017

By: _____ /s/ Linda Lye

6 MORGAN, LEWIS & BOCKIUS LLP
 7 Jeffrey S. Raskin (SBN 169096)
 jeffrey.raskin@morganlewis.com
 8 Phillip J. Wiese (SBN 291842)
 phillip.wiese@morganlewis.com
 9 One Market, Spear Street Tower
 San Francisco, CA
 Telephone: (415) 442-1000
 Facsimile: (415) 442-1001

11 MORGAN, LEWIS & BOCKIUS LLP
 12 Stephen Scotch-Marmo (admitted *pro hac*
vice)
 13 Stephen.scotch-marmo@morganlewis.com
 Michael James Ableson (admitted *pro hac*
vice)
 14 michael.ableson@morganlewis.com
 15 101 Park Avenue
 New York, NY 10178
 Telephone: (212) 309-6000; Facsimile:
 16 (212) 309-6001

17 AMERICAN CIVIL LIBERTIES UNION
 18 FOUNDATION
 Hina Shamsi (admitted *pro hac vice*)
 19 hshamsi@aclu.org
 Hugh Handeyside (admitted *pro hac vice*)
 20 hhandeyside@aclu.org
 125 Broad Street
 21 New York, NY 10004
 Telephone: (212) 549-2500
 22 Facsimile: (212) 549-2654

23 AMERICAN CIVIL LIBERTIES UNION
 24 FOUNDATION OF SAN DIEGO AND
 IMPERIAL COUNTIES
 David Loy (SBN 229235)
 25 dloy@aclusandiego.org
 Mitra Ebadolahi (SBN 275157)
 26 mebadolahi@aclusandiego.org
 P.O. Box 87131
 27 San Diego, CA 92138
 Telephone: (619) 232-2121
 28 Facsimile: (619) 232-0036

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF SOUTHERN
CALIFORNIA

Peter Bibring (SBN 223981)

pbibring@aclusocal.org

1313 West 8th Street

Los Angeles, CA 90017

Telephone: (213) 977-9500

Facsimile: (213) 977-5299

Attorneys for Plaintiffs

Additional counsel listed on caption page

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

**REPRESENTATION STATEMENT
Fed R. App. P. 12(b); 9th Cir. R. 3-2(b)**

All of the plaintiffs in the above-captioned action are appellants in this appeal. The following list shows the parties to the action and identifies their counsel by name, address, and telephone number.

COUNSEL FOR ALL PLAINTIFFS

Stephen Scotch-Marmo
Michael James Ableson
101 Park Avenue
New York, NY 10178
Telephone: (212) 309-6000

Jeffrey S. Raskin
Phillip J. Wiese
MORGAN LEWIS & BOCKIUS LLP
One Market, Spear Street Tower
San Francisco, CA 94105
Telephone: (415) 442-1000

Linda Lye
Julia Harum Mass
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 621-2493

Hina Shamsi
Hugh Handeyside
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
New York, NY 10004
Telephone: (212) 249-2500

Christina Sinha
ASIAN AMERICANS ADVANCING JUSTICE – ASIAN LAW CAUCUS
55 Columbus Avenue
San Francisco, CA 94111
Telephone: (415) 848-7711

David Loy
Mitra Ebadolahi
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF SAN DIEGO AND IMPERIAL
COUNTIES
PO Box 87131
San Diego, CA 92138
Telephone: (619) 232-2121

1 **COUNSEL FOR ALL DEFENDANTS**

2 Steven Andrew Myers
3 U.S. Department of Justice
4 Civil Division, Federal Programs Branch
5 20 Massachusetts Avenue N.W.
6 Washington, D.C. 20001
7 Telephone: (203) 353-0543
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

United States District Court
Northern District of California

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

WILEY GILL, et al.,
Plaintiffs,

v.

DEPARTMENT OF JUSTICE, et al.,
Defendants.

Case No. [14-cv-03120-RS](#)

JUDGMENT

Pursuant to the order on the parties' cross-motions for summary judgment entered March 27, 2017, judgment is hereby entered in favor of defendants and against plaintiffs.

IT IS SO ORDERED.

Dated: March 29, 2017



RICHARD SEEBORG
United States District Judge

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

MORGAN, LEWIS & BOCKIUS LLP
Stephen Scotch-Marmo (admitted *pro hac vice*)
stephen.scotch-marmo@morganlewis.com
Michael James Ableson (admitted *pro hac vice*)
michael.ableson@morganlewis.com
101 Park Avenue
New York, NY 10178
Telephone: (212) 309-6000; Facsimile: (212) 309-6001

AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN CALIFORNIA
Linda Lye (SBN 215584), llye@aclunc.org
Julia Harumi Mass (SBN 189649), jmass@aclunc.org
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 621-2493; Facsimile: (415) 255-8437

ASIAN AMERICANS ADVANCING
JUSTICE - ASIAN LAW CAUCUS
Christina Sinha (SBN 278893), christinas@advancingjustice-alc.org
55 Columbus Avenue
San Francisco, CA 94111
Telephone: (415) 848-7711; Facsimile: (415) 896-1702

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

WILEY GILL; JAMES PRIGOFF; TARIQ
RAZAK; KHALID IBRAHIM; and AARON
CONKLIN,

Plaintiffs,

v.

DEPARTMENT OF JUSTICE; LORETTA
LYNCH, in her official capacity as the
Attorney General of the United States;
PROGRAM MANAGER – INFORMATION
SHARING ENVIRONMENT;
KSHEMENDRA PAUL, in his official
capacity as the Program Manager of the
Information Sharing Environment,

Defendants.

Case No. 3:14-cv-03120-RS-KAW

**DECLARATION OF WILEY GILL IN
SUPPORT OF PLAINTIFFS' MOTION
FOR SUMMARY JUDGMENT**

Hearing Date: December 8, 2016
Time: 1:30 pm
Judge: Hon. Richard Seeborg
Courtroom: 3, 17th Floor
Date of Filing: July 10, 2014
Trial Date: None Set

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

I, Wiley Wayne Gill, declare as follows:

1. I am one of the Plaintiffs in the above-titled action. I submit this declaration in support of Plaintiffs’ Motion for Summary Judgment and Plaintiffs’ Opposition to Defendants’ Motion for Summary Judgment. I have personal knowledge of each fact stated in this declaration and, if called as a witness, I could and would competently and truthfully testify hereto.

2. I am a U.S. citizen and was born in San Francisco, California. I reside in Chico, California.

3. I attended Butte Community College. I transferred from Butte Community College to California State University, Chico (“Chico State”), where I completed my undergraduate degree in 2010. I learned about Islam during a course I took at Chico State, and in 2009, I decided to convert to Islam. I have researched Islam extensively and believe it is the right path and the right religion for me.

4. After college, I was out of work for a while, but in 2012, I took a job at Chico State as a janitor, working the night shift from 6:00 P.M. to 2:30 A.M. I continue to work as a janitor at Chico State and I am now also in the process of getting a certification to be a counselor.

5. On December 3, 2013, my attorneys submitted on my behalf a request under the California Public Records Act to the Central California Intelligence Center (“CCIC”) for records about me. By letter dated January 3, 2014, the CCIC responded to the request and produced a “Suspicious Activity Report” (“SAR”) about me. A true and correct copy of the CCIC’s response and the SAR about me that it enclosed with its response is attached as Exhibit 1 to this declaration.

6. I have had a number of encounters with the Chico Police Department (“CPD”). It is my understanding that several of those encounters have been documented in the SAR about me.

7. My first encounter with CPD occurred sometime around September, 2010, after I had newly converted to Islam. Two CPD officers visited me at my apartment at around 10:30 A.M. I had just woken up and did not even have my contact lenses in, and thus I was somewhat disoriented when I went to the door. One of the CPD officers identified himself as Officer Jim

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Parrot; I do not remember the other officer’s name. Officer Parrot said that they wanted to speak with me about certain “anti-American statements” I had supposedly made. I informed him that I had no idea what he was talking about and asked him to explain what he meant. Officer Parrot referred to having a “file” on me, which was not in his possession at the time, but he refused to explain what he meant by “anti-American statements.” The Officer also made a point to state that he knew I had recently been to San Francisco with some friends and had seen me later that day having lunch at Granzella’s, a restaurant in Williams, California; this led me to worry about whether he had been following me. He also told me that he wanted to make sure that I did not turn into another Mohammed Atta, one of the individuals identified as a September 11th hijacker. This made me very upset because I believe Officer Parrot was negatively judging my religion and I did not even know how Officer Parrot knew I was Muslim. I asked Officer Parrot if he would be saying these things to me if I had converted to Christianity or another religion and the conversation ended with Officer Parrot leaving me his business card.

8. Sometime in 2011, I had another interaction with CPD. I was at the Chico Islamic Center when CPD officers made a visit to the mosque. I believe that the CPD officers characterized their presence as being a courtesy visit intended to build good relations with the Muslim community. I listened to the presentation and then a CPD officer asked me my name, whether I went to school, and if I was employed. I responded with my name, that I had graduated from Chico State, and that I was unemployed. I do not believe the CPD officers asked anyone else questions like those that were asked of me. I believe this interaction was reported in the SAR about me; it states that the reporting agent found me to be “hesitant to interact with law enforcement,” and claimed that I “avoided eye contact, and appeared to be eavesdropping while I [the agent] spoke with other members [of the mosque].” The SAR also noted that, “based on his appearance [full beard and traditional garb] is a full convert to Islam at the young age of 26.” (Bracketed text in original). This was especially odd to me, since I was wearing blue jeans and a tee-shirt at the time.

9. At some point after the above incident, I was approached by yet another CPD

1 officer. I was walking around in downtown Chico with two older Muslim men who are friends of
 2 mine when we passed three CPD officers walking on the same street. One of the officers asked if
 3 I was Wiley, and asked if I had found a job. I confirmed my identity, told him I had not yet found
 4 a job, and jokingly asked if they wanted to give me one. They responded in the negative and the
 5 interaction essentially ended. This interaction was likewise reported in the SAR about me; it
 6 states that, “[s]ince the interaction I have seen [redacted] several times walking through
 7 [redacted] in traditional garb walking with elders of [redacted], I approached the group on at least
 8 one occasion and found [redacted] to avoid eye contact and hesitant to answer questions.”

9 10. Around May 20, 2012, I had another encounter with CPD. At the time, I was
 10 living at the small house on the same property as the Chico Islamic Center. I very much enjoy
 11 playing video games, and on that day, I was viewing a series of online reviews of different video
 12 games. I had my headphones on but was able to discern that someone was knocking loudly on
 13 the front door of my house. I got up from my computer and went to answer the door. Upon
 14 opening the door, I said “hello,” but I could not see anyone there. A moment later, two CPD
 15 officers came from around the back to the front door with their guns drawn and pointed at me.
 16 The CPD officers identified themselves and they told me they were investigating a domestic
 17 violence call. With their guns still drawn, the CPD officers instructed me to step outside of my
 18 house. I put my hands over my head and stepped outside of my house and leaned my hands
 19 against a glass window. At this point, the CPD officers lowered their guns. I informed the
 20 officers that there was no one inside the house, but they would not listen to me. Instead, they
 21 asked me if they could walk through the house. I told them I thought their shoes were dirty,
 22 indicating that I did not want them to walk through my house with their dirty shoes, but they
 23 asked again. I asked them if they had to search the house and the CPD officers responded that
 24 they wanted to search it to make sure no one was there. One officer stayed outside with me while
 25 the other went inside my house.

26 11. After searching my house, the CPD officer came outside the house and asked for
 27 my identification, which I showed him; after looking at it briefly he handed it back to me and then
 28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

both officers left. This interaction too was reported in the SAR about me; it states that the officer had looked at my computer and that my computer display was opened to a screen stating “Games that fly under the radar,” and that according to the officer, this appeared to be some sort of “flight simulator type of game.” The SAR also describes the following characteristics about me as “worthy of note”: “full conversion to Islam as a young WMA [white, male, adult],” “pious demeanor,” and “potential access to flight simulators over via [sic] the internet.” I felt that the CPD officers were just looking for a reason to look inside my house. Indeed, the SAR even notes that the supposed “domestic violence incident” was “later determined to be unfounded.” Because the SAR specifically discusses my religion and “pious demeanor” as “worthy of note,” I believe that the CPD officers had targeted me specifically and did so because of my religion.

12. A couple of months after this incident, in July 2012, I got a phone call from Officer Parrot of CPD. Officer Parrot informed me that he had spoken with me before and I told him that I remembered him. He then told me that I should take down my Facebook page because of my posts about video games. I responded that I would not take down my Facebook page and that I did not believe that my posts about video games were the reason for Officer Parrot’s request. I believe that the reason I was told to take down my Facebook page is because of my Islamic faith. Officer Parrot then told me that I was on a watch list and ended the call.

13. The call with Officer Parrot really upset me. I believe I was being targeted and am continually being subjected to law enforcement visits and scrutiny simply because of my religious beliefs.

14. Through my attorneys, I filed a Freedom of Information Act request with the Federal Bureau of Investigation (“FBI”) for records in its possession about me, and the FBI’s response shows that it maintains a file about me. By letters dated June 23, 2014 and February 29, 2016, I received documents from the FBI referencing information contained in the SAR. A true and correct copy (with personally identifying information redacted) of the June 23, 2014 letter—along with the attached documents about me—is attached to this declaration as Exhibit 2. A true and correct copy (with personally identifying information redacted) of the February 29, 2016

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

letter—along with the attached documents about me—is attached to this declaration as Exhibit 3.

15. I believe that, because of the SAR about me, information about me has been uploaded to eGuardian and an FBI database. Based on my review of the Defendants’ Answer in this matter, it is my understanding that an incident report containing information in the SAR about me was uploaded to eGuardian, which I understand to be a national database to which law enforcement agencies across the country have access. In addition, based on the documents I received from the FBI in response to my FOIA request, I believe the FBI also maintains, in some kind of database, information about me related to the information in the SAR about me.

16. As a result of the inclusion of this information about me in these databases, my reputation has been injured, as I have been branded as a person engaged in activity with a potential nexus to terrorism, even though I was simply looking at online reviews of video games.

17. In addition, as a result of the inclusion of this information about me in these databases, my privacy has been invaded because any person with access to either database has access to information about me, even though I was simply looking at online reviews of video games.

18. I believe I and even my family members have been subjected to additional law enforcement scrutiny because of the existence of the SAR about me.

19. After I filed this lawsuit, in August 2015, my sister told me that she was visited by FBI agents. She conveyed to me that the officers asked her a series of questions about me and my religious beliefs. I am concerned that those questions were prompted because of the SAR, because I brought this lawsuit, or both.

20. Given the repeated harassment I have been subjected to, including the questioning of my sister about my religious beliefs, I fear that further action may be taken against me by the FBI or by CPD as a result of the SAR about me. I also fear that further investigative harassment at the hands of the FBI or CPD might occur due to the existence of the SAR on me.

21. I continue to experience frustration and stress resulting from the creation of the SAR based on my innocent conduct of playing and reading about video games and attending

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

religious services. I am also deeply troubled by what may result from the collection, maintenance, and dissemination in a national database of a report describing me as engaging in suspicious activity with a potential nexus to terrorism.

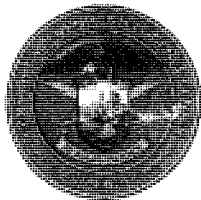
22. I believe that the defendants in this case would have benefited from input from the public on the standard for suspicious activity reporting. I would have wanted the defendants to know when they adopted their standard for suspicious activity reporting that a standard that does not require reasonable suspicion of criminal activity harms innocent people, like me, who have not engaged in any wrongdoing: it makes us the targets of law enforcement scrutiny; puts our information in government databases; and adversely affects our reputations by identifying us as individuals who have engaged in conduct with a potential nexus to terrorism. I would also have wanted the defendants to know the specific facts of my case so that they could understand the factual basis for my concerns. I would specifically have wanted the defendants to understand, based on what happened to me, that their standard for suspicious activity reporting encourages racial and religious profiling. I was not aware that the defendants sought input on the standard for suspicious activity reporting. As a result, I did not have an opportunity to share my perspective or the factual basis for my concerns.

I declare under penalty of perjury that the foregoing is true and correct. Executed this 9th day of September 2016 in Chico, California.

23.

By: 
Wiley Wayne Gill

EXHIBIT 1

**Central California Intelligence Center**

www.sacrtac.org ♦ (916) 808-8383 or (888) 884-8383 ♦ Fax (916) 874-6180

January 3, 2014

Mr. Yaman Salahi
Staff Attorney
Asian Americans Advancing Justice
Asian Law Caucus
55 Columbus Ave.
San Francisco, CA 94111
(415) 896-1701

Dear Mr. Salahi:

This letter is in response to the Public Records Act request received from the Asian Law Caucus dated December 3, 2013.

After reviewing your Public Records Act request it appears the request is for additional SAR data, from the timeframes of June 2010 to June 2012, stored in the CCIC databases and previously submitted to the ACLU in August 2012. You have specifically requested the following:

"This letter constitutes a request under the California Public Records Act, Cal. Gov. Code 6250, et seq., and Article I s 3(b) of the California Constitution on behalf of Mr. Wiley Wayne Gill for all records, including but not limited to Suspicious Activity Reports, pertaining to or referencing Mr. Gill."

The CCIC/RTAC has located only one (1) Suspicious Activity Report (SAR) related to Mr. Gill. Please see the attached redacted SAR (enclosure 1). After a thorough review of our records, there is no further information available regarding Mr. Wiley Wayne Gill.

Respectfully,

A handwritten signature in black ink, appearing to read "Herb Brown" with a stylized flourish at the end.

Herb Brown, Executive Director
Central California Intelligence Center
(916) 874-1287

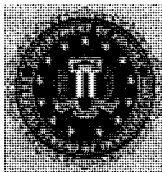
Enclosures (1)

Member Record	Task Created	Activity Date	Title	Disposition	Assignment	Activity
CCSA0000 2180	5/23/2012	5/20/2012	Suspicious Male Subject in Possession of Flight Simulator Game	pending		<p>During early 2011 I made a professional visit to the [REDACTED] [REDACTED] at [REDACTED] [REDACTED] [REDACTED] (I was in a full patrol uniform). During the visit I found the members to be welcoming and appreciative of the visit with the exception of one subject later identified as [REDACTED] [REDACTED]; CDL # [REDACTED].</p> <p>[REDACTED] was hesitant to interact with law enforcement, avoided eye contact, and appeared to be eavesdropping while I spoke with other members. I believe [REDACTED] reported he was a previous student of [REDACTED]. [REDACTED] is a [REDACTED] who based on his appearance (full beard and traditional garb) is a full convert to Islam at the young age of 26. [REDACTED] does not have a job at the time and was living on site at [REDACTED]. Since this interaction I have seen [REDACTED] several times walking through [REDACTED] in traditional garb walking with elders of [REDACTED]. I approached the group on at least one occasion and found [REDACTED] to avoid eye contact and hesitant to answer questions.</p> <p>On 5/20/12 [REDACTED] was investigating a domestic violence incident that took him to [REDACTED] in search of a suspect. During the search he conducted a cursory search of [REDACTED]'s house as there was some indication he suspect may have fled into the residence (later determined to be unfounded). [REDACTED] found the house immaculate. [REDACTED] was not very happy with [REDACTED] entering the house, presumably because he still had his shoes on. [REDACTED] noticed [REDACTED] had a computer console located in the residence. As [REDACTED] attempted to hastily close down the screen [REDACTED] noted [REDACTED] was on a [REDACTED] page titled something similar to "Games that fly under the radar." [REDACTED] noted [REDACTED] appeared to be accessing a flight simulator type of game. [REDACTED] full conversion to Islam as a young WMA and pious demeanor is rare. Coupled with the fact he is unemployed, appears to shun law enforcement contact, has potential access to flight simulators via the internet which he tried to minimize is worthy of note.</p>

Case 3:14-cv-03120-RS Document 127 Filed 11/03/18 Page 11 of 51

EXHIBIT 2

U.S. Department of Justice



Federal Bureau of Investigation
Washington, D.C. 20535

June 23, 2014

MR. YAMAN SALAHI
STAFF ATTORNEY
ADVANCING JUSTICE - ASIAN LAW CAUCUS
55 COLUMBUS AVENUE
SAN FRANCISCO, CA 94111

FOIPA Request No.: 1242637-000
Subject: GILL, WILEY WAYNE

Dear Mr. Salahi:

The enclosed documents were reviewed under the Freedom of Information/Privacy Acts (FOIPA), Title 5, United States Code, Section 552/552a. Deletions have been made to protect information which is exempt from disclosure, with the appropriate exemptions noted on the page next to the excision. In addition, a deleted page information sheet was inserted in the file to indicate where pages were withheld entirely. The exemptions used to withhold information are marked below and explained on the enclosed Explanation of Exemptions:

Section 552		Section 552a	
<input checked="" type="checkbox"/> (b)(1)	<input type="checkbox"/> (b)(7)(A)	<input type="checkbox"/> (d)(5)	
<input type="checkbox"/> (b)(2)	<input type="checkbox"/> (b)(7)(B)	<input checked="" type="checkbox"/> (j)(2)	
<input checked="" type="checkbox"/> (b)(3)	<input checked="" type="checkbox"/> (b)(7)(C)	<input type="checkbox"/> (k)(1)	
<u>50 USC § 3024(i)(1)</u>	<input checked="" type="checkbox"/> (b)(7)(D)	<input type="checkbox"/> (k)(2)	
	<input checked="" type="checkbox"/> (b)(7)(E)	<input type="checkbox"/> (k)(3)	
	<input type="checkbox"/> (b)(7)(F)	<input type="checkbox"/> (k)(4)	
<input type="checkbox"/> (b)(4)	<input type="checkbox"/> (b)(8)	<input type="checkbox"/> (k)(5)	
<input type="checkbox"/> (b)(5)	<input type="checkbox"/> (b)(9)	<input type="checkbox"/> (k)(6)	
<input checked="" type="checkbox"/> (b)(6)		<input type="checkbox"/> (k)(7)	

16 pages were reviewed and 16 pages are being released.

- Document(s) were located which originated with, or contained information concerning other Government agency(ies) [OGA]. This information has been:
 - referred to the OGA for review and direct response to you.
 - referred to the OGA for consultation. The FBI will correspond with you regarding this information when the consultation is finished.
- In accordance with standard FBI practice and pursuant to FOIA exemption (b)(7)(E) and Privacy Act exemption (j)(2) [5 U.S.C. § 552/552a (b)(7)(E)/(j)(2)], this response neither confirms nor denies the existence of your subject's name on any watch lists.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S. C. § 552(c) (2006 & Supp. IV (2010)). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist. Enclosed for your information is a copy of the Explanation of Exemptions.

You have the right to appeal any denials in this release. Appeals should be directed in writing to the Director, Office of Information Policy (OIP), U.S. Department of Justice, 1425 New York Ave., NW, Suite 11050, Washington, D.C. 20530-0001, or you may submit an appeal through OIP's eFOIA portal at <http://www.justice.gov/oip/efoia-portal.html>. Your appeal must be received by OIP within sixty (60) days from the date of this letter in order to be considered timely. The envelope and the letter should be clearly marked "Freedom of Information Appeal." Please cite the FOIPA Request Number assigned to your request so that it may be easily identified.

The enclosed material is from the main investigative file(s) in which the subject(s) of your request was the focus of the investigation. Our search located additional references, in files relating to other individuals, or matters, which may or may not be about your subject(s). Our experience has shown when ident, references usually contain information similar to the information processed in the main file(s). Because of our significant backlog, we have given priority to processing only the main investigative file(s). If you want the references, you must submit a separate request for them in writing, and they will be reviewed at a later date, as time and resources permit.

See additional information which follows.

Sincerely,



David M. Hardy
Section Chief
Record/Information
Dissemination Section
Records Management Division

Enclosures

In response to your Freedom of Information/Privacy Act (FOIPA) request submitted to the Records Management Division at Winchester, VA, enclosed is a processed copy of the documents responsive to your request.

The enclosed documents responsive to your request are exempt from disclosure in their entirety pursuant to the Privacy Act, Title 5, United States Code, Section 552(a), subsection (j)(2). However, these records have been processed pursuant to the Freedom of Information Act, Title 5, United States Code, Section 552, thereby affording you the greatest degree of access authorized by both laws.

The enclosed material is being provided at no charge.

EXPLANATION OF EXEMPTIONS**SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552**

- (b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;
- (b)(2) related solely to the internal personnel rules and practices of an agency;
- (b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute(A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could be reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could be reasonably expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;
- (b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

- (d)(5) information compiled in reasonable anticipation of a civil action proceeding;
- (j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
- (k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;
- (k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;
- (k)(4) required by statute to be maintained and used solely as statistical records;
- (k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;
- (k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

DECLASSIFIED BY: NSICG/070365761
ON: 02-19-2014

FD-1036 (Rev. 10-16-2009)

~~SECRET//NOFORN~~



FEDERAL BUREAU OF INVESTIGATION

Import Form

Form Type: FD-71A

Date: 08/09/2012

Title: U [Redacted]

b6
b7C
b7E

Approved By: [Redacted]

(U) Drafted By: [Redacted]

Case ID #: [Redacted] ~~(S)~~ ZERO FILE -

Synopsis: U On 5/20/2012, a Chico Police Department (CPD) officer made contact with Wiley Wayne GILL, DOB [Redacted] while conducting a residence search for a fleeing suspect. While in the residence, the officer turned toward a computer and observed the subject hastily attempting to close down the screen in a possible attempt to hide what he was doing on the computer from the officer. [Redacted]

[Redacted]

~~Reason: 1.4(b), (c), (d)
Derived From: Multiple Sources
Declassify On: 20370809~~

◆◆

~~SECRET//NOFORN~~

Serial 49

DECLASSIFIED BY NSICG/ J75365761
ON 02-28-2014

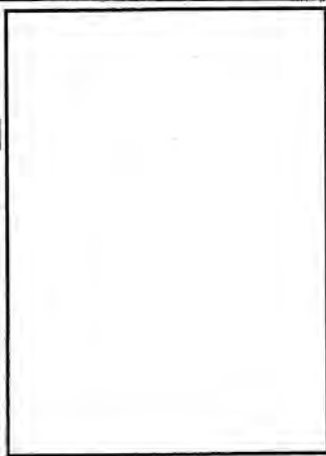
~~SECRET//NOFORN~~

Generated: 08/09/2012 3:34 PM EDT

Incident Summary

197249_SC (U) [Redacted]

(U) On 5/20/2012, a Chico Police Department (CPD) officer made contact with Wiley Wayne GILL, DOB [Redacted] while conducting a residence search for a fleeing suspect. While in the residence, the officer turned toward a computer and observed the subject hastily attempting to close down the screen in a possible attempt to hide what he was doing on the computer from the officer. [Redacted]



b6
b7C
b7E

Subjects

(U) Wiley Wayne GILL (Male, Approx. Age 26)
Eye Color: Brown
Hair Color: Brown
Height: 73 inches
Weight: 200 lbs
Build: Medium
US Person: Yes
Public Figure: No
Complexion: Fair

Witnesses

(U) [Redacted] Police Officer (Male)
Other Information: Chico Police Department Officer
Witness Type: Law Enforcement
Protect Witness: No
Witness Available: Yes

(U) [Redacted] Detective (Male)
Other Information: Chico Police Department TLO
Officer
Witness Type: Law Enforcement
Witness Available: Yes

Other Persons

Targets

Vehicles

Weapons

Locations

~~SECRET//NOFORN~~

(U) The Islamic Center of Chico
Other
1316 Nord Avenue
Chico, California 95927
United States

Leads

Attachments

(U) [Redacted]

Links

Notes

(U) GILL, Wiley
Description: Birth Date Range Begin: [Redacted]
Status: Approved
Attachments:
History: 08/08/2012 04:48 PM Imported note from [Redacted] [Redacted]

b6
b7C
b7E

(U) Incident Additional Details

Description: The CPD officer reported that he initially met GILL in 2011 when he made an official visit to The Islamic Center of Chico where GILL was a member. He said all of the members were welcoming and appreciative of a visit from law enforcement with the exception of GILL. Additionally, GILL is described as avoiding eye contact, hesitant to interact with the officer, and at one point appeared to be eavesdropping while the officer spoke with other members at the center. The officer reported that GILL did not have a job and resided at the Mosque.
The officer described GILL as being agitated during the recent encounter, possibly because GILL is a Muslim and the officer was wearing shoes inside his residence.
Status: Approved
Attachments:
History: 08/08/2012 04:48 PM Imported note from [Redacted] [Redacted]

(U) Witness [Redacted] Police Officer additional information

Description: [Redacted]
Credible: [Redacted]
Status: Approved
Attachments:
History: 08/08/2012 04:48 PM Imported note from [Redacted] [Redacted]

(U) Incident Additional Details

Description: [Redacted]
male subject: Wiley Wayne GILL, DOB: [Redacted]
[Redacted]
Status: Approved
Attachments:
History:

~~SECRET//NOFORN~~

08/08/2012 04:48: PM Imported note from [redacted] [redacted]

(U) Witness [redacted] Detective additional information

Description: [redacted]

Credible [redacted]

Status: Approved

Attachments:

History: 08/08/2012 04:48: PM Imported note from [redacted] [redacted]

b6
b7C
b7E

(U) Incident Additional Details

Description: On Jul 27, 2012, Central California Intelligence Center Analyst [redacted] conducted basic database queries on Wiley Wayne GILL [redacted]

[redacted]

A California DMV records check returned a match to a valid Class C non-commercial California driver's license number [redacted] with an expiration date of February 21, 2016 and a mailing address of [redacted] in Chico. An address of [redacted] in Chico is listed as (Other) in the DMV record as of May 4, 2007. GILL is the registered owner of a 1973 Plymouth Valiant 2-door hardtop, license number [redacted]. The Islamic Center of Chico at 1316 Nord Avenue in Chico is the listed address for the vehicle.

Query searches of NCIC, Automated Firearms System, Coplink [redacted] Sac Known Persons Finder, Parole Leads, Supervised Release File, Wanted Persons, Missing and Unidentified Persons, Sex and Arson Registration searches returned no information on GILL.

A search of automated Criminal History Search returned no derogatory information. The subject has a CII number of [redacted] as an applicant for a public agency.

The TLO.com CLEAR public database records for GILL lists The Islamic Center of Chico at 1316 Nord Avenue in Chico as his last known address. There are two known phone numbers listed in GILL's name, which include a cell phone, [redacted] and a land-line phone, [redacted].

An open source query returned no matches to GILL on social media network accounts such as Facebook and MySpace, and no matches on search engines Yahoo, Google, and Bing.

A search of the [redacted]

[redacted]

Status: Approved

Attachments:

History: 08/08/2012 04:48: PM Imported note from [redacted] [redacted]

(U) Incident additional information

Description: Submitting Organization Details

ORI: CAF00100

Name: Sacramento CCIC

Email: [redacted]

Agency Name 1: Sacramento CCIC

City: Sacramento

State: CA

Country: US

Field Office: SC

~~SECRET//NOFORN~~

Incident Author Information
 ORI: CAF00100
 Email: [Redacted]
 Last Name: [Redacted]
 First Name: [Redacted]
 Police Report: None
 Created Timestamp: 2012-08-02T16:40:32.166
 Modified Timestamp: 2012-08-08T16:34:43.324
 Status: Approved
 Attachments:
 History:
 08/08/2012 04:48 PM Imported note from [Redacted] [Redacted]

b6
b7C
b7D
b7E

(U) Incident Additional Details
 Description: On 8/2/2012, FBI/IA [Redacted] queries on the subject [Redacted]
 Status: Approved
 Attachments:
 History:
 08/08/2012 04:48 PM Imported note from [Redacted] [Redacted]

(U) ~~(S//NF)~~ [Redacted]
 Investigative Method: Access/examine FBI/DOJ records, and obtain information from FBI/DOJ personnel.
 Description: (U) IA [Redacted] FBI, conducted [Redacted]
 [Redacted]
 (U) [Redacted]
 (U) ~~(S//NF)~~ [Redacted]
 [Redacted]
 (U) [Redacted]
 (U) [Redacted]
 Status: No additional information was found
 Completed
 Attachments:
 History:
 08/09/2012 01:19 PM [Redacted] [Redacted]

Disposition

Workflow

08/08/2012 04:48 PM	Imported Incident from [Redacted]	Assigned By	[Redacted]
08/09/2012 01:21 PM	Incident assigned	Assigned To	[Redacted]
		Assigned By	[Redacted]
		Assigned To	[Redacted]

~~SECRET//NOFORN~~

08/09/2012 03:33 PM Incident opened

Assigned By:

Assigned To:



b6
b7C
b7E

SENTINEL Uploads

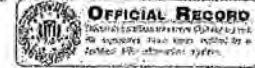
(S)

CLASSIFIED BY NSICG/J75065761
REASON 1.4 (G)
DECLASSIFY ON: 02-25-2089
DATE: 02-25-2014

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

FD-1036 (Rev. 10-16-2009)

~~SECRET // ORCON // NOFOR~~



b1
b3
b6
b7C
b7E

FEDERAL BUREAU OF INVESTIGATION

Import Form

Form Type: FD-71A

Date: 10/03/2012

Title: U [Redacted]

Approved By: [Redacted]

Drafted By: [Redacted]

(U)

Case ID #: [Redacted] ~~(S)~~ ZERO FILE -

Synopsis: U On 5/20/2012, a Chico Police Department (CPD) officer made contact with Wiley Wayne GILL, DOB [Redacted] while conducting a residence search for a fleeing suspect. While in the residence, the officer turned toward a computer and observed the subject hastily attempting to close down the screen in a possible attempt to hide what he was doing on the computer from the officer. [Redacted]

[Redacted]

~~Reason: 1.4(b), (c), (d)
Derived From: Multiple Sources
Declassify On: 20370809~~

◆◆

(S)

~~SECRET // ORCON // NOFOR~~



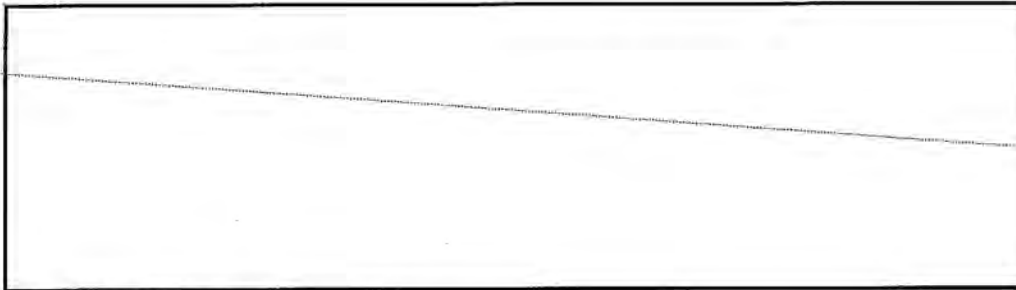
Serial 18

CLASSIFIED BY: NSICG/J78J65T61
REASON: 1.4 (G)
DECLASSIFY ON: 02-25-2039
DATE: 02-25-2014

~~SECRET//ORCON//NOFOR~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)



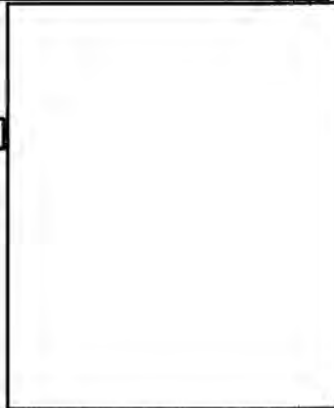
b1
b3
b6
b7C
b7E

Generated: 10/03/2012 12:20 PM EDT

Incident Summary

197249_SC (U)

(U) On 5/20/2012, a Chico Police Department (CPD) officer made contact with Wiley Wayne GILL, DOB [redacted] while conducting a residence search for a fleeing suspect. While in the residence, the officer turned toward a computer and observed the subject hastily attempting to close down the screen in a possible attempt to hide what he was doing on the computer from the officer [redacted]



Subjects

(U) Wiley Wayne GILL (Male, Approx. Age 26)
Eye Color: Brown
Hair Color: Brown
Height: 73 inches
Weight: 200 lbs
Build: Medium
US Person: Yes
Public Figure: No
Complexion: Fair

Witnesses

(U) [redacted] Police Officer (Male)
Other Information: Chico Police Department Officer
Witness Type: Law Enforcement
Protect Witness: No
Witness Available: Yes

(U) [redacted] Detective (Male)
Other Information: Chico Police Department TLO
Officer
Witness Type: Law Enforcement
Witness Available: Yes

Other Persons

1
~~SECRET~~

(S)

~~SECRET//ORCON//NOFORN~~



- Targets
- Vehicles
- Weapons
- Locations

(U) The Islamic Center of Chico
 Other
 1316 Nord Avenue
 Chico, California 95927
 United States

Leads

Attachments



Links

Notes

b1
b3
b6
b7C
b7E

(U) GILL, Willey
 Description: Birth Date Range Begin: [Redacted]
 Status: Approved
 Attachments:
 History: 08/08/2012 04:48 PM Imported note from [Redacted] [Redacted]

(U) Incident Additional Details

Description: The CPD officer reported that he initially met GILL in 2011 when he made an official visit to The Islamic Center of Chico where GILL was a member. He said all of the members were welcoming and appreciative of a visit from law enforcement with the exception of GILL. Additionally, GILL is described as avoiding eye contact, hesitant to interact with the officer, and at one point appeared to be eavesdropping while the officer spoke with other members at the center. The officer reported that GILL did not have a job and resided at the Mosque.
 The officer described GILL as being agitated during the recent encounter, possibly because GILL is a Muslim and the officer was wearing shoes inside his residence.
 Status: Approved
 Attachments:
 History: 08/08/2012 04:48 PM Imported note from [Redacted] [Redacted]

(U) Witness [Redacted] Police Officer additional information

Description: [Redacted]
 Credible: [Redacted]
 Status: Approved
 Attachments:
 History: 08/08/2012 04:48 PM Imported note from [Redacted] [Redacted]

(U) Incident Additional Details

~~SECRET~~

(S)

~~SECRET//ORCON//NOFORN~~

b1
b3
b6
b7C
b7E

Description: [Redacted]
[Redacted]
[Redacted]

Status: Approved

Attachments:

History: 08/08/2012 04:48 PM Imported note from [Redacted] [Redacted]

(U) Witness [Redacted] Detective additional information

Description: [Redacted]
Credible [Redacted]

Status: Approved

Attachments:

History: 08/08/2012 04:49 PM Imported note from [Redacted] [Redacted]

(U) Incident Additional Details

Description: On Jul 27, 2012, Central California Intelligence Center Analyst [Redacted] conducted basic database queries on Wiley Wayne GILL [Redacted]

A California DMV records check returned a match to a valid Class C non-commercial California driver's license, number [Redacted] with an expiration date of February 21, 2015 and a mailing address of [Redacted] in Chico. An address of [Redacted] in Chico is listed as [Redacted] Olher, in the DMV record as of May 4, 2007. GILL is the registered owner of a 1973 Plymouth Valiant, 2-door hardtop, license number [Redacted]. The Islamic Center of Chico at 1316 Nord Avenue in Chico is the listed address for the vehicle.

Query searches of NCIC, Automated Firearms System, Coplink [Redacted] Sac Known Persons Finder, Parole Leads, Supervised Release File, Wanted Persons, Missing and Unidentified Persons, Sex and Arson Registration searches returned no information on GILL.

A search of automated Criminal History Search returned no derogatory information. The subject has a CII number of [Redacted] as an applicant for a public agency.

The TLO.com CLEAR public database records for GILL lists The Islamic Center of Chico at 1316 Nord Avenue in Chico as his last known address. There are two known phone numbers listed in GILL's name, which include a cell phone, [Redacted] and a land-line phone, [Redacted].

An open source query returned no matches to GILL on social media network accounts such as Facebook and MySpace; and no matches on search engines Yahoo, Google, and Bing.

A search of the [Redacted]
[Redacted]
[Redacted]

Status: Approved

Attachments:

History: 08/08/2012 04:48 PM Imported note from [Redacted] [Redacted]

(U) Incident additional information

Description: Submitting Organization Details

~~SECRET~~

(S) ~~SECRET//ORCON/NOFORN~~ [Redacted]

b1
b3
b6
b7C
b7D
b7E

ORI: CAFCD0100
 Name: Sacramento CCIC
 Email: [Redacted]
 Agency Name: Sacramento CCIC
 City: Sacramento
 State: CA
 Country: US
 Field Office: SC

Incident Author Information
 ORI: CAFCD0100
 Email: [Redacted]
 Last Name: [Redacted]
 First Name: [Redacted]

Police Report: None
 Created Timestamp: 2012-08-02T16:46:32.166
 Modified Timestamp: 2012-08-08T16:34:43.324

Status: Approved

Attachments:

History:
 08/08/2012 04:46 PM Imported note from [Redacted]

(U) Incident Additional Details

Description: On 8/2/2012, FBI IA [Redacted] queries on the subject [Redacted]

Status: Approved

Attachments:

History:
 08/08/2012 04:46 PM Imported note from [Redacted]

(U)

~~(S//NF)~~ Classified database checks

Investigative: Access/examine FBI/DOJ records, and obtain information from FBI/DOJ personnel.
 Method: [Redacted]
 Description: (U) IA [Redacted] FBI conducted [Redacted]

(U) [Redacted]

(U) [Redacted]

(U) [Redacted]

No additional information was found

Status: Completed

Attachments:

History:
 08/09/2012 01:19 PM [Redacted]

(U) [Redacted]

Investigative Method:
 Description: [Redacted]

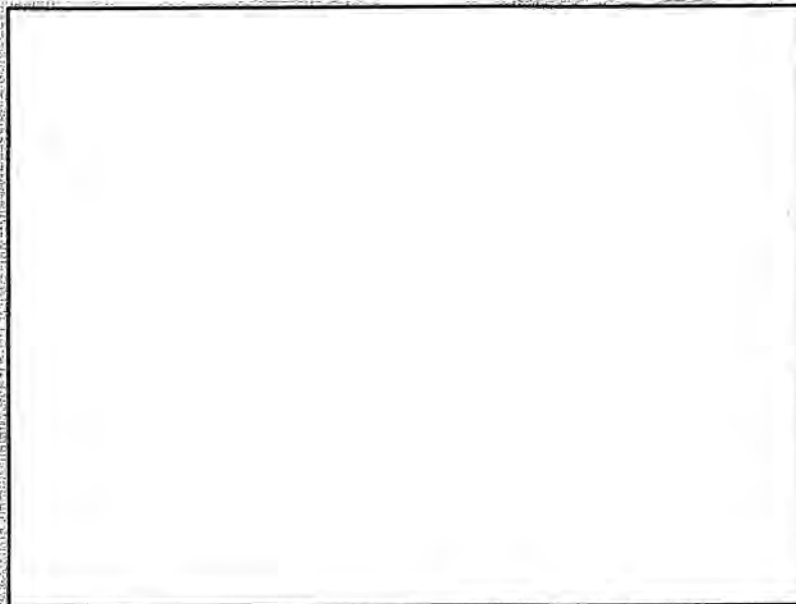
4
~~SECRET~~

(S)

~~SECRET//ORCON/NOFORN~~



b1
b3
b6
b7C
b7E



Status: Approved

Attachments:

History:

- 08/20/2012 02:17 PM Created Note
- 10/01/2012 05:06 PM Submit note for approval
- 10/01/2012 05:18 PM Approve note



(U) Interview of Wiley Gill

Investigative Method: Interview or request information from members of the public and private entities.

Description:

On approximately September 12, 2012, TFO's [redacted] and [redacted] attempted to interview WILEY GILL at his residence 1316 Nord Avenue, Chico, CA. This residence is co-located with and owned by the Chico Islamic Center. TFO's [redacted] and [redacted] were informed that GILL no longer lives at the residence.

On October 1, 2012, TFO [redacted] contacted GILL via his cell phone, [redacted] in an attempt to set up an interview with him. GILL did not answer his phone and TFO [redacted] did not leave a message. Approximately an hour later, GILL called [redacted] phone back. TFO [redacted] informed GILL of his identity and the nature of his telephone call. GILL seemed suspicious at first but then provided the following information:

GILL allowed law enforcement officers to come into his house at 1316 Nord Avenue a few months ago when he was told that they were searching the area for a fleeing suspect. This is the only time that GILL knows that law enforcement officers have been in his residence.

GILL was informed that one of the officers in his house saw something on his computer screen titled "Games that Fly Under the Radar." GILL acknowledged that this is probably what the officer saw. GILL stated that this is a YouTube video that highlights the top ten best and worst games people play.

GILL asked why the officers didn't question him then when they believed that something appeared suspicious? TFO [redacted] agreed that this was a logical question to which he did not know the answer.

~~SECRET~~

(S)

~~SECRET//ORCON//NOFORN~~ [Redacted]

b1
b3
b6
b7C
b7D
b7E

GILL was cooperative throughout the telephonic interview with TFC [Redacted]

Status: Approved

Attachments:

History:

- 10/01/2012 03:28 PM Created Note: Attempted Interview of Wiley Gill [Redacted]
- 10/01/2012 05:08 PM Submit note for approval [Redacted]
- 10/01/2012 05:19 PM Approve note [Redacted]

(U//FOUO)

[Redacted] Report

Investigative Method: [Redacted]

Description: A review of [Redacted] report for WILEY GILL reveals the following identifiers:

Name: WILEY WAYNE GILL
 DOB: [Redacted]
 SSN: [Redacted]
 Cell Phone: [Redacted]
 Residential Phone: [Redacted] (registered in Stoneford, CA)
 Address: [Redacted]
 Former Addresses: [Redacted]

Status: Approved

Attachments:

History:

- 10/01/2012 06:04 PM Created Note: [Redacted] report [Redacted]
- 10/01/2012 05:19 PM Approve note [Redacted]

(S)

(U) ~~(S//OC/N)~~

[Redacted] Baseline Checks

Investigative Method: Access/examine FBI/DOJ records, and obtain information from FBI/DOJ personnel.

Description: 8. Subject's current place of employment and position. When available, identifying information has been obtained. It should be used to conduct the checks necessary to answer the following questions:

[Redacted]

1a [Redacted]

2a [Redacted]

6
~~SECRET~~

~~SECRET//ORCON//NOFORN~~

(S)

[Redacted]

b1
b3
b6
b7C
b7E

[Redacted]

[Redacted] NCIC query reveals that GILL was an applicant for the California State University, Chico Police Department on 12/09/2011.

(S)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted] According to TFC [Redacted] GILL is a night-shift custodian at the California State University, Chico.

[Redacted]

~~SECRET~~

(S)

~~SECRET//ORCON/NOFORN~~ [Redacted]

b1
b3
b6
b7C
b7E

[Redacted]

[Redacted]

Status: Approved

Attachments:

History:

10/01/2012 05:10 PM Created Note: Baseline Checks

10/02/2012 12:14 PM Submit note for approval

10/03/2012 12:19 PM Approve note

[Redacted]

Disposition

(U//FOUO) Disposition

Note:

[Redacted]

Wiley

Wayne GILL. It should be noted that in the past when GILL was interviewed he was uncooperative and claimed that he was being spied on by the NSA and other governmental agencies. A second interview was conducted with GILL. GILL was overall cooperative with law enforcement. GILL explained that the suspicious video that law enforcement saw on his computer screen in May 2012 was about computer gaming, which has been corroborated via [Redacted]

Disposition:

[Redacted]

Workflow

08/08/2012 04:48 PM Imported incident from [Redacted]

Assigned By: [Redacted]

08/09/2012 01:21 PM Incident assigned

Assigned To: [Redacted]
Assigned By: [Redacted]

08/09/2012 03:33 PM Incident opened

Assigned To: [Redacted]
Assigned By: [Redacted]

09/06/2012 03:02 PM

[Redacted]

Assigned By: [Redacted]

Assigned To: [Redacted]

(S)

~~SECRET//ORCON//NOFORN~~ [Redacted]

b1
b3
b6
b7C
b7E

10/02/2012 12:15 PM	Incident submitted for closure	Assigned By:	[Redacted]
		Assigned To:	[Redacted]
10/03/2012 12:20 PM	Incident closed	Assigned By:	[Redacted]
		Assigned To:	[Redacted]

SENTINEL Uploads

08/09/2012 03:35 PM SENTINEL Case File: [Redacted]



EXHIBIT 3



U.S. Department of Justice

Federal Bureau of Investigation
Washington, D.C. 20535

February 29, 2016

MR. YAMAN SALAHI
STAFF ATTORNEY
ADVANCING JUSTICE - ASIAN LAW CAUCUS
55 COLUMBUS AVENUE
SAN FRANCISCO, CA 94111

FOIPA Request No.: 1242637-000
Appeal No.: AP-2014-04336
Subject: GILL, WILEY WAYNE

Dear Mr. Salahi:

As a result of your administrative appeal to the Office of Information Policy (OIP), Department of Justice (DOJ), material was located responsive to your request for information concerning Wiley Wayne Gill. Enclosed is a processed copy of the responsive information the FBI has on file. The enclosed documents were reviewed under the Freedom of Information/Privacy Acts (FOIPA), Title 5, United States Code, Section 552/552a. Deletions have been made to protect information which is exempt from disclosure, with the appropriate exemptions noted on the page next to the excision. In addition, a deleted page information sheet was inserted in the file to indicate where pages were withheld entirely. The exemptions used to withhold information are marked below and explained on the enclosed Explanation of Exemptions:

Section 552		Section 552a	
<input checked="" type="checkbox"/> (b)(1)	<input type="checkbox"/> (b)(7)(A)	<input type="checkbox"/> (d)(5)	
<input type="checkbox"/> (b)(2)	<input type="checkbox"/> (b)(7)(B)	<input checked="" type="checkbox"/> (j)(2)	
<input checked="" type="checkbox"/> (b)(3)	<input checked="" type="checkbox"/> (b)(7)(C)	<input type="checkbox"/> (k)(1)	
<u>50 U.S.C. 3024(i)(1)</u>	<input type="checkbox"/> (b)(7)(D)	<input type="checkbox"/> (k)(2)	
_____	<input checked="" type="checkbox"/> (b)(7)(E)	<input type="checkbox"/> (k)(3)	
_____	<input type="checkbox"/> (b)(7)(F)	<input type="checkbox"/> (k)(4)	
<input type="checkbox"/> (b)(4)	<input type="checkbox"/> (b)(8)	<input type="checkbox"/> (k)(5)	
<input type="checkbox"/> (b)(5)	<input type="checkbox"/> (b)(9)	<input type="checkbox"/> (k)(6)	
<input checked="" type="checkbox"/> (b)(6)		<input type="checkbox"/> (k)(7)	

16 pages were reviewed and 16 pages are being released.

Document(s) were located which originated with, or contained information concerning, other Government Agency (ies) [OGA].

This information has been referred to the OGA(s) for review and direct response to you.

We are consulting with another agency. The FBI will correspond with you regarding this information when the consultation is completed.

In accordance with standard FBI practice and pursuant to FOIA exemption (b)(7)(E) and Privacy Act exemption (j)(2) [5 U.S.C. § 552/552a (b)(7)(E)/(j)(2)], this response neither confirms nor denies the existence of your subject's name on any watch lists.

Case 3:14-cv-03120-RS Document 127 Filed 11/03/16 Page 34 of 51

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S. C. § 552(c) (2006 & Supp. IV (2010)). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist. Enclosed for your information is a copy of the Explanation of Exemptions.

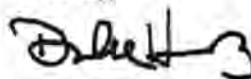
For questions regarding our determinations, visit the www.fbi.gov/foia website under "Contact Us." The FOIPA Request Number listed above has been assigned to your request. Please use this number in all correspondence concerning your request. Your patience is appreciated.

You have the right to appeal any denials in this release. Appeals should be directed in writing to the Director, Office Information Policy (OIP), U.S. Department of Justice, 1425 New York Ave., NW, Suite 11050, Washington, D.C. 20530-0001, or you may submit an appeal through OIP's eFOIA portal at <http://www.justice.gov/oip/efoia-portal.html>. Your appeal must be received by OIP within sixty (60) days from the date of this letter in order to be considered timely. The envelope and the letter should be clearly marked "Freedom of Information Appeal." Please cite the FOIPA Request Number assigned to your request so that it may be easily identified.

The enclosed material is from the main investigative file(s) in which the subject(s) of your request was the focus of the investigation. Our search located additional references, in files relating to other individuals, or matters, which may or may not be about your subject(s). Our experience has shown when ident, references usually contain information similar to the information processed in the main file(s). Because of our significant backlog, we have given priority to processing only the main investigative file(s). If you want the references, you must submit a separate request for them in writing, and they will be reviewed at a later date, as time and resources permit.

See additional information which follows.

Sincerely,



David M. Hardy
Section Chief
Record/Information
Dissemination Section
Records Management Division

Enclosure(s)

In response to your administrative appeal to OIP, enclosed is a processed copy of the FBI file information you appealed.

The enclosed documents responsive to your request are exempt from disclosure in their entirety pursuant to the Privacy Act, Title 5, United States Code, Section 552(a), subsection (j)(2). However, these records have been processed pursuant to the Freedom of Information Act, Title 5, United States Code, Section 552, thereby affording you the greatest degree of access authorized by both laws.

The enclosed documents contained represent the final release of information responsive to your administrative appeal from the FBI.

This material is being provided to you at no charge.

EXPLANATION OF EXEMPTIONS**SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552**

- (b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;
- (b)(2) related solely to the internal personnel rules and practices of an agency;
- (b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;
- (b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

- (d)(5) information compiled in reasonable anticipation of a civil action proceeding;
- (j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
- (k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;
- (k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;
- (k)(4) required by statute to be maintained and used solely as statistical records;
- (k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;
- (k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

DECLASSIFIED BY NSICG/J75J65T61
ON 02-19-2014

FD-1036 (Rev. 10-16-2009)

~~SECRET//NOFORN~~



FEDERAL BUREAU OF INVESTIGATION
Import Form

Form Type: FD-71A

Date: 08/09/2012

Title: U Suspicious behavior by identified male subject accessing flight simulator game in Chico

Approved By:

Drafted By:

Case ID #: ~~(S)~~ ZERO FILE -

b6
b7C
b7E

(U)

Synopsis: U On 5/20/2012, a Chico Police Department (CPD) officer made contact with Wiley Wayne GILL, DOB while conducting a residence search for a fleeing suspect. While in the residence, the officer turned toward a computer and observed the subject hastily attempting to close down the screen in a possible attempt to hide what he was doing on the computer from the officer. Before the screen was closed, the officer noted what appeared to be YouTube access on the screen titled something to the effect of "Games that fly under the radar." The officer suspected GILL was accessing a flight simulator type game.

~~Reason: 1.4(b), (c), (d)
Derived From: Multiple Sources
Declassify On: 20370809~~

◆◆

~~SECRET//NOFORN~~

Serial 49

DECLASSIFIED BY NSICG/ J75J65T61
ON 02-28-2014

Case 3:14-cv-03120-RS Document 127 Filed 11/03/16 Page 37 of 51

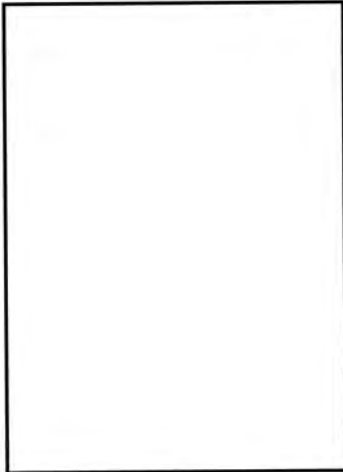
~~SECRET//NOFORN~~

Generated: 08/09/2012 3:34 PM EDT

Incident Summary

197249_SC (U) Suspicious behavior by identified male subject accessing flight simulator game in Chico

(U) On 5/20/2012, a Chico Police Department (CPD) officer made contact with Wiley Wayne GILL, DOB [REDACTED] while conducting a residence search for a fleeing suspect. While in the residence, the officer turned toward a computer and observed the subject hastily attempting to close down the screen in a possible attempt to hide what he was doing on the computer from the officer. Before the screen was closed, the officer noted what appeared to be YouTube access on the screen titled something to the effect of "Games that fly under the radar." The officer suspected GILL was accessing a flight simulator type game.



b6
b7C
b7E

Subjects

(U) Wiley Wayne GILL (Male, Approx. Age 26)
Eye Color: Brown
Hair Color: Brown
Height: 73 inches
Weight: 200 lbs.
Build: Medium
US Person: Yes
Public Figure: No
Complexion: Fair

Witnesses

(U) [REDACTED] Police Officer (Male)
Other Information: Chico Police Department Officer.
Witness Type: Law Enforcement
Protect Witness: No
Witness Available: Yes

(U) [REDACTED] Detective (Male)
Other Information: Chico Police Department TLO
Officer
Witness Type: Law Enforcement
Witness Available: Yes

Other Persons

Targets

Vehicles

Weapons

Locations

~~SECRET//NOFORN~~

(U) The Islamic Center of Chico
Other
1316 Nord Avenue
Chico, California 95927
United States

Leads

Attachments

(U) [Redacted]

b7E

Links

Notes

(U) GILL, Wiley

Description: Birth Date Range Begin: [Redacted]

Status: Approved

Attachments:

History: 08/08/2012 04:48 PM Imported note from [Redacted] [Redacted]

b7E

(U) Incident Additional Details

Description: The CPD officer reported that he initially met GILL in 2011 when he made an official visit to The Islamic Center of Chico where GILL was a member. He said all of the members were welcoming and appreciative of a visit from law enforcement with the exception of GILL. Additionally, GILL is described as avoiding eye contact, hesitant to interact with the officer; and at one point appeared to be eavesdropping while the officer spoke with other members at the center. The officer reported that GILL did not have a job and resided at the Mosque.

The officer described GILL as being agitated during the recent encounter, possibly because GILL is a Muslim and the officer was wearing shoes inside his residence.

Status: Approved

Attachments:

History: 08/08/2012 04:48 PM Imported note from [Redacted] [Redacted]

b7E

(U) Witness [Redacted] Police Officer additional information

Description: [Redacted]

Credible: YES

Status: Approved

Attachments:

History: 08/08/2012 04:48 PM Imported note from [Redacted] [Redacted]

b7E

(U) Incident Additional Details

Description: [Redacted] due to suspicious activity related to an identified male subject, Wiley Wayne GILL, DOB [Redacted] who was reportedly accessing a flight simulator game on YouTube with the title "Games that fly under the radar", and where he was acting suspiciously and appeared to be avoiding interaction with law enforcement [Redacted]

Status: Approved

Attachments:

History:

b7E

~~SECRET//NOFORN~~

08/08/2012 04:48 PM Imported note from [redacted] [redacted]

b7E

(U) Witness [redacted] Detective additional information

b6
b7C

Description: [redacted]
Credible: YES

Status: Approved
Attachments:

History: 08/08/2012 04:48 PM Imported note from [redacted] [redacted]

b7E

(U) Incident Additional Details

Description: On Jul 27, 2012, Central California Intelligence Center Analyst [redacted] conducted basic database queries on Wiley Wayne GILL, who was reportedly on a YouTube video site titled something to the effect of ¿Games that fly under the radar¿. GILL is suspected of accessing a flight simulator type game.

b6
b7C

A California DMV records check returned a match to a valid Class C non-commercial California driver¿s license, number [redacted] with an expiration date of February 21, 2015 and a mailing address of [redacted] in Chico. An address of [redacted] in Chico is listed as ¿Other¿ in the DMV record as of May 4, 2007. GILL is the registered owner of a 1973 Plymouth Valiant, 2-door hardtop, license number [redacted]. The Islamic Center of Chico at 1316 Nord Avenue in Chico is the listed address for the vehicle.

Query searches of NCIC, Automated Firearms System, Coplink [redacted] Sac Known Persons Finder, Parole Leads, Supervised Release File, Wanted Persons, Missing and Unidentified Persons, Sex and Arson Registration searches returned no information on GILL.

b7E

A search of automated Criminal History Search returned no derogatory information. The subject has a CII number of [redacted] as an applicant for a public agency.

The TLO.com CLEAR public database records for GILL lists The Islamic Center of Chico at 1316 Nord Avenue in Chico as his last known address. There are two known phone numbers listed in GILL¿s name, which include a cell phone, [redacted] and a land-line phone, [redacted].

An open source query returned no matches to GILL on social media network accounts such as Facebook and MySpace; and no matches on search engines Yahoo, Google, and Bing.

A search of the ¿Games that fly under the radar¿ on YouTube returned no exact match to that title; however, many games with similar titles were easily accessible on YouTube.

[redacted]

b7E

Status: Approved

Attachments:

History: 08/08/2012 04:48 PM Imported note from [redacted] [redacted]

b7E

(U) Incident additional information

Description: Submitting Organization Details
ORI: CAFUC0100
Name: Sacramento CCIC
Email: [redacted]
Agency Name 1: Sacramento CCIC
City: Sacramento
State: CA
Country: US
Field Office: SC

b6
b7C

~~SECRET//NOFORN~~

Incident Author Information

ORI: CAFUCU0100

Email: [Redacted]

Last Name: [Redacted]

First Name: [Redacted]

Police Report: None

Created Timestamp: 2012-08-02T16:46:32.166

Modified Timestamp: 2012-08-08T16:34:43.324

Status: Approved

Attachments:

History:

08/08/2012 04:48 PM Imported note from [Redacted] [Redacted]

b6
b7C

b7E

(U) Incident Additional Details

Description: On 8/2/2012, FBI IA [Redacted] queries on the subject. [Redacted]

Status: Approved

Attachments:

History:

08/08/2012 04:48 PM Imported note from [Redacted] [Redacted]

b6
b7C
b7E

b7E

(U)

~~(S//NF)~~ [Redacted]

Investigative Method: Access/examine FBI/DOJ records, and obtain information from FBI/DOJ personnel.

Description: (U) IA [Redacted] FBI, conducted [Redacted]

b7E

b6
b7C
b7E

(U) [Redacted]

b7E

(U)

~~(S//NF)~~ [Redacted]

(U) See handling agent SA [Redacted] for more information

(U) [Redacted]

b6
b7C
b7E

No additional information was found

Status: Completed

Attachments:

History:

08/09/2012 01:19 PM [Redacted] [Redacted]

b6
b7C
b7E

Disposition

Workflow

08/08/2012 04:48 PM	Imported Incident from [Redacted]	Assigned By	[Redacted]
08/09/2012 01:21 PM	Incident assigned.	Assigned To	[Redacted]
		Assigned By	[Redacted]
		Assigned To	[Redacted]

b6
b7C
b7E

~~SECRET//NOFORN~~

08/09/2012 03:33 PM Incident opened

Assigned By:



Assigned To:

b6
b7C
b7E

SENTINEL Uploads

CLASSIFIED BY NSICG/J75J65T61

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DECLASSIFY ON: 02-25-2039

DATE: 02-25-2014

FD-1036 (Rev. 10-16-2009)

~~SECRET//ORCON//NOFOR~~



b1
b3
b6
b7C
b7E

FEDERAL BUREAU OF INVESTIGATION

Import Form

Form Type: FD-71A

Date: 10/03/2012

Title: U Suspicious behavior by identified male subject accessing flight simulator game in Chico

Approved By: [Redacted]

Drafted By: [Redacted]

Case ID #: [Redacted]

~~(S)~~ ZERO FILE -

Synopsis: U On 5/20/2012, a Chico Police Department (CPD) officer made contact with Wiley Wayne GILL, DOB [Redacted] while conducting a residence search for a fleeing suspect. While in the residence, the officer turned toward a computer and observed the subject hastily attempting to close down the screen in a possible attempt to hide what he was doing on the computer from the officer. Before the screen was closed, the officer noted what appeared to be YouTube access on the screen titled something to the effect of "Games that fly under the radar." The officer suspected GILL was accessing a flight simulator type game.

~~Reason: 1.4(b), (c), (d)~~

~~Derived From: Multiple Sources~~

~~Declassify On: 20370809~~

◆◆

(S)

~~SECRET//ORCON//NOFOR~~

Serial 18

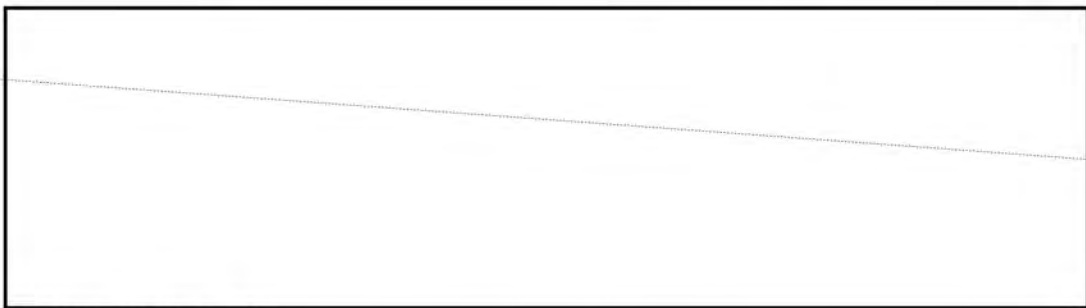
CLASSIFIED BY NSICG/17J36AT61
REASON: 1.4 (c)
DECLASSIFY ON: 02-25-2039
DATE: 02-25-2014

Case 3:14-cv-03120-RS Document 127 Filed 11/03/16 Page 46 of 51

~~SECRET//ORCON//NOFORN~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)



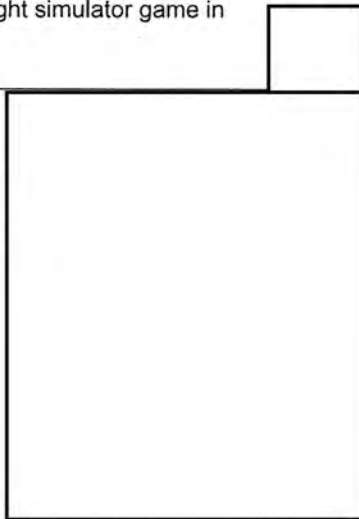
b1
b3

Generated: 10/03/2012 12:20 PM EDT

Incident Summary

197249_SC (U) Suspicious behavior by identified male subject accessing flight simulator game in Chico

(U) On 5/20/2012, a Chico Police Department (CPD) officer made contact with Wiley Wayne GILL, DOB [redacted] while conducting a residence search for a fleeing suspect. While in the residence, the officer turned toward a computer and observed the subject hastily attempting to close down the screen in a possible attempt to hide what he was doing on the computer from the officer. Before the screen was closed, the officer noted what appeared to be YouTube access on the screen titled something to the effect of "Games that fly under the radar." The officer suspected GILL was accessing a flight simulator type game.



b7E

Subjects

(U) Wiley Wayne GILL (Male, Approx. Age 26)
Eye Color: Brown
Hair Color: Brown
Height: 73 inches
Weight: 200 lbs.
Build: Medium
US Person: Yes
Public Figure: No
Complexion: Fair

Witnesses

(U) [redacted] Police Officer (Male)
Other Information: Chico Police Department Officer.
Witness Type: Law Enforcement
Protect Witness: No
Witness Available: Yes

b6
b7C

(U) [redacted] Detective (Male)
Other Information: Chico Police Department TLO
Officer
Witness Type: Law Enforcement
Witness Available: Yes

b6
b7C

Other Persons

~~SECRET~~

~~SECRET//ORCON/NOFORN~~ [Redacted]

b1
b3

Targets

Vehicles

Weapons

Locations

(U) The Islamic Center of Chico
Other
1316 Nord Avenue
Chico, California 95927
United States

Leads

Attachments

(U) [Redacted]

b7E

Links

Notes

(U) GILL, Wiley

Description: Birth Date Range Begin: [Redacted]

Status: Approved

Attachments:

History: 08/08/2012 04:48 PM Imported note from [Redacted] [Redacted]

b7E

(U) Incident Additional Details

Description: The CPD officer reported that he initially met GILL in 2011 when he made an official visit to The Islamic Center of Chico where GILL was a member. He said all of the members were welcoming and appreciative of a visit from law enforcement with the exception of GILL. Additionally, GILL is described as avoiding eye contact, hesitant to interact with the officer; and at one point appeared to be eavesdropping while the officer spoke with other members at the center. The officer reported that GILL did not have a job and resided at the Mosque.

The officer described GILL as being agitated during the recent encounter, possibly because GILL is a Muslim and the officer was wearing shoes inside his residence.

Status: Approved

Attachments:

History: 08/08/2012 04:48 PM Imported note from [Redacted] [Redacted]

b7E

(U) Witness [Redacted] Police Officer additional information

Description: [Redacted]
Credible: YES

b6
b7C

Status: Approved

Attachments:

History: 08/08/2012 04:48 PM Imported note from [Redacted] [Redacted]

b7E

(U) Incident Additional Details

~~SECRET//ORCON//NOFORN~~ [Redacted]

b1
b3

Description: [Redacted] due to suspicious activity related to an identified male subject, Wiley Wayne GILL, DOB [Redacted] who was reportedly accessing a flight simulator game on YouTube with the title "Games that fly under the radar", and where he was acting suspiciously and appeared to be avoiding interaction with law enforcement. [Redacted]

b7E

Status: Approved

Attachments:

History: 08/08/2012 04:48 PM Imported note from [Redacted] [Redacted]

b7E

(U) Witness [Redacted] Detective additional information

Description: [Redacted]
Credible: YES

b6
b7C

Status: Approved

Attachments:

History: 08/08/2012 04:48 PM Imported note from [Redacted] [Redacted]

b7E

(U) Incident Additional Details

Description: On Jul 27, 2012, Central California Intelligence Center Analyst [Redacted] conducted basic database queries on Wiley Wayne GILL, who was reportedly on a YouTube video site titled something to the effect of "Games that fly under the radar." GILL is suspected of accessing a flight simulator type game.

b6
b7C

A California DMV records check returned a match to a valid Class C non-commercial California driver's license, number [Redacted] with an expiration date of February 21, 2015 and a mailing address of [Redacted] in Chico. An address of [Redacted] in Chico is listed as "Other" in the DMV record as of May 4, 2007. GILL is the registered owner of a 1973 Plymouth Valiant, 2-door hardtop, license number [Redacted]. The Islamic Center of Chico at 1316 Nord Avenue in Chico is the listed address for the vehicle.

Query searches of NCIC, Automated Firearms System, Coplink, [Redacted] Sac Known Persons Finder, Parole Leads, Supervised Release File, Wanted Persons, Missing and Unidentified Persons, Sex and Arson Registration searches returned no information on GILL.

b7E

A search of automated Criminal History Search returned no derogatory information. The subject has a CII number of [Redacted] as an applicant for a public agency.

The TLO.com CLEAR public database records for GILL lists The Islamic Center of Chico at 1316 Nord Avenue in Chico as his last known address. There are two known phone numbers listed in GILL's name, which include a cell phone, [Redacted] and a land-line phone, [Redacted].

An open source query returned no matches to GILL on social media network accounts such as Facebook and MySpace; and no matches on search engines Yahoo, Google, and Bing.

A search of the "Games that fly under the radar" on YouTube returned no exact match to that title; however, many games with similar titles were easily accessible on YouTube.

[Redacted]

b7E

Status: Approved

Attachments:

History: 08/08/2012 04:48 PM Imported note from [Redacted] [Redacted]

b7E

(U) Incident additional information

Description: Submitting Organization Details

~~SECRET//ORCON/NOFORN~~ [Redacted]

b1
b3

ORI: CAFCU0100
 Name: Sacramento CCIC
 Email: [Redacted]
 Agency Name 1: Sacramento CCIC
 City: Sacramento
 State: CA
 Country: US
 Field Office: SC

Incident Author Information
 ORI: CAFCU0100
 Email: [Redacted]
 Last Name: [Redacted]
 First Name: [Redacted]

Police Report: None
 Created Timestamp: 2012-08-02T16:46:32.166
 Modified Timestamp: 2012-08-08T16:34:43.324

Status: Approved
 Attachments:

History:
 08/08/2012 04:48 PM Imported note from [Redacted] [Redacted]

b6
b7C

b6
b7C

b7E

(U) Incident Additional Details

Description: On 8/2/2012, FBI IA [Redacted] queries on the subject [Redacted]

Status: Approved
 Attachments:

History:
 08/08/2012 04:48 PM Imported note from [Redacted] [Redacted]

b6
b7C
b7E

b7E

(U)

~~(S//NF)~~ Classified database checks

Investigative: Access/examine FBI/DOJ records, and obtain information from FBI/DOJ personnel.
 Method: [Redacted]
 Description: (U) IA [Redacted] FBI, conducted [Redacted]

(U) [Redacted]

(U) [Redacted]

(U) [Redacted]

(U) [Redacted]

(U) [Redacted]

(U) [Redacted]

No additional information was found

Status: Completed
 Attachments:

History:
 08/09/2012 01:19 PM [Redacted] [Redacted]

b6
b7C
b7E

b7D
b7E

b6
b7C
b7E

b6
b7C
b7E

(U) [Redacted]

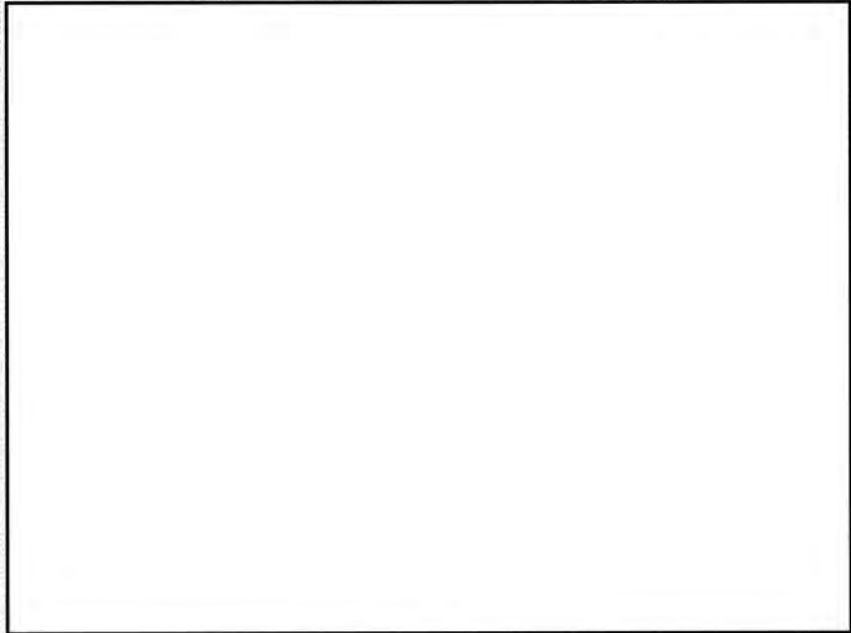
Investigative: [Redacted]
 Method: [Redacted]
 Description: [Redacted]

b6
b7C
b7E

(S)

~~SECRET//ORCON//NOFORN~~ [redacted]

b1
b3



b7E

Status: Approved

Attachments:

History:

08/20/2012 02:17 PM	Created Note	[redacted]
10/01/2012 05:06 PM	Submit note for approval	[redacted]
10/01/2012 05:18 PM	Approve note	[redacted]

b6
b7C
b7E

(U) Interview of Wiley Gill

Investigative Method: Interview or request information from members of the public and private entities.

Description: On approximately September 12, 2012, TFO's [redacted] and [redacted] attempted to interview WILEY GILL at his residence 1316 Nord Avenue, Chico, CA. This residence is co-located with and owned by the Chico Islamic Center. TFO's [redacted] and [redacted] were informed that GILL no longer lives at the residence.

b6
b7C

On October 1, 2012, TFO [redacted] contacted GILL via his cell phone, [redacted] in an attempt to set up an interview with him. GILL did not answer his phone and TFO [redacted] did not leave a message. Approximately an hour later, GILL called [redacted] phone back. TFO [redacted] informed GILL of his identity and the nature of his telephone call. GILL seemed suspicious at first but then provided the following information:

b6
b7C

GILL allowed law enforcement officers to come into his house at 1316 Nord Avenue a few months ago when he was told that they were searching the area for a fleeing suspect. This is the only time that GILL knows that law enforcement officers have been in his residence.

GILL was informed that one of the officers in his house saw something on his computer screen titled "Games that Fly Under the Radar." GILL acknowledged that this is probably what the officer saw. GILL stated that this is a YouTube video that highlights the top ten best and worst games people play.

GILL asked why the officers didn't question him then, when they believed that something appeared suspicious? TFO [redacted] agreed that this was a logical question to which he did not know the answer.

b6
b7C

(S)

~~SECRET//ORCON/NOFORN~~ [redacted]

b1
b3

GILL was cooperative throughout the telephonic interview with TFO [redacted]

Status: Approved

Attachments:

History:

10/01/2012 03:28 PM	Created Note: Attempted Interview of Wiley Gill	[redacted]
10/01/2012 05:06 PM	Submit note for approval	[redacted]
10/01/2012 05:19 PM	Approve note	[redacted]

b6
b7C

b6
b7C
b7E

(U//FOUO) [redacted] Report

Investigative Method: [redacted]

Description: A review of [redacted] report for WILEY GILL reveals the following identifiers:

b7E

Name: WILEY WAYNE GILL
 DON: [redacted]
 SSN: [redacted]
 Cell Phone: [redacted]
 Residential Phone: [redacted] (registered in Stoneyford, CA)
 Address: [redacted] Chico, CA
 Former Addresses:
 [redacted]

Status: Approved

Attachments:

History:

10/01/2012 05:04 PM	Created Note: [redacted] Report	[redacted]
10/01/2012 05:19 PM	Approve note	[redacted]

b6
b7C
b7E

(S)

(U) ~~(S//OC/N)~~ [redacted] Baseline Checks

Investigative Method: Access/examine FBI/DOJ records, and obtain information from FBI/DOJ personnel.

Description: 8. Subject's current place of employment and position. When available identifying information has been obtained, it should be used to conduct the checks necessary to answer the following questions: [redacted]

b1
b3

b7E

[redacted]

1a. [redacted]

[redacted]

b7E

2a. [redacted]

[redacted]

[redacted]

[redacted]

b6
b7C
b7E

~~SECRET//ORCON//NOFORN~~ [Redacted]

(S)

b1
b3

[Redacted]

b7E

[Redacted] NCIC query reveals that GILL was an applicant for the California State University, Chico Police Department on 12/09/2011.

b7E

(S)

[Redacted]

b7E

[Redacted]

b1
b3

[Redacted]

b7E

[Redacted]

b7E

[Redacted]

b7E

[Redacted]

b6
b7C
b7E

[Redacted]

[Redacted]

b7E

[Redacted]

b6
b7C
b7E

[Redacted] According to TFO [Redacted] GILL is a night-shift custodian at the California State University, Chico.

[Redacted]

b7E

(S)

~~SECRET//ORCON//NOFORN~~



b1
b3



b7E



b7E

Status: Approved

Attachments:

History:

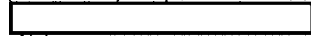
- 10/01/2012 05:10 PM Created Note: Baseline Checks
- 10/02/2012 12:14 PM Submit note for approval
- 10/03/2012 12:19 PM Approve note



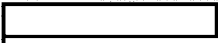
b6
b7C
b7E

Disposition

(U//FOUO) Disposition



Note:

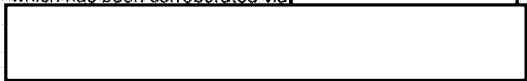


Wiley

Wayne GILL. It should be noted that in the past when GILL was interviewed he was uncooperative and claimed that he was being spied on by the NSA and other governmental agencies. A second interview was conducted with GILL [redacted]. GILL was overall cooperative with law enforcement. GILL explained that the suspicious video that law enforcement saw on his computer screen in May 2012 was about computer gaming, which has been corroborated via [redacted].

b7E

Disposition:



b7E

Workflow

08/08/2012 04:48 PM Imported Incident from [redacted]

Assigned By: [redacted]

08/09/2012 01:21 PM Incident assigned

Assigned To: [redacted]
Assigned By: [redacted]

08/09/2012 03:33 PM Incident opened

Assigned To: [redacted]
Assigned By: [redacted]

09/06/2012 03:02 PM



Assigned By: [redacted]
Assigned To: [redacted]

b6
b7C
b7E

~~SECRET~~

(S)

~~SECRET//ORCON//NOFORN~~ [Redacted]

b1
b3

10/02/2012 12:15 PM Incident submitted for closure

Assigned By:

[Redacted]

Assigned To:

b6
b7C
b7E

10/03/2012 12:20 PM Incident closed

Assigned By:

Assigned To:

SENTINEL Uploads

08/09/2012 03:35 PM SENTINEL Case File:

[Redacted]

b7E

1 BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General
2 ANTHONY J. COPPOLINO
Deputy Branch Director
3 STEVEN A. MYERS
Trial Attorney
4
5 Civil Division, Federal Programs Branch
U.S. Department of Justice
P.O. Box 883
6 Washington, D.C. 20044
Telephone: (202) 305-8648
7 Facsimile: (202) 616-8460
E-mail: steven.a.myers@usdoj.gov

8 *Attorneys for Federal Defendants*

9
10 **UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

11
12 WILEY GILL; JAMES PRIGOFF; TARIQ
13 RAZAK; KHALID IBRAHIM; and AARON
CONKLIN,

14 Plaintiffs,

15 v.

16 DEPARTMENT OF JUSTICE, *et al.*,

17 Defendants.
18

No. 3:14-cv-03120 (RS)(KAW)

**DEFENDANTS' REPLY IN SUPPORT
OF MOTION FOR SUMMARY
JUDGMENT, OPPOSITION TO
PLAINTIFFS' MOTION FOR
SUMMARY JUDGMENT, AND
OPPOSITION TO PLAINTIFFS'
MOTION TO STRIKE DEFENDANTS'
DECLARATIONS
AND TO SUPPLEMENT THE
RECORD WITH PLAINTIFFS'
DECLARATIONS**

Hearing Date: December 8, 2016
Time: 1:30 PM

19
20
21
22
23
24
25
26
27
Gill v. Dep't of Justice, No. 14-3120 (RS)
Defendants' Reply in Support of Motion for Summary Judgment, Opposition to Plaintiffs' Motion for Summary Judgment, and Opposition to Plaintiffs' Motion to Strike Defendants' Declarations and to Supplement the Record With Plaintiffs' Declarations

TABLE OF CONTENTS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

TABLE OF AUTHORITIES ii

INTRODUCTION.....1

ARGUMENT.....4

I. Defendants Were Not Required To Publish The Functional Standard In The Federal Register, And Any Failure To Do So Was Harmless Error Because Defendants Considered And Rejected The Arguments That Plaintiffs Present In This Case.....4

 A. The Functional Standard Is Not A Legislative Rule Subject To Notice-and-Comment Rulemaking5

 B. Any Failure To Comply With Notice-and-Comment Rulemaking Was Harmless Because PM-ISE Considered And Rejected The Contention That Plaintiffs Bring Here8

II. The Functional Standard Is Not Arbitrary And Capricious11

 A. Plaintiffs’ Facial Challenge Cannot Succeed Because They Cannot Show That The Functional Standard Is Invalid In All Applications.11

 B. An As-Applied Challenge Would Fail Because The Functional Standard Is Not Arbitrary And Capricious In Any Application13

 1. Suspicious Activity Reports Are Not “Criminal Intelligence Information” As Specifically Defined By 28 C.F.R. Part 23.....14

 2. The Functional Standard Does Not Govern The Sharing of ISE-SARs On Omnibus-Act Funded Systems18

III. Remand Without Vacatur Would Be The Only Appropriate Remedy21

IV. The Court Should Deny Plaintiffs’ Motion To Strike Defendants’ Declarations And Supplement The Record With Plaintiffs’ Declarations22

 A. The Court Should Not Strike Defendants’ Declarations.....22

 B. The Court Should Not Consider The Individual Plaintiffs’ Declarations.....24

CONCLUSION25

1 to notice and comment if it is otherwise expressly exempt under the APA.” *Id.* at 1016
2 (citation omitted); *see also* Pls.’ Opp. at 30 (agreeing that *Mada-Luna* states the actual test).

3 Thus, while it is true that the “final agency action” and “legislative rule” analysis
4 “largely coalesce,” *see* Defs.’ MTD Reply (ECF No. 28) at 7, the overlap is not complete.
5 As the Ninth Circuit explained in *Mada-Luna*, “[t]he determinations of whether an
6 agency’s decisions implementing a particular directive are subject to judicial review and
7 whether the directive itself constitutes a general statement of policy exempt from section
8 553’s notice-and-comment requirements are not necessarily interdependent,” as the “two
9 issues involve different statutory provisions, are analyzed under different standards, and
10 arise at different chronological stages of a directive’s history.” 813 F.2d at 1014-15;
11 *accord id.* at 1015 (“[O]ur decision . . . finding determinations made pursuant to the 1978
12 Operating Instruction reviewable, does not foreclose the possibility that the 1978
13 Instruction constitutes a general statement of policy for purposes of section 553.”).

14 Under the test established by the Ninth Circuit, Plaintiffs cannot show that the
15 Functional Standard creates a binding norm that does not leave agency officials free to
16 exercise discretion with respect to the facts of individual cases as they arise. It is not
17 relevant whether “agencies that choose to participate in the Initiative” do or do not have
18 discretion to follow “the Functional Standard’s process and criteria for designating reports
19 that have . . . a potential nexus to terrorism,” Pls.’ Opp. at 31, nor would it matter if (as
20 Plaintiffs say) the Functional Standard contains “language requiring Initiative participants
21 to comply.” *Id.* The only question is whether PM-ISE has restricted its own discretion.
22 Plaintiffs cannot show this standard is satisfied because the document is intended solely as
23 descriptive guidance for participants in the NSI.

1 The Functional Standard explicitly indicates that it is “limited to *describing* the
 2 ISE-SAR process.” A.R. 414 (emphasis added). Plaintiffs point to language indicating
 3 that “only those tips and leads that comply with the ISE-SAR Functional Standard are
 4 broadly shared with NSI participants,” A.R. 429, characterizing this language as a “built-
 5 in compliance mechanism.” Pls.’ Opp. at 31. The language provides nothing of the sort,
 6 and critically does not indicate that there is any role for PM-ISE in policing SARs for
 7 compliance with the Functional Standard. Nor, pursuant to the Intelligence Reform and
 8 Terrorism Prevention Act of 2004, is there even statutory authority for PM-ISE to play
 9 such an enforcement role. Read in context, this language is purely descriptive of how the
 10 NSI works:

11 Multiple federal agencies currently have the authority to collect terrorism-
 12 related tips and leads. However, only those tips and leads that comply with
 13 the ISE-SAR Functional Standard are broadly shared with NSI participants.
 14 At the SLTT level, crime and terrorism information, including terrorism-
 related non-ISE-SAR information, can and should be reported to
 appropriate Federal agencies based on their relevant legal authorities.

15 A.R. 429. Plaintiffs cannot identify a single respect in which the Functional Standard limits
 16 PM-ISE’s discretion to do anything, which makes sense because PM-ISE does not have a
 17 role in evaluating specific tips and leads or in determining which will or will not be shared
 18 among participating law enforcement agencies. Rather, it is the various law enforcement
 19 agencies that document, submit, and share SARs that are responsible, by virtue of their
 20 own respective agency privacy policies, for following the Functional Standard.

21 Plaintiffs’ invocation of out-of-Circuit precedent, *see Chamber of Commerce v.*
 22 *U.S. Dep’t of Labor*, 174 F.3d 206 (D.C. Cir. 1999), misses the mark largely for that reason.
 23 The agency decision challenged in that case “provide[d] that every employer that does not
 24 participate [in the program] will be searched,” and so the “effect of the rule is . . . to inform

1 of foreign policy and national security,” *Al-Haramain Islamic Found., Inc. v. Bush*, 507
2 F.3d 1190, 1203 (9th Cir. 2007), and there is no reason for the Court to do otherwise in this
3 case.

4 Finally, Plaintiffs contend that “leaving the Functional Standard in place risks
5 ongoing, serious harm to Plaintiffs and countless other individuals who engage in innocent
6 conduct but risk being swept up in Defendants’ net.” Pls.’ Opp. at 39. As Defendants have
7 explained, however, if the Functional Standard were vacated, the federal government could
8 simply operate the NSI without any information sharing guidance at all. *See* Defs.’ Mot.
9 at 34. Plaintiffs cannot explain — and notably do not try to explain — how this result
10 better serves their privacy and civil-liberty concerns.

11 **IV. The Court Should Deny Plaintiffs’ Motion To Strike Defendants’**
12 **Declarations And Supplement The Record With Plaintiffs’ Declarations.**

13 Finally, the Court should deny Plaintiffs’ motion to strike Defendants’ declarations
14 and also deny their request to supplement the record with the individual Plaintiffs’
15 declarations. (Defendant has no opposition to the Court’s consideration of the Lye
16 Declaration submitted by Plaintiffs, though it has no bearing on any of the issues before
17 the Court for the reasons explained above.)

18 **A. The Court Should Not Strike Defendants’ Declarations.**

19 Defendants submitted two declarations alongside their motion for summary
20 judgment: one from Basil N. Harris (ECF No. 113-1), which addresses the collaborative
21 process used by PM-ISE in promulgating the Functional Standard, and one from Marilyn
22 B. Atsatt (ECF No. 113-2), which explains that the NSI SAR Data Repository does not
23 receive any funding under the Omnibus Act. Plaintiffs’ motion to strike both declarations
24 should be denied.

1 MORGAN, LEWIS & BOCKIUS LLP
 2 Stephen Scotch-Marmo (admitted *pro hac vice*)
 3 stephen.scotch-marmo@morganlewis.com
 4 Michael James Ableson (admitted *pro hac vice*)
 5 michael.ableson@morganlewis.com
 101 Park Avenue
 New York, NY 10178
 Telephone: (212) 309-6000; Facsimile: (212) 309-6001

6 AMERICAN CIVIL LIBERTIES UNION
 FOUNDATION OF NORTHERN CALIFORNIA
 Linda Lye (SBN 215584), llye@aclunc.org
 7 Julia Harumi Mass (SBN 189649), jmass@aclunc.org
 39 Drumm Street
 8 San Francisco, CA 94111
 Telephone: (415) 621-2493; Facsimile: (415) 255-8437

9 ASIAN AMERICANS ADVANCING
 10 JUSTICE - ASIAN LAW CAUCUS
 Christina Sinha (SBN 278893), christinas@advancingjustic-alc.org
 11 55 Columbus Avenue
 San Francisco, CA 94111
 12 Telephone: (415) 848-7711; Facsimile: (415) 896-1702

13 *Attorneys for Plaintiffs*
 14 Additional counsel listed on signature page

15 UNITED STATES DISTRICT COURT
 NORTHERN DISTRICT OF CALIFORNIA
 16 SAN FRANCISCO DIVISION

17 WILEY GILL; JAMES PRIGOFF; TARIQ
 18 RAZAK; KHALID IBRAHIM; and AARON
 19 CONKLIN,

20 Plaintiffs,

21 v.

22 DEPARTMENT OF JUSTICE; LORETTA
 LYNCH, in her official capacity as the
 Attorney General of the United States;
 23 PROGRAM MANAGER – INFORMATION
 SHARING ENVIRONMENT;
 24 KSHEMENDRA PAUL, in his official
 capacity as the Program Manager of the
 25 Information Sharing Environment,

26 Defendants.

Case No. 3:14-cv-03120-RS-KAW

**PLAINTIFFS’ MOTION TO STRIKE
 DEFENDANTS’ DECLARATIONS
 AND TO SUPPLEMENT THE
 RECORD WITH PLAINTIFFS’
 DECLARATIONS; MEMORANDUM
 OF POINTS AND AUTHORITIES IN
 SUPPORT**

Hearing Date: December 8, 2016
 Time: 1:30 p.m.
 Judge: Hon. Richard Seeborg
 Courtroom: 3, 17th Floor
 Date Of Filing: July 10, 2014
 Trial Date: None Set

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF SAN DIEGO AND
IMPERIAL COUNTIES
David Loy (SBN 229235)
dloy@aclusandiego.org
Mitra Ebadolahi (SBN 275157)
mebadolahi@aclusandiego.org
P.O. Box 87131
San Diego, CA 92138
Telephone: (619) 232-2121
Facsimile: (619) 232-0036

AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF SOUTHERN
CALIFORNIA
Peter Bibring (SBN 223981)
pbibring@aclusocal.org
1313 West 8th Street
Los Angeles, CA 90017
Telephone: (213) 977-9500
Facsimile: (213) 977-5299

Attorneys for Plaintiffs
Additional counsel listed on caption page

TABLE OF CONTENTS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Page

I. INTRODUCTION 1

II. LEGAL STANDARD 1

III. ARGUMENT 2

 A. The Court Should Strike Defendants’ Declarations Because They Seek to Introduce Facts Outside the Administrative Record 2

 B. The Court Should Supplement the Record with the Gill, Razak, Ibrahim, Conklin and Prigoff Declarations Regarding Standing 4

 C. The Court Should Supplement the Record with Information in the Lye Declaration About Funding 4

IV. CONCLUSION 6

TABLE OF AUTHORITIES

1				Page(s)
2				
3	CASES			
4	<i>Burlington Truck Lines, Inc. v. United States,</i>			
5	371 U.S. 156 (1962).....			4
6	<i>Envtl. Def. Fund, Inc. v. Blum,</i>			
7	458 F. Supp. 650 (D.D.C. 1978).....			3
8	<i>Fence Creek Cattle Co. v. U.S. Forest Serv.,</i>			
9	602 F.3d 1125 (9th Cir. 2010).....			2
10	<i>McCrary v. Gutierrez,</i>			
11	495 F. Supp. 2d 1038 (N.D. Cal. 2007).....			1, 2, 4
12	<i>Motor Vehicle Mfrs. Ass’n v. State Farm Mut. Auto. Ins. Co.,</i>			
13	463 U.S. 29 (1983).....			4
14	<i>Nw. Env’tl. Def. Ctr. v. Bonneville Power Admin.,</i>			
15	117 F.3d 1520 (9th Cir. 1997).....			2, 4
16	<i>Sw. Ctr. for Biological Diversity v. U.S. Forest Serv.,</i>			
17	100 F.3d 1443 (9th Cir. 1996).....			2, 5
18	<i>Thompson v. U.S. Dep’t of Labor,</i>			
19	885 F.2d 551 (9th Cir. 1989).....			1
20	STATUTES			
21	5 U.S.C. § 706.....			1, 4
22	OTHER AUTHORITIES			
23	28 C.F.R. Part 23.....			3, 5

1 **I. INTRODUCTION**

2 Plaintiffs move to strike the declarations of Marilyn Atsatt and Basil Harris submitted by
3 Defendants, and to supplement the Administrative Record with the declarations of Wiley Gill,
4 Tariq Razak, Khaled Ibrahim, Aaron Conklin, James Prigoff, and Linda Lye, submitted by
5 Plaintiffs. This action is a challenge under the Administrative Procedure Act (“APA”) to the
6 Functional Standard, which establishes a nationwide process for collecting, evaluating, and
7 disseminating information about activity that Defendants deem to have a potential nexus to
8 terrorism. In APA actions, the scope of judicial review is limited to the Administrative Record
9 certified by the agency, subject to certain exceptions.

10 Defendants seek to introduce evidence through two extra-record declarations, but have not
11 moved to supplement the Record or otherwise offered any reason why this Court should consider
12 the information in their declarations. The declarations should therefore be stricken.

13 The Court should supplement the Record, however, with the declarations of the Plaintiffs
14 in this action, Gill, Razak, Ibrahim, Conklin, and Prigoff, which provide factual information
15 related to their standing. Courts may consider extra-record evidence to establish standing.

16 The Court should also supplement the Record with the declaration of Linda Lye, which
17 provides information related to the funding used by systems on which suspicious activity reports
18 are stored and exchanged. This information falls within exceptions to the general rule limiting
19 APA review to the Record.

20 **II. LEGAL STANDARD**

21 The Administrative Procedure Act limits the scope of judicial review to the administrative
22 record. *See* 5 U.S.C. § 706; *Thompson v. U.S. Dep’t of Labor*, 885 F.2d 551, 555 (9th Cir. 1989);
23 *McCrary v. Gutierrez*, 495 F. Supp. 2d 1038, 1044 (N.D. Cal. 2007) (denying motion to add
24 documents to record). An agency’s designation and certification of an administrative record is
25 entitled to a “presumption of administrative regularity.” *McCrary*, 495 F. Supp. 2d at 1041.
26 Courts presume that the agency properly designated the record absent “clear evidence to the
27 contrary.” *Id.* To rebut the presumption of regularity, the party seeking to supplement the record
28

1 bears a “heavy burden.” *Fence Creek Cattle Co. v. U.S. Forest Serv.*, 602 F.3d 1125, 1131 (9th
2 Cir. 2010).

3 The Ninth Circuit has recognized several exceptions, however, to the record-review rule.
4 First, consideration of extra-record declarations is plainly proper to address jurisdictional issues
5 such as standing. *See, e.g., Nw. Envtl. Def. Ctr. v. Bonneville Power Admin.*, 117 F.3d 1520,
6 1528 (9th Cir. 1997). Second, courts may supplement the record “if necessary to determine
7 whether the agency has considered all relevant factors and has explained its decision” or “to
8 explain technical terms or complex subject matter.” *Sw. Ctr. for Biological Diversity v. U.S.*
9 *Forest Serv.*, 100 F.3d 1443, 1450 (9th Cir. 1996) (citation and internal quotation marks omitted).

10 **III. ARGUMENT**

11 **A. The Court Should Strike Defendants’ Declarations Because They Seek to** 12 **Introduce Facts Outside the Administrative Record.**

13 In support of their motion for summary judgment, Defendants have filed two extra-record
14 declarations. The Declaration of Marilyn Atsatt, an official in the Department of Justice’s Office
15 of Justice Programs, states that her office did not provide “funding to the Federal Bureau of
16 Investigation (FBI) for eGuardian or the NSI SAR Data Repository.” *See* Dkt. No. 113-2 ¶ 3.
17 The Declaration of Basil Harris, the Chief of Staff to Defendant Office of the Program Manager
18 for the Information Sharing Environment, describes the process undertaken by that office in
19 developing the Functional Standard. *See* Dkt. No. 113-1. But Defendants have not moved to
20 supplement the record with these declarations, nor provided any reasons why this Court should
21 depart from the default rule in APA cases that limits the court’s review to “the administrative
22 record that the agency compiles and submits to the court.” *McCrary*, 495 F. Supp. 2d at 1041.
23 The declarations should therefore be stricken.

24 It bears emphasis that throughout this proceeding, Defendants have asserted vigorously
25 that this matter should be decided solely on the basis of the Administrative Record they certified,
26 and they fought aggressively any efforts to expand the Record. Defendants repeatedly invoked
27 the record-review rule in objecting to Plaintiffs’ efforts to take discovery. *See, e.g., Case*
28 *Management Statements* (Dkt. No. 36 at 6-9; Dkt. No. 40 at 5-6). After Defendants certified the

1 Administrative Record, (*see* Dkt. No. 52-1), Plaintiffs identified numerous gaps in the Record.
2 After meet and confer efforts proved unfruitful, Plaintiffs were forced to litigate the adequacy of
3 the Record. *See* Pltfs.’ Mot. to Complete Administrative Record (Dkt. No. 73). Although
4 Plaintiffs largely prevailed before the Magistrate Judge, Defendants continued to fight any effort
5 to expand the Record and sought relief before this Court from the Magistrate Judge’s order. *See*
6 Magistrate Judge Order (Dkt. No. 88); Defs.’ Mot. for Relief from Nondispositive Pretrial Order
7 of Magistrate Judge (Dkt. No. 94). Only after this Court sustained portions of the Magistrate
8 Judge’s order requiring Defendants to revisit their compilation of the Administrative Record did
9 they file a Supplemental Administrative Record. *See* Order Re Defs.’ Mot. for Relief (Dkt. No.
10 102); Am. Certification of Administrative Record and Suppl. Administrative Record (Dkt. No.
11 107-1).

12 Allowing Defendants to supplement the Record—a Record they twice certified as
13 complete (Dkt. Nos. 52-1, 107-1)—with declarations of individuals whom Plaintiffs have had no
14 opportunity to depose would violate the APA’s record-review rule and sanction gamesmanship by
15 allowing the agency to “skew the ‘record’ for review in its favor.” *Envtl. Def. Fund, Inc. v. Blum*,
16 458 F. Supp. 650, 661 (D.D.C. 1978).

17 Moreover, the Atsatt declaration seeks to introduce information about the funding
18 received by information systems used to exchange suspicious activity reports—a factual issue that
19 is not relevant to the legal question before this Court.

20 Plaintiffs in this APA action contend that the Functional Standard is arbitrary and
21 capricious because, among other things, it creates a standard for reporting suspicious activity that
22 conflicts with a duly promulgated regulation, 28 C.F.R. Part 23, which prohibits the collection of
23 criminal intelligence, absent reasonable suspicion of criminal activity. Defendants’ defense of the
24 Functional Standard in this litigation rests heavily on the argument that information systems used
25 to exchange suspicious activity reports do not receive the funding from the Office of Justice
26 Programs that would trigger the applicability of 28 C.F.R. Part 23. *See* Defs.’ Br. at 23-25, 27.
27 But Defendants nowhere articulated funding issues in the Administrative Record as the basis for
28 their decision to reject 28 C.F.R. Part 23’s reasonable suspicion requirement. *See* AR 413. “It is

1 well-established that an agency’s action must be upheld, if at all, on the basis articulated by the
2 agency itself.” *Motor Vehicle Mfrs. Ass’n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 50
3 (1983).

4 Indeed, the fact that Defendants now rely on an extra-record declaration to support their
5 funding argument underscores the *post-hoc* nature of their arguments. If the funding received by
6 information systems used to exchange suspicious activity reports had played a role in Defendants’
7 decision to reject the regulation, the Record would contain factual information on this issue.
8 Defendants must defend the Functional Standard on the basis of the rationale and facts contained
9 in the Administrative Record. *See Burlington Truck Lines, Inc. v. United States*, 371 U.S. 156,
10 168 (1962) (“[C]ourts may not accept...counsel’s post hoc rationalizations for agency action.”).
11 This Court should not permit Defendants to support their impermissible *post-hoc* rationalization
12 through extra-record evidence. As this Court has explained, “[i]n reviewing an agency decision,
13 the reviewing court is to apply the appropriate APA standard of review, 5 U.S.C. § 706, based on
14 the administrative record that the agency compiles and submits to the court.” *McCrary*, 495 F.
15 Supp. 2d at 1041. For this additional reason, the *Atsatt* declaration should be stricken.

16 **B. The Court Should Supplement the Record with the Gill, Razak, Ibrahim,
17 Conklin and Prigoff Declarations Regarding Standing.**

18 Plaintiffs are filing a declaration from each of the Plaintiffs in this action. The
19 declarations explain Plaintiffs’ individual experiences and provide the factual basis for their
20 standing to bring this suit. *See Nw. Env’tl. Def. Ctr.*, 117 F.3d at 1528 (considering extra-record
21 affidavits submitted to establish standing). Defendants have acknowledged that “evidence
22 outside of the administrative record can be considered on the question of standing.” *See, e.g.*,
23 Joint Case Management Statement (Dkt. No. 36) at 6:23-24. The Court should therefore
24 supplement the Record with Plaintiffs’ declarations.

25 **C. The Court Should Supplement the Record with Information in the Lye
26 Declaration About Funding.**

27 Plaintiffs are also filing a declaration from Linda Lye, counsel in this matter, to
28 authenticate various government documents and correspondence with government agencies that

1 provide information about (1) the funding received by a fusion center in Northern California to
 2 store suspicious activity reports (*see* Lye Decl. ¶¶ 2-7 & Exhs. 1-4) and (2) the funding received
 3 by the Regional Information Sharing System (*see id.* ¶¶ 8-9 & Exhs. 5-6), which, according to the
 4 Record, is used as a “connection and transport mechanism[] for sharing [suspicious activity
 5 reports].” Supp. AR at 254.

6 Plaintiffs contend that the funding used to support suspicious activity report information
 7 systems is not relevant to the question of whether the Functional Standard is arbitrary and
 8 capricious. This is so because Defendants never articulated funding as their rationale for rejecting
 9 28 C.F.R. Part 23 and its reasonable suspicion requirement. For this reason, the Atsatt declaration
 10 submitted by Defendants should be stricken.

11 But if the Court deems the funding issue relevant, then it should supplement the Record
 12 with the funding information in the Lye declaration. The Ninth Circuit allows a court to consider
 13 extra-record materials “if necessary to determine ‘whether the agency has considered all relevant
 14 factors and has explained its decision.’” *Sw. Ctr. for Biological Diversity*, 100 F.3d at 1450
 15 (citation omitted).

16 Even if the Court does not deem funding relevant, however, it should also supplement the
 17 Record with information in the Lye declaration pertaining to the funding received by the Regional
 18 Information Sharing System (¶¶ 8-9 & Exhs. 5-6). As discussed above, the Record states “the
 19 DOJ-supported Regional Information Sharing Systems® Secure Intranet (RISSNET™)” is one of
 20 several systems used “as the connection and transport mechanisms for sharing SARs.” Supp. AR
 21 at 254. The Record does not explain the technical term “Regional Information Sharing
 22 Systems®.” The Court should therefore supplement the Record with the portion of the Lye
 23 declaration that sheds light on this term (Lye Decl. at ¶¶ 8-9 & Exhs. 5-6) for the separate and
 24 independent reason that it assists the Court by “explain[ing] technical terms or complex subject
 25 matter.” *Sw. Ctr. for Biological Diversity*, 100 F.3d at 1450.

26
 27
 28

1 **IV. CONCLUSION**

2 For the foregoing reasons, the Court should strike the Atsatt and Harris declarations
3 submitted by Defendants, and supplement the Record with the Gill, Razak, Ibrahim, Conklin,
4 Prigoff, and Lye declarations submitted by Plaintiffs.

5
6 Dated: September 22, 2016

By: _____ /s/ Linda Lye

7
8 MORGAN, LEWIS & BOCKIUS LLP
Jeffrey S. Raskin (SBN 169096)
jeffrey.raskin@morganlewis.com
9 Phillip J. Wiese (SBN 291842)
phillip.wiese@morganlewis.com
10 Ellie F. Chapman (SBN 305473)
ellie.chapman@morganlewis.com
11 One Market, Spear Street Tower
San Francisco, CA
12 Telephone: (415) 442-1000
Facsimile: (415) 442-1001

13
14 AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
Hina Shamsi (admitted *pro hac vice*)
15 hshamsi@aclu.org
Hugh Handeyside (admitted *pro hac vice*)
16 hhandeyside@aclu.org
125 Broad Street
17 New York, NY 10004
Telephone: (212) 549-2500
18 Facsimile: (212) 549-2654

19
20 AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF SAN DIEGO AND
IMPERIAL COUNTIES
21 David Loy (SBN 229235)
dloy@aclusandiego.org
22 Mitra Ebadolahi (SBN 275157)
mebadolahi@aclusandiego.org
23 P.O. Box 87131
San Diego, CA 92138
24 Telephone: (619) 232-2121
Facsimile: (619) 232-0036

25 *(continued on next page)*

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF SOUTHERN
CALIFORNIA

Peter Bibring (SBN 223981)
pbibring@aclusocal.org
1313 West 8th Street
Los Angeles, CA 90017
Telephone: (213) 977-9500
Facsimile: (213) 977-5299

Attorneys for Plaintiffs

Additional counsel listed on caption page

7

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

FILER'S ATTESTATION

I, Phillip J. Wiese, am the ECF user whose identification and password are being used to file this PLAINTIFFS' MOTION TO STRIKE DEFENDANTS' DECLARATIONS AND TO SUPPLEMENT THE RECORD WITH PLAINTIFFS' DECLARATIONS. Pursuant to L.R. 5-1(i)(3), I hereby attest that concurrence in the electronic filing of this document has been obtained from each of the other signatories.

Dated: September 22, 2016

By /s/ Phillip J. Wiese
Phillip J. Wiese

1 MORGAN, LEWIS & BOCKIUS LLP
 2 Stephen Scotch-Marmo (admitted *pro hac vice*)
 3 stephen.scotch-marmo@morganlewis.com
 4 Michael James Ableson (admitted *pro hac vice*)
 5 michael.ableson@morganlewis.com
 101 Park Avenue
 New York, NY 10178
 Telephone: (212) 309-6000; Facsimile: (212) 309-6001

6 AMERICAN CIVIL LIBERTIES UNION
 FOUNDATION OF NORTHERN CALIFORNIA
 7 Linda Lye (SBN 215584), llye@aclunc.org
 8 Julia Harumi Mass (SBN 189649), jmass@aclunc.org
 39 Drumm Street
 San Francisco, CA 94111
 Telephone: (415) 621-2493; Facsimile: (415) 255-8437

10 ASIAN AMERICANS ADVANCING
 JUSTICE - ASIAN LAW CAUCUS
 11 Christina Sinha (SBN 278893)
 christinas@advancingjustice-alc.org
 55 Columbus Avenue
 12 San Francisco, CA 94111
 Telephone: (415) 848-7711; Facsimile: (415) 896-1702

Attorneys for Plaintiffs

Additional counsel listed on signature page of Plaintiffs' Motions

15 UNITED STATES DISTRICT COURT
 16 NORTHERN DISTRICT OF CALIFORNIA
 SAN FRANCISCO DIVISION

18 WILEY GILL; JAMES PRIGOFF; TARIQ
 RAZAK; KHALID IBRAHIM; and AARON
 19 CONKLIN,

Plaintiffs,

v.

21 DEPARTMENT OF JUSTICE; LORETTA
 22 LYNCH, in her official capacity as the
 Attorney General of the United States;
 23 PROGRAM MANAGER – INFORMATION
 SHARING ENVIRONMENT;
 24 KSHEMENDRA PAUL, in his official
 capacity as the Program Manager of the
 25 Information Sharing Environment,

Defendants.

Case No. 3:14-cv-03120-RS-KAW

**[PROPOSED] ORDER DENYING
 DEFENDANTS' MOTION FOR
 SUMMARY JUDGMENT, GRANTING
 PLAINTIFFS' MOTIONS TO STRIKE
 AND SUPPLEMENT, AND
 GRANTING PLAINTIFFS' MOTION
 FOR SUMMARY JUDGMENT**

Judge: Hon. Richard Seeborg

[PROPOSED] ORDER ON
 DEFENDANTS' MOTION FOR
 SUMMARY JUDGMENT AND
 PLAINTIFFS' MOTIONS TO STRIKE
 AND FOR SUMMARY JUDGMENT

3:14-cv-03120-RS-KAW

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[PROPOSED] ORDER

This matter comes before the Court on Defendant’s Motion for Summary Judgment, Plaintiffs’ Cross-Motion for Partial Summary Judgment, and Plaintiffs’ Motion to Strike Defendants’ Declarations and to Supplement the Record with Plaintiffs’ Declarations. Upon consideration of the argument and evidence submitted by the parties, it is hereby ORDERED that:

Defendants’ motion for summary judgment is DENIED.

Plaintiffs’ motion to strike the Declarations of Basil Harris and Marilyn Atsatt, submitted by Defendants, is GRANTED.

Plaintiffs’ motion to supplement the Administrative Record with the Declarations of Wiley Gill, Tariq Razak, Khaled Ibrahim, Aaron Conklin, James Prigoff, and Linda Lye, is GRANTED.

Plaintiffs motion for summary judgment is GRANTED. The Functional Standard’s definition of suspicious activity, including the behavioral criteria underlying that definition, is arbitrary and capricious. The Functional Standard is also a legislative rule that should have been issued pursuant to the public notice and comment procedures of the Administrative Procedure Act. For these reasons, the Functional Standard is unlawful and hereby set aside.

IT IS SO ORDERED.

Date: _____

Judge Richard Seeborg

1 MORGAN, LEWIS & BOCKIUS LLP
 2 Stephen Scotch-Marmo (admitted *pro hac vice*)
 3 stephen.scotch-marmo@morganlewis.com
 4 Michael James Ableson (admitted *pro hac vice*)
 5 michael.ableson@morganlewis.com
 6 101 Park Avenue
 7 New York, NY 10178
 8 Telephone: (212) 309-6000; Facsimile: (212) 309-6001

9 AMERICAN CIVIL LIBERTIES UNION
 10 FOUNDATION OF NORTHERN CALIFORNIA
 11 Linda Lye (SBN 215584), llye@aclunc.org
 12 Julia Harumi Mass (SBN 189649), jmass@aclunc.org
 13 39 Drumm Street
 14 San Francisco, CA 94111
 15 Telephone: (415) 621-2493; Facsimile: (415) 255-8437

16 ASIAN AMERICANS ADVANCING
 17 JUSTICE - ASIAN LAW CAUCUS
 18 Christina Sinha (SBN 278893), christinas@advancingjustice-alc.org
 19 55 Columbus Avenue
 20 San Francisco, CA 94111
 21 Telephone: (415) 848-7711; Facsimile: (415) 896-1702

22 *Attorneys for Plaintiffs*

23 UNITED STATES DISTRICT COURT
 24 NORTHERN DISTRICT OF CALIFORNIA
 25 SAN FRANCISCO DIVISION

26 WILEY GILL; JAMES PRIGOFF; TARIQ
 27 RAZAK; KHALID IBRAHIM; and AARON
 28 CONKLIN,

Plaintiffs,

v.

DEPARTMENT OF JUSTICE; LORETTA
 LYNCH, in her official capacity as the
 Attorney General of the United States;
 PROGRAM MANAGER – INFORMATION
 SHARING ENVIRONMENT;
 KSHEMENDRA PAUL, in his official
 capacity as the Program Manager of the
 Information Sharing Environment,

Defendants.

Case No. 3:14-cv-03120-RS-KAW

**DECLARATION OF AARON
 CONKLIN IN SUPPORT OF
 PLAINTIFFS’ MOTION FOR
 SUMMARY JUDGMENT AND
 PLAINTIFFS’ OPPOSITION TO
 DEFENDANTS’ MOTION FOR
 SUMMARY JUDGMENT**

Hearing Date: December 8, 2016
 Time: 1:30 pm
 Judge: Hon. Richard Seeborg
 Courtroom: 3, 17th Floor
 Date of Filing: July 10, 2014
 Trial Date: None Set

1 I, Aaron Conklin, declare as follows:

2 1. I am one of the Plaintiffs in the above-titled action. I submit this declaration in
3 support of Plaintiffs’ Motion for Summary Judgment and Plaintiffs’ Opposition to Defendants’
4 Motion for Summary Judgment. I have personal knowledge of each fact stated in this
5 declaration and, if called as a witness, I could and would competently and truthfully testify
6 hereto.

7 2. I reside in Vallejo, California. I am student at Diablo Valley College, studying
8 graphic design. I am also an amateur photographer, and maintain a website where I post a
9 selection of my works. I have a particular interest in photographing industrial architecture.

10 3. In either 2011 or 2012, I traveled to Benicia, California, for the purpose of
11 photographing the Valero oil refinery located there. For aesthetic reasons, I decided to visit
12 Benicia in the evening, so as to capture images of the refinery illuminated against the night sky.

13 4. I arrived at approximately 10:00pm, and set up my camera in an empty lot outside
14 the refinery’s fenced perimeter. This empty lot was close to a publicly accessible sidewalk and a
15 bus stop. I knew that this lot was accessible to the general public, because during the day a taco
16 truck used to park there and sell food.

17 5. Shortly after I began taking photos, a private security guard approached from the
18 refinery, and informed me that I was not allowed to be there. He told me that I should leave, and
19 warned me that “bad things” would happen if I did not comply. I believe that the lot I was
20 standing in was a public space, and that I was within my rights to take photos from there.
21 However, because I felt threatened and was fearful of what would happen to me if I remained, I
22 stopped taking photos and left the location.

23 6. I would like to return to Benicia and take more photos of the Valero refinery to
24 add to my portfolio, but I am afraid to do so. I fear that I would be subjected to further
25 harassment. I have since discovered that photographs of the Valero refinery, taken from roughly
26 the same location as where I was standing, are publicly available online via Google Maps.

27 7. On or around November 30, 2013, I again attempted to take photos of an oil
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

refinery. This time, I traveled to the Shell refinery in Martinez, California. I arrived in Martinez at approximately 9:30pm or 10:00 pm, and began setting up my camera in the parking lot of a strip mall across the street from the refinery’s fenced perimeter.

8. A few minutes after I arrived, and before I had the opportunity to take any photos, a private security guard left the fenced perimeter of the refinery and approached me. He informed me that I could not take photos of the refinery, and asked me to show him some form of identification. I complied with the security guard’s instructions.

9. A few minutes later, another private security guard arrived. The guards told me that it was a bad idea for me to be taking photos of an oil refinery, and claimed that this was illegal. They also implied that my actions might somehow be connected to terrorism. They made repeated references to the September 11th terrorist attacks, and said that what I was doing was “endangering our country.”

10. Despite the fact that I had complied with all of the guards’ requests, they called the Contra Costa County Sheriff’s Office. Shortly thereafter, at least two Sheriff’s deputies arrived on the scene. By this point, approximately twenty minutes had passed since the beginning of the encounter, and there were between five and six people present. I cannot recall exactly how many of those individuals were private security guards, but I do recall that at least two Sheriff’s deputies were present.

11. The deputies asked me for personal information, such as my name and address, which I provided. They wrote this information down, and then took my camera from me and looked through the photographs stored on it. They then searched my vehicle. After searching my vehicle they took photos of me, my camera equipment, and my vehicle. At no point during this encounter did I feel that I was free to leave or that I could prevent them from searching my camera and vehicle.

12. Approximately forty-five minutes to an hour after the encounter began, the Sheriff’s deputies told me that I was free to go, but that I was going to be placed on an “NSA watch list.” From context, I believe the deputy who used the term “NSA watch list” was saying

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

he was going to submit a Suspicious Activity Report about me.

13. The concern that a Suspicious Activity Report has been created about me, which may include my name and other identifying information, has caused me a great deal of anxiety and distress. Both that concern and the experiences described above have discouraged me from continuing to pursue my interest in photography. Although I have a passion for taking photos of industrial sites, I am worried that my presence on a Suspicious Activity Report would place me at greater risk of being detained, searched, investigated, or even arrested. I am also concerned that if I continue to pursue my interest in photography, I will be detained and searched again, as has happened to me twice before.

14. I believe that the defendants in this case would have benefited from input from the public on the standard for suspicious activity reporting. I would have wanted the defendants to know when they adopted their standard for suspicious activity reporting that a standard that does not require reasonable suspicion of criminal activity harms innocent people, like me, who have not engaged in any wrongdoing: It makes us the targets of law enforcement scrutiny, puts our information in government databases, and adversely affects our reputations by identifying us as individuals who have engaged in conduct with a potential nexus to terrorism. I would also have wanted defendants to know the specific facts of my case so that they could understand the factual basis for my concerns. I was not aware that defendants sought input on the standard for suspicious activity reporting. As a result, I did not have an opportunity to share my perspective or the factual basis for my concerns.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct. Executed this 9 day of September, 2016 in Vallejo, California.

By: 
Aaron Conklin

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

FILER’S ATTESTATION

I, Phillip J. Wiese, am the ECF user whose identification and password are being used to file this DECLARATION OF AARON CONKLIN IN SUPPORT OF PLAINTIFFS’ MOTION FOR SUMMARY JUDGMENT AND PLAINTIFFS’ OPPOSITION TO DEFENDANTS’ MOTION FOR SUMMARY JUDGMENT. Pursuant to L.R. 5-1(i)(3), I hereby attest that concurrence in the electronic filing of this document has been obtained from each of the other signatories.

Dated: September 22, 2016 By /s/ Phillip J. Wiese
Phillip J. Wiese

1 MORGAN, LEWIS & BOCKIUS LLP
 2 Stephen Scotch-Marmo (admitted *pro hac vice*)
 3 stephen.scotch-marmo@morganlewis.com
 4 Michael James Ableson (admitted *pro hac vice*)
 5 michael.ableson@morganlewis.com
 6 101 Park Avenue
 7 New York, NY 10178
 8 Telephone: (212) 309-6000; Facsimile: (212) 309-6001

9 AMERICAN CIVIL LIBERTIES UNION
 10 FOUNDATION OF NORTHERN CALIFORNIA
 11 Linda Lye (SBN 215584), llye@aclunc.org
 12 Julia Harumi Mass (SBN 189649), jmass@aclunc.org
 13 39 Drumm Street
 14 San Francisco, CA 94111
 15 Telephone: (415) 621-2493; Facsimile: (415) 255-8437

16 ASIAN AMERICANS ADVANCING
 17 JUSTICE - ASIAN LAW CAUCUS
 18 Christina Sinha (SBN 278893), christinas@advancingjustice-alc.org
 19 55 Columbus Avenue
 20 San Francisco, CA 94111
 21 Telephone: (415) 848-7711; Facsimile: (415) 896-1702

22 *Attorneys for Plaintiffs*

23 UNITED STATES DISTRICT COURT
 24 NORTHERN DISTRICT OF CALIFORNIA
 25 SAN FRANCISCO DIVISION

26 WILEY GILL; JAMES PRIGOFF; TARIQ
 27 RAZAK; KHALID IBRAHIM; and AARON
 28 CONKLIN,

Plaintiffs,

v.

DEPARTMENT OF JUSTICE; LORETTA
 LYNCH, in her official capacity as the
 Attorney General of the United States;
 PROGRAM MANAGER – INFORMATION
 SHARING ENVIRONMENT;
 KSHEMENDRA PAUL, in his official
 capacity as the Program Manager of the
 Information Sharing Environment,

Defendants.

Case No. 3:14-cv-03120-RS-KAW

**DECLARATION OF KHALED
 IBRAHIM IN SUPPORT OF
 PLAINTIFFS’ MOTION FOR
 SUMMARY JUDGMENT**

Hearing Date: December 8, 2016
 Time: 1:30 pm
 Judge: Hon. Richard Seeborg
 Courtroom: 3, 17th Floor
 Date of Filing: July 10, 2014
 Trial Date: None Set

DECLARATION OF KHALED IBRAHIM
 ISO PLTF’S MOT. FOR SUMMARY
 JUDGMENT

3:14-CV-03120-RS-KAW

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

I, Khaled Ibrahim, declare as follows:

1. I am one of the Plaintiffs in the above-titled action. I submit this declaration in support of Plaintiffs’ Motion for Summary Judgment and Plaintiffs’ Opposition to Defendants’ Motion for Summary Judgment. I have personal knowledge of each fact stated in this declaration and, if called as a witness, I could and would competently and truthfully testify hereto.

2. I am a U.S. citizen of Egyptian descent. I reside in San Jose, California.

3. On and off from 2009 to 2015, I worked in the accounting and purchasing departments for Nordix Computer Corporation (“Nordix”), a computer network consulting and service company located in Santa Clara, California.

4. I worked in the accounting department from 2013 to 2015. Before that, I worked for two-and-a-half years as a purchasing agent for Nordix, from 2009 to 2012. As part of my job as purchasing agent, I bought computers in bulk from retail stores in the San Francisco Bay Area such as Best Buy, Circuit City, and Micro Center. Nordix would then resell the computers in the Middle East for a profit. In my role as purchasing agent, I estimate that I purchased between 2,000 and 3,000 laptops for Nordix.

5. I was particularly successful buying computers from Best Buy stores. I built connections over time with Best Buy employees and managers who would help me locate particular stores with excess stock of computers. I would then travel to those individual stores and buy the computers in bulk. When successful, I was able to purchase between 40 and 80 computers at a time.

6. I had particular success purchasing computers from the Best Buy store in Dublin, California, until late-2010, when I had a dispute with the manager regarding some computers I purchased that were not delivered. Out of frustration with the manager, I did not attempt to purchase computers at that Best Buy for several months.

7. In February 2011, I returned to the Dublin, California Best Buy store to purchase more laptops. That store was my best store, where I had the most luck purchasing computers. Because of new policies concerning bulk purchases, I had to purchase fewer laptops each visit,

DECLARATION OF KHALED IBRAHIM
ISO PLTF’S MOT. FOR SUMMARY
JUDGMENT
3:14-CV-03120-RS-KAW

1 but I still had some success. There were a few times, however, when I was turned away. On one
 2 occasion, I was told that management does not allow such bulk purchases, and I was unable to
 3 purchase any computers that day. On another occasion, in early November, which was one of the
 4 last times I tried to purchase computers from the Dublin, California Best Buy, an employee asked
 5 what I planned to do with the computers. I explained that the company I work for resells
 6 computers in the Middle East. The employee asked if I was Middle Eastern and I told him I was
 7 Egyptian. I was unable to purchase any computers that day, too. I do not know if there was a
 8 correlation between my race and my inability to purchase computers.

9 8. Through my attorneys I learned that the government created a Suspicious Activity
 10 Report (“SAR”) of my attempts to purchase computers from the Dublin, California Best Buy
 11 store. Through my attorneys, I submitted a request for records under the California Public
 12 Records Act and received a copy of the SAR in response. A true and correct copy of that SAR is
 13 attached as Exhibit 1. It is entitled “Suspicious attempt to purchase large number of computers,”
 14 and relates to attempted purchases I made the week of November 6, 2011. It is my understanding
 15 based on reviewing Defendants’ Answer in this matter, that two incident reports containing
 16 information in the Suspicious Activity Report about me were uploaded to the eGuardian system,
 17 which I understand to be a national database to which thousands of law enforcement agencies
 18 have access.

19 9. I believe that the defendants in this case would have benefited from input from the
 20 public on the standard for suspicious activity reporting. I would have wanted the defendants to
 21 know when they adopted their standard for suspicious activity reporting that a standard that does
 22 not require reasonable suspicion of criminal activity harms innocent people, like me, who have
 23 not engaged in any wrongdoing: It makes us the targets of law enforcement scrutiny, puts our
 24 information in government databases, and adversely affects our reputations by identifying us as
 25 individuals who have engaged in conduct with a potential nexus to terrorism. I would also have
 26 wanted defendants to know the specific facts of my case so that they could understand the factual
 27 basis for my concerns. I would have specifically wanted defendants to understand, based on what
 28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

happened to me, that their standard for suspicious activity reporting encourages religious profiling. I was not aware that defendants sought input on the standard for suspicious activity reporting. As a result, I did not have an opportunity to share my perspective or the factual basis for my concerns.

10. As a result of the SAR about me, and the inclusion of information from the SAR about me in a national database, my reputation has been injured because I have been branded as a person engaged in activity with a potential nexus to terrorism, even though I was simply doing my job.

11. As a result of the SAR about me, and the inclusion of information from the SAR about me in a national database, my privacy has been invaded because any person with access to the database has access to information about me, even though I was simply doing my job.

12. I am deeply troubled by what may result from the collection, maintenance, and dissemination in a national database of a report describing me as engaging in suspicious activity with a potential nexus to terrorism.

13. Since learning about the SAR, I have felt despair. The knowledge that people are watching me and documenting my activities, even those activities that are entirely lawful and related to my work, has affected my confidence and created paranoia. I worry that anything I do could be misconstrued or manipulated to be used against me. I am constantly watching my actions and careful not to step out of line for fear of the consequences.

//
//
//
//
//
//
//

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

14. Since learning of the SAR, I have changed my behavior in many ways, big and small. For instance, I have shied away from interaction with my peers and built emotional walls. I have also not taken many leadership roles or other opportunities that were presented to me because I did not want to be open to further scrutiny. I was worried that my membership in a Muslim student group would garner further attention from the government and authorities.

I declare under penalty of perjury that the foregoing is true and correct. Executed this 9th day of September 2016 in San Jose, California.

By:  _____
Khaled Ibrahim

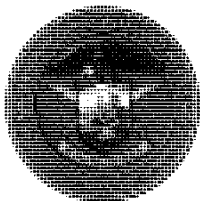
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

FILER'S ATTESTATION

I, Phillip J. Wiese, am the ECF user whose identification and password are being used to file this DECLARATION OF KHALED IBRAHIM IN SUPPORT OF PLAINTIFFS' MOTION FOR SUMMARY JUDGMENT. Pursuant to L.R. 5-1(i)(3), I hereby attest that concurrence in the electronic filing of this document has been obtained from each of the other signatories.

Dated: September 22, 2016 By /s/ Phillip J. Wiese
Phillip J. Wiese

Exhibit 1

**Central California Intelligence Center**

www.sacrtac.org ♦ (916) 808-8383 or (888) 884-8383 ♦ Fax (916) 874-6180

February 25, 2014

Mr. Yaman Salahi
Staff Attorney
Asian Americans Advancing Justice
Asian Law Caucus
55 Columbus Ave.
San Francisco, CA 94111
(415) 896-1701

Dear Mr. Salahi:

This letter is in response to the Public Records Act request received from the Asian Law Caucus dated January 22, 2014.

After reviewing your Public Records Act request it appears you have specifically requested the following:

"This letter constitutes a request under the California Public Records Act, Cal. Gov. Code 6250, et seq., and Article I s 3(b) of the California Constitution on behalf of Mr. Khaled Ibrahim for all records, including but not limited to Suspicious Activity Reports, pertaining to or referencing Mr. Ibrahim."

The CCIC/RTAC has located only one (1) Suspicious Activity Report (SAR) related to Mr. Ibrahim. Please see the attached redacted SAR (enclosure 1). After a thorough review of our records, there is no further information available regarding Mr. Khaled Ibrahim.

Respectfully,

A handwritten signature in black ink, appearing to read "Herb Brown".

Herb Brown, Executive Director
Central California Intelligence Center
(916) 874-1287

Enclosures (1)

ENCLOSURE 1

Case 3:14-cv-03120-RS Document 119 Filed 09/22/16 Page 9 of 10

Memex Record Number	Date Created	Activity Date	Title	Disposition	Activity
CCSA00001881	11/14/2011	11/6/2011	Suspicious attempt to purchase large number of computers	eGuardian Entry	<p>Contact was made with [REDACTED] by [REDACTED] during the week of 11-6-11 through 11-12-11 at the same [REDACTED] located in [REDACTED] Ca. [REDACTED] wanted to buy a large amount of computers from [REDACTED]. [REDACTED] told him to leave and did not sell any computers to [REDACTED]. This is the [REDACTED] [REDACTED] has made with [REDACTED].</p> <p>[REDACTED] The second contact with [REDACTED] occurred in [REDACTED].</p> <p>Thank you for your time. I have since [REDACTED] and work as a [REDACTED].</p> <p>Information submitted to [REDACTED] on [REDACTED] For [REDACTED] Located [REDACTED] Ca. I received a follow up from the [REDACTED] Located in [REDACTED] regarding the incident.</p> <p>I am a [REDACTED] located at [REDACTED] located at [REDACTED] [REDACTED] located in [REDACTED]. I have a friend whose name is named [REDACTED] and works as a [REDACTED] at [REDACTED] Located at [REDACTED].</p> <p>A customer [REDACTED] looking to buy merchandice [REDACTED] to be shipped to [REDACTED] old me that [REDACTED] bought over [REDACTED] to be [REDACTED] at that time.</p> <p>[REDACTED] said it would be OK for you to contact him for additional information [REDACTED] from [REDACTED] [REDACTED] said he cannot provide certain info because of customer privacy laws. Here is some additional information listed below:</p> <p>[REDACTED] said that the guy's name is [REDACTED] of [REDACTED] The [REDACTED] provided [REDACTED] is: [REDACTED] [REDACTED]'s [REDACTED] s [REDACTED] [REDACTED] is [REDACTED] [REDACTED] won't divulge [REDACTED] that the purchased all of the computers are shipped to the [REDACTED].</p> <p>When [REDACTED] asked [REDACTED] why he doesn't [REDACTED] or [REDACTED] [REDACTED] responded and said that those companies [REDACTED] and because the [REDACTED].</p>

					<p>[REDACTED] they can't sell to him directly.</p> <p>[REDACTED] requests [REDACTED] [REDACTED] [REDACTED]</p> <p>[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] continues to contact him to see if [REDACTED] [REDACTED] has [REDACTED]</p> <p>Please feel free to contact me at [REDACTED] [REDACTED] [REDACTED] [REDACTED] Thank you for your time.</p> <p>[REDACTED] [REDACTED] [REDACTED] [REDACTED]</p>
--	--	--	--	--	--

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

MORGAN, LEWIS & BOCKIUS LLP
Stephen Scotch-Marmo (admitted *pro hac vice*)
stephen.scotch-marmo@morganlewis.com
Michael James Ableson (admitted *pro hac vice*)
michael.ableson@morganlewis.com
101 Park Avenue
New York, NY 10178
Telephone: (212) 309-6000; Facsimile: (212) 309-6001

AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN CALIFORNIA
Linda Lye (SBN 215584), llye@aclunc.org
Julia Harumi Mass (SBN 189649), jmass@aclunc.org
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 621-2493; Facsimile: (415) 255-8437

ASIAN AMERICANS ADVANCING
JUSTICE - ASIAN LAW CAUCUS
Christina Sinha (SBN 278893), christinas@advancingjustice-alc.org
55 Columbus Avenue
San Francisco, CA 94111
Telephone: (415) 848-7711; Facsimile: (415) 896-1702

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

WILEY GILL; JAMES PRIGOFF; TARIQ
RAZAK; KHALID IBRAHIM; and AARON
CONKLIN,

Plaintiffs,

v.

DEPARTMENT OF JUSTICE; LORETTA
LYNCH, in her official capacity as the
Attorney General of the United States;
PROGRAM MANAGER – INFORMATION
SHARING ENVIRONMENT;
KSHEMENDRA PAUL, in his official
capacity as the Program Manager of the
Information Sharing Environment,

Defendants.

Case No. 3:14-cv-03120-RS-KAW

**DECLARATION OF TARIQ RAZAK IN
SUPPORT OF PLAINTIFFS' MOTION
FOR SUMMARY JUDGMENT**

Hearing Date: December 8, 2016
Time: 1:30 pm
Judge: Hon. Richard Seeborg
Courtroom: 3, 17th Floor
Date of Filing: July 10, 2014
Trial Date: None Set

1 I, Tariq Razak, declare as follows:

2 1. I am one of the Plaintiffs in the above-titled action. I submit this declaration in
3 support of Plaintiffs' Motion for Summary Judgment and Plaintiffs' Opposition to Defendants'
4 Motion for Summary Judgment. I have personal knowledge of each fact stated in this declaration
5 and, if called as a witness, I could and would competently and truthfully testify hereto.

6 2. I am a U.S. citizen of Pakistani descent. I reside in Placentia, California.

7 3. I currently work as an Automation Engineer for a bio-technology company in
8 Southern California. I previously worked at Quest Diagnostics as a Clinical Lab Associate.

9 4. On May 16, 2011, I went to the Santa Ana Regional Transportation Center, also
10 known as the Depot, because I had an appointment at the Santa Ana Work Center, which
11 connects job seekers with resources and opportunities and is housed at the Depot. I had recently
12 been laid off from my job at Quest Diagnostics and was hoping to find new job opportunities in
13 my field. I unfortunately was running late, and by the time I arrived, I had already missed my
14 appointment. I decided to go in and see if a job counselor could squeeze me in for an
15 appointment, or at least pick up some materials to aid my search.

16 5. My mother and I had been running errands earlier that day, and she accompanied
17 me to the Depot. She wears a hijab in public.

18 6. I had never been to the Depot before, and had some trouble locating the Work
19 Center, whose location within the Depot is not readily apparent; we looked around the Depot for a
20 while, attempting to discern its location, but also enjoying the look of the Depot, which is an
21 interesting building with some distinctive architecture. We eventually took an elevator to an
22 upper floor and found the Center. I separated from my mother, who went in search of a restroom,
23 while I spoke briefly with one of the employees and utilized some of the free materials that the
24 Center offered job seekers. I then walked to the restrooms and waited outside for my mother.
25 When she came out of the restroom, we walked back to our car and left the Depot.

26 7. At no point during my visit to the Depot did I engage in any conduct that could
27 reasonably be interpreted as indicating that I was involved with, or preparing to commit, any
28 criminal activity.

1 8. My attorneys subsequently showed me a copy of a Suspicious Activity Report
2 about me from the Santa Ana Police Department; a true and correct copy is attached to this
3 declaration as Exhibit 1. According to that report, a security officer at the Depot called the Santa
4 Ana Police Department to report me as suspicious after my brief visit to the Depot. The Report
5 also indicates that the police officer who responded to the call obtained my identity—apparently
6 through my license plate number—and created a Suspicious Activity Report recounting what the
7 security officer had told him about me.

8 9. The Suspicious Activity Report’s factual synopsis states, “Male of Middle Eastern
9 decent [sic] observed surveying entry/exit points,” and it describes me as “Male / Arab.” The
10 Report recounts that the security officer at the Depot stated that I “appeared to be observant” of
11 my surroundings and that I was “constantly surveying” the Depot. It also describes my mother as
12 “Female / Arab” and as wearing “a white burka head dress.” According to the security officer,
13 my conduct “was similar to examples shown in her training raising her suspicion and making the
14 decision to notify police.” The officer who submitted the Report requested that it be forwarded to
15 the Orange County Intelligence Assessment Center “for review and possible follow-up.”

16 10. I am deeply troubled that a security officer found my innocent behavior
17 suspicious; that she tracked me through the Depot and recorded my license plate number; and that
18 she reported me to the Santa Ana Police Department without any valid reason for doing so.

19 11. I am also deeply troubled that the Suspicious Activity Report reflects the officers’
20 apparent suspicion of what is actually my South Asian, not Arab, heritage and my mother’s hijab
21 (which is quite different from a “burka head dress”).

22 12. Through my attorneys, I submitted a request on February 18, 2014 to the FBI
23 under the Freedom of Information Act for documents in the FBI’s possession about me. In
24 response, the FBI produced redacted documents by letter dated February 13, 2015 (“FBI
25 Documents”). A true and correct copy of those documents (with my personally identifying
26 information further redacted) is attached to this declaration as Exhibit 2. The documents seem to
27 show that the FBI maintains information about me related to the incident reported in the
28

1 Suspicious Activity Report about me in some kind of database.

2 13. The FBI Documents show that the FBI’s Counterterrorism Division and Los
3 Angeles field office took various actions in response to the information they received in the
4 Suspicious Activity Report about me. For instance, the documents show that on June 27, 2011—
5 over a month after the FBI had received the Suspicious Activity Report about me—someone at
6 the FBI reviewed the Report and information obtained from data checks and “found no evidence
7 of the Subject’s being involved in terrorism or criminal activity.” It further states that the writer
8 of the entry “believes the lead was sent only because [redacted].” Another entry from the same
9 date states that the writer “request[ed] the lead [be] closed.”

10 14. Despite the above, another entry from the same document, dated July 06, 2011—
11 about a week after the above entry requesting the lead be closed—indicates that the Report about
12 me was nonetheless reviewed further. That later entry states that “[a]fter interviewing the Subject
13 and verifying his story through a contact at the EDD. [sic] Writer request the lead closed.”

14 15. I find these two entries about me deeply troubling, not just because it seems as
15 though my innocent and lawful behavior was investigated, but also because the investigation
16 apparently continued despite the “writer” finding that my behavior had no nexus to terrorism. It
17 is worrisome indeed that my innocent behavior was turned into a Suspicious Activity Report that
18 was investigated for weeks after the fact, and presumably by at least two investigators. The fact
19 that the investigation continued even after an agent requested that the “lead” be closed makes me
20 worry that the investigation could be reopened at any time without good cause.

21 16. Based on my review of the Defendants’ Answer in this matter, it is my
22 understanding that an incident report containing information in the Suspicious Activity Report
23 about me was uploaded to eGuardian, which I understand is a national database to which
24 thousands of law enforcement agencies have access.

25 17. I am deeply troubled by what has occurred, and what may yet occur, due to the
26 collection, maintenance, and dissemination in national databases of a Report describing me as
27 engaging in suspicious activity with a potential nexus to terrorism. As a result of the inclusion of
28

1 this information about me in these databases, my reputation has been injured, as I have been
2 branded as a person engaged in activity with a potential nexus to terrorism, even though I was
3 simply walking through a train station looking for an employment resource center and waiting for
4 my mother to exit the restroom.

5 18. In addition, as a result of the inclusion of this information about me in these
6 databases, my privacy has been invaded because any person with access to the database has
7 access to information about me.

8 19. I am worried that the maintenance of the Suspicious Activity Report about me in
9 the FBI database or any database will cause law enforcement officers who see it to further
10 scrutinize and vilify my lawful behavior, since the Suspicious Activity Report makes it seem as
11 though I take part in nefarious activities. This worry is only compounded by my understanding
12 that the Suspicious Activity Report has been distributed widely to other law enforcement officers
13 via these databases.

14 20. I am also troubled that the FBI's file on me includes my address and a description
15 of my vehicle and license plate number, all described as relevant to "Counterterrorism." I am
16 concerned that the retention and dissemination of that information will draw undue law
17 enforcement attention to my home and vehicle, and will intensify the law enforcement response
18 during any otherwise routine encounters with law enforcement.

19 21. On April 9, 2015, through my attorneys, I appealed the FBI's redactions of the
20 documents produced on February 13, 2015. A true and correct copy of the appeal is attached as
21 Exhibit 3. By letter dated May 21, 2015, the FBI denied my appeal and asserted its view that I do
22 not have a right to access certain information that the FBI possesses about me under the Privacy
23 Act or FOIA. A true and correct copy of the FBI's May 21, 2015 letter is attached as Exhibit 4.

24 22. The FBI's response to my FOIA request leads me to believe that, because of the
25 Suspicious Activity Report about me, information about me has been uploaded not only to
26 eGuardian, but also to a separate FBI database.

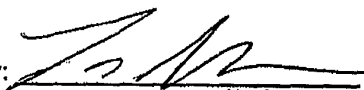
27 23. On June 25, 2014, I submitted a request to the FBI and the Program Manager for
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

the Information Sharing Environment seeking an expungement of information in their files that describes conduct of mine that does not support reasonable suspicion of criminal activity or that does not implicate criminal conduct. The expungement request is attached to this declaration as Exhibit 5. To my knowledge, as of the date of the filing of this declaration, neither the FBI nor the Program Manager has responded to my request.

24. I believe that the defendants in this case would have benefited from input from the public on the standard for suspicious activity reporting. I would have wanted the defendants to know when they adopted their standard for suspicious activity reporting that a standard that does not require reasonable suspicion of criminal activity harms innocent people, like me, who have not engaged in any wrongdoing: it makes us the targets of law enforcement scrutiny; puts our information in government databases; and adversely affects our reputations by identifying us as individuals who have engaged in conduct with a potential nexus to terrorism. I would also have wanted the defendants to know the specific facts of my case, so that they could understand the factual basis for my concerns. I would specifically have wanted the defendants to understand, based on what happened to me, that their standard for suspicious activity reporting encourages racial and religious profiling. I was not aware that the defendants sought input on the standard for suspicious activity reporting. As a result, I did not have an opportunity to share my perspective or the factual basis for my concerns.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct. Executed this 14th day of September 2016 in Placentia, California.

By: 
Tariq Razak

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

FILER’S ATTESTATION


I, Phillip J. Wiese, am the ECF user whose identification and password are being used to file this DECLARATION OF TARIQ RAZAK IN SUPPORT OF PLAINTIFFS’ MOTION FOR SUMMARY JUDGMENT. Pursuant to L.R. 5-1(i)(3), I hereby attest that concurrence in the electronic filing of this document has been obtained from each of the other signatories.

Dated: September 22, 2016 By /s/ Phillip J. Wiese
Phillip J. Wiese

EXHIBIT 1

Santa Ana PD 2011-15770: Suspicious Activity Report by #3203

Page 1 of 3

	Santa Ana Police Department 60 Civic Center Plaza -- Santa Ana, CA 92701	Case No. 2011-15770
	Information Report	
Case Type:	Suspicious Activity Report	
Prepared by:	Ofc. J. Gallardo #3203 Section: Patrol Watch 1/NE	
Date prepared:	5/16/2011 1502 hours	

Reviewed by: R. Rodriguez 2755 Date/Time: 5-16-11 1720 (Rev. 0.60)

Records Distribution: Review: 1/82 Total Copies: 2 By: 1882 Date: _____

<input type="checkbox"/> Animal Control	<input type="checkbox"/> Court Liaison	<input type="checkbox"/> Orangewood	<input type="checkbox"/> Traffic	<input type="checkbox"/> Trackers
<input checked="" type="checkbox"/> District Inv.	<input type="checkbox"/> CAP	<input type="checkbox"/> Evidence	<input type="checkbox"/> Vice	<input type="checkbox"/> Sex Crimes
<input type="checkbox"/> Domestic Violence	<input type="checkbox"/> Crime Prevention	<input type="checkbox"/> Narcotics	<input type="checkbox"/> Juvenile Inv.	<input type="checkbox"/> Graffiti
<input type="checkbox"/> Career Criminal Unit	<input type="checkbox"/> Crime Analysis	<input type="checkbox"/> Gangs	<input type="checkbox"/> Fax/Name	
<input type="checkbox"/> Juvenile Hall	<input type="checkbox"/> Stats	<input type="checkbox"/> Rap	<input checked="" type="checkbox"/> Other <u>Home land Sec</u>	
#31000000000024029	<input type="checkbox"/> Other _____		<input type="checkbox"/> Other _____	

Incident Activity Summary:

Special Attention:

Information Report: Train Station Subject

Incident Date/Time: Occurred: 05/16/2011 10:20 to 05/16/2011 10:30
Reported: 05/16/2011 12:18

Location Occurred: 1000 E. Santa Ana Boulevard, Santa Ana, CA 92702-0000
Grid: 205 Dist.: 2

Factual Synopsis: Male of Middle Eastern decent observed surveying entry/exit points.

Person: **Karina De La Rosa**

Involvement: **Contact**

Person Note: *Security Officer*

Gender/Race: Female / Hispanic

DOBs:

Address:

Grid: 205 Dist.: 2

Contact Info:

Description: Physical: 5'05" tall, 125 lbs., thin build, long brown straight hair, black eyes,

Person: **Tariq Razak**

Involvement: **Mentioned**

Person Note:

Santa Ana PD 2011-15770: Suspicious Activity Report by #3203

Page 2 of 3

Close Cropped Beard.

Gender/Race: Male / Arab

Address: Location association: Resides

Description: [REDACTED]
Physical: 5'11" tall, 175 lbs., medium build, short black straight hair, brown eyes, beard,

Person: **Unknown**

Involvement: **Mentioned**

Person Note: *Unknown information about female.*

Gender/Race: Female / Arab

Vehicle: **Passenger Car**

Involvement: Involved / Retained by Owner

Description: 2007 Honda Accord, 4 Door Sedan or Hatchback, White/White

License Plate: CA, Reg 07/2011

Registered owner:

Legal owner:

Narrative:

On 5-16-11 at about 1220 hours, I responded to The Santa Ana Train Depot at 1000 E Santa Ana Blvd.

I contacted Security Officer Karina De La Rosa who told me the following:

At approximately 1020 hours, Karina took the elevator from the second floor to the first floor. In the elevator with Karina was a male between male of who Karina believed was of Middle Eastern descent. Karina's suspicion became aroused because the male appeared to be observant of his surroundings and was constantly surveying all areas of the facility. The male's appearance was neat and clean with a closely cropped beard, short hair wearing blue jeans and a blue plaid shirt.

Upon exiting the elevator, Karina observed the male meticulously study the entry/exit points, different lobby areas of the train station where large groups of passengers gather. The male then went to the north end of station where male and female restrooms are located and stood by outside the restrooms. Minutes later, a female wearing a white burka head dress, black pants and a blue shirt exited the restroom.

The two individuals then both exited the train station out of the north doors, entered a white 2007 Honda Accord (Ca Li) and left the Train Station in an unknown direction.

Karina continued to say that she received 'suspicious activity as related to terrorism training' by a local police agency. Karina said the behavior depicted by the male was similar to examples shown in her training raising her suspicion and making the decision to notify police. Attached to this report is a photocopy of Karina's incident report.

Request this report be forwarded to SAPD Homeland Security Division and to the Orange County Intelligence Assessment Center (OCIAC) for review and possible follow-up.

http://ir2stg/Report.aspx?RecordType_=Narrative&RecordID_=10004&Action_=Edit&Fc... 5/16/2011

Santa Ana PD 2011-15770: Suspicious Activity Report by #3203

Page 3 of 3

Ofcr. J. Gallardo # 3203
Terrorism Liaison Officer (TLO)
Santa Ana Police Department

EXHIBIT 2

U.S. Department of Justice



Federal Bureau of Investigation
Washington, D.C. 20535

February 13, 2015

MR. YAMAN SALAH
ADVANCING JUSTICE- ASIAN LAW CAUCUS
STAFF ATTORNEY
55 COLUMBUS AVENUE
SAN FRANCISCO, CA 94111

FOIPA Request No.: 1253741-000
Subject: RAZAK, TARIQ

Dear Mr. Salah:

The enclosed documents were reviewed under the Freedom of Information/Privacy Acts (FOIPA), Title 5, United States Code, Section 552/552a. Deletions have been made to protect information which is exempt from disclosure, with the appropriate exemptions noted on the page next to the excision. In addition, a deleted page information sheet was inserted in the file to indicate where pages were withheld entirely. The exemptions used to withhold information are marked below and explained on the enclosed Explanation of Exemptions:

Section 552		Section 552a
<input type="checkbox"/> (b)(1)	<input type="checkbox"/> (b)(7)(A)	<input type="checkbox"/> (d)(5)
<input type="checkbox"/> (b)(2)	<input type="checkbox"/> (b)(7)(B)	<input checked="" type="checkbox"/> (j)(2)
<input type="checkbox"/> (b)(3)	<input checked="" type="checkbox"/> (b)(7)(C)	<input type="checkbox"/> (k)(1)
_____	<input type="checkbox"/> (b)(7)(D)	<input type="checkbox"/> (k)(2)
_____	<input checked="" type="checkbox"/> (b)(7)(E)	<input type="checkbox"/> (k)(3)
_____	<input type="checkbox"/> (b)(7)(F)	<input type="checkbox"/> (k)(4)
<input type="checkbox"/> (b)(4)	<input type="checkbox"/> (b)(8)	<input type="checkbox"/> (k)(5)
<input type="checkbox"/> (b)(5)	<input type="checkbox"/> (b)(9)	<input type="checkbox"/> (k)(6)
<input checked="" type="checkbox"/> (b)(6)		<input type="checkbox"/> (k)(7)

13 pages were reviewed and 13 pages are being released.

- Document(s) were located which originated with, or contained information concerning other Government agency(ies) [OGA]. This information has been:
 - referred to the OGA for review and direct response to you.
 - referred to the OGA for consultation. The FBI will correspond with you regarding this information when the consultation is finished.
 - In accordance with standard FBI practice and pursuant to FOIA exemption (b)(7)(E) and Privacy Act exemption (j)(2) [5 U.S.C. § 552/552a (b)(7)(E)/(j)(2)], this response neither confirms nor denies the existence of your subject's name on any watch lists.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S.C. § 552(c) (2006 & Supp. IV (2010)). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist. Enclosed for your information is a copy of the Explanation of Exemptions.

You have the right to appeal any denials in this release. Appeals should be directed in writing to the Director, Office of Information Policy (OIP), U.S. Department of Justice, 1425 New York Ave., NW, Suite 11050, Washington, D.C. 20530-0001, or you may submit an appeal through OIP's eFOIA portal at <http://www.justice.gov/oip/efoia-portal.html>. Your appeal must be received by OIP within sixty (60) days from the date of this letter in order to be considered timely. The envelope and the letter should be clearly marked "Freedom of Information Appeal." Please cite the FOIPA Request Number assigned to your request so that it may be easily identified.

The enclosed material is from the main investigative file(s) in which the subject(s) of your request was the focus of the investigation. Our search located additional references, in files relating to other individuals, or matters, which may or may not be about your subject(s). Our experience has shown when ident, references usually contain information similar to the information processed in the main file(s). Because of our significant backlog, we have given priority to processing only the main investigative file(s). If you want the references, you must submit a separate request for them in writing, and they will be reviewed at a later date, as time and resources permit.

See additional information which follows.

Sincerely,



David M. Hardy
Section Chief
Record/Information
Dissemination Section
Records Management Division

Enclosure(s)

The enclosed documents responsive to your request are exempt from disclosure in their entirety pursuant to the Privacy Act, Title 5, United States Code, Section 552(a), subsection (j)(2). However, these records have been processed pursuant to the Freedom of Information Act, Title 5, United States Code, Section 552, thereby affording you the greatest degree of access authorized by both laws.

This material is being provided to you at no charge.

EXPLANATION OF EXEMPTIONS**SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552**

- (b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;
- (b)(2) related solely to the internal personnel rules and practices of an agency;
- (b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute(A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could be reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could be reasonably expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;
- (b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

- (d)(5) information compiled in reasonable anticipation of a civil action proceeding;
- (j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
- (k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;
- (k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;
- (k)(4) required by statute to be maintained and used solely as statistical records;
- (k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;
- (k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

FBI/DOJ

Sentinel Working Copy

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 04-03-2014 BY NSICG/F22M46K38

[Redacted]

b7E

Filing and Security

Primary Case: [Redacted]

Case Title: (S) ZERO FILE -

Serial Number: [Redacted]

Serialized: 05/19/2011

b7E

Initiated: 01/04/2009

Details

Serial #: [Redacted]

Type: OTHER

b7E

Document Title: 11-0236 SUSPICIOUS SUBJECT OBSERVED AT THE SANTA ANA TRAIN S

Approval Date: 05/19/2011

Classification: U

Contents: Unclassified

IncidentNum: (U) [Redacted]
IncidentType: (U) Suspicious Activity
Status: (U) Open
ModifiedTmstp: (U) 2011-05-25 21:55:46.0
IncidentPriority: (U) Routine
ReceiptMethod: (U) Other
SuspiciousActivityCode: (U) [Redacted]
ReportSummary: (U) 11-0236 Suspicious subject observed at the Santa Ana train station

b7E

Assessment Type: (U) [Redacted]

Disposition: (U) [Redacted]

IncidentFacts: (U) On 17 May 2011 OCIAC received information from the Santa Ana Police Department regarding a suspicious subject seen at the Santa Ana train station on 16 May. Santa Ana PD was contacted by [Redacted]

[Redacted] Due to heightened security concerns regarding the rail sector and [Redacted] noticed a male subject who she believed was exhibiting suspicious behavior. During her contact with Ofc. [Redacted] she described the incident which occurred at the train station on 16 May at about 1020 in the morning. [Redacted] said she first encountered the male subject in the elevator at the station and described him as being a male Middle-Eastern in his late 20's, 5'-11", with short dark hair, a beard, and wearing a blue plaid shirt and jeans. A short time later she saw the same subject pacing in the lobby of the station paying "meticulous" attention to the exits, signage, tenant areas, and areas where large groups of passengers gather. [Redacted] continued to watch the subject as he moved to the North end of the station near the restrooms. She then saw [Redacted]

b6
b7C

[Redacted] then left the station and drove away in a white Honda Accord with a license plate of [Redacted] documented her observations on a Securitas Incident Report, see attached copy. A records check on the license plate of [Redacted] revealed it was currently registered to Tariq RAZAK with an address of [Redacted] in Irvine, CA. A records check on RAZAK revealed he matches the description provided by [Redacted] as he is 27 years old, 6'-00", with brown hair and brown eyes. A driver's license photo was located for RAZAK, however it was taken in early 2000. [Redacted]

b6
b7C

b7E

Sentinel Working Copy

[Redacted]

[Redacted]

b7E

b7E

Subjects:

FullName: (U) Tariq , Anjum, Razak
GenderDesc: (U) Male
FileType: (U) PERSON
WhiteUsPersonDesc: (U) Yes
NoDescriptiveText: (U) DOB: [Redacted]

FullName: (U) [Redacted]
GenderDesc: (U) [Redacted]
FileType: (U) [Redacted]
WhiteUsPersonDesc: (U) [Redacted]
NoDescriptiveText: (U) [Redacted]

b6
b7C

Sources:

SourceName: (U) Ofc [Redacted]
SourceTypeDesc: (U) Law Enforcement
SourceGenderCode: (U) M
Protect: (U) N
Credible: (U) YES
Contact: (U) Y
Polygraph: (U) N
SourceContactInfo: (U) [Redacted]

b6
b7C

Targets:

Weapons:

Vehicles:

MakeDesc: (U) Honda
ModelText: (U) ACCORD
YearText: (U) 2007

Sentinel Working Copy



b7E

ProvinceDesc: (U) California
CountryDesc: (U) United States
Tag: (U) [redacted]
Description: (U) 4 door

Leads:

Tasks:

Notes:

AssignmentTypeDesc: (U) Note
StatusDesc: (U) Completed
Tofieldofficedesc: (U) Hq - Counterterrorism
Fromuserdesc: (U) [redacted]
CreatedOn: (U) 2011-05-19 17:41:24
Instruction: (U) Referred to [redacted] per their request.

b7E

AssignmentTypeDesc: (U) Note
StatusDesc: (U) Completed
Tofieldofficedesc: (U) Hq - Counterterrorism
Fromuserdesc: (U) [redacted]
CreatedOn: (U) 2011-05-19 17:44:31
Instruction: (U) Location Name: Santa Ana Train Station
Location Type: OTHER
Location Street: 1000 E. Santa Ana, Blvd
Location
City: Santa Ana
Location State: CA
Location Country: USA

AssignmentTypeDesc: (U) Note
StatusDesc: (U) Completed
Tofieldofficedesc: (U) Hq - Counterterrorism
Fromuserdesc: (U) [redacted]
CreatedOn: (U) 2011-05-19 17:44:31



Sentinel Working Copy

Instruction: (U) ORI ID: CAF00000
ORI Name: Los Angeles JRIC
ORI Phone: [Redacted]
ORI Email: [Redacted]
ORI Street Number: [Redacted]
ORI Street Name: [Redacted]
ORI City: [Redacted]
ORI State: CA
ORI Country: US
ORI Postal Code: 90650
ORI Field Office Code: LA

b7E

b6
b7C
b7E

AssignmentTypeDesc: (U) Note
StatusDesc: (U) Completed
Tofieldofficedesc: (U) Hq - Counterterrorism
Fromuserdesc: (U) [Redacted]
CreatedOn: (U) 2011-05-19 17:44:31

AssignmentTypeDesc: (U) Note
StatusDesc: (U) Completed
Tofieldofficedesc: (U) Hq - Counterterrorism
Fromuserdesc: (U) [Redacted]
CreatedOn: (U) 2011-05-19 17:44:31

b7E

AssignmentTypeDesc: (U) Note
StatusDesc: (U) Completed
Tofieldofficedesc: (U) Hq - Counterterrorism
Fromuserdesc: (U) [Redacted]
CreatedOn: (U) 2011-05-19 17:44:31

AssignmentTypeDesc: (U) Note
StatusDesc: (U) Completed
Tofieldofficedesc: (U) Hq - Counterterrorism
Fromuserdesc: (U) [Redacted]
CreatedOn: (U) 2011-05-19 17:44:31

AssignmentTypeDesc: (U) Note
StatusDesc: (U) Completed
Tofieldofficedesc: (U) Hq - Counterterrorism
Fromuserdesc: (U) [Redacted]
CreatedOn: (U) 2011-05-19 17:44:31

AssignmentTypeDesc: (U) Note
StatusDesc: (U) Completed
Tofieldofficedesc: (U) Hq - Counterterrorism
Fromuserdesc: (U) [Redacted]
CreatedOn: (U) 2011-05-19 17:44:31
Instruction: (U) [Redacted]

b6
b7C
b7E

Police Report Number: 11-0236
Creator Surname: [Redacted]
Creator Given Name: [Redacted]
Creator Email: [Redacted]
Creator Telephone: [Redacted]

Sentinel Working Copy

b7E

Groups:

Unclassified

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 11-25-2014 BY K22M45K35/NSICG

Case 3:14-cv-03120-RS Document 118 Filed 09/22/16 Page 21 of 39

Filing and Security

Primary Case: [redacted]

Case Title: (S) ZERO FILE -

Serial Number: [redacted]

b7E

Serialized: 05/19/2011

Initiated: 01/04/2009

Details

Serial #: [redacted]

Type: OTHER

Document Title: 11-0236 SUSPICIOUS SUBJECT OBSERVED AT THE SANTA ANA TRAIN S

Approval Date: 05/19/2011

Classification: U

Contents: Unclassified

IncidentNum: (U) [redacted]

IncidentType: (U) Suspicious Activity

Status: (U) Closed

ModifiedTmstp: (U) 2011-07-28 14:18:41.0

IncidentPriority: (U) Routine

ReceiptMethod: (U) Other

SuspiciousActivityCode: (U) [redacted]

b7E

ReportSummary: (U) 11-0236 SUSPICIOUS subject observed at the Santa Ana train station

Assessment Type: (U) [redacted]

Disposition: (U) CLOSED

DispositionNotes: (U) (U) On 07/06/2011, After interviewing the Subject and verifying his story through a contact at the EDD. Writer request the lead closed.

(U) On 06/27/2011, After reviewing the lead. Writer has found no nexus to terrorism and request the lead closed inconclusive.

It is noted that the individuals and groups identified during the assessment do not warrant further FBI investigation at this time. It is recommended that this assessment be closed.

Incident close request sent by [redacted] on 2011-06-27 13:12:27.0.

b6
b7C

Incident close request sent by [redacted] on 2011-07-06 18:04:15.0.

** Incident closed by [redacted] on 2011-07-28 14:18:41.0. **

IncidentFacts: (U) On 17 May 2011 OCIAC received information from

Sentinel Working Copy

Case 3:14-cv-03120-RS Document 118 Filed 09/22/16 Page 22 of 39

b7E

the Santa Ana Police Department regarding a suspicious subject seen at the Santa Ana train station on 16 May. Santa Ana PD was contacted by [redacted]

[redacted] Due to heightened security concerns regarding the rail sector and [redacted]

[redacted] noticed a male subject who she believed was exhibiting suspicious behavior. During her contact with Ofc. [redacted] she described the incident

which occurred at the train station on 16 May at about 1020 in the morning. [redacted] said she first encountered the male subject in the elevator at the station and described him as being a male Middle-Eastern in his late 20's, 5'-11", with short dark hair, a

b6
b7C

beard, and wearing a blue plaid shirt and jeans. A short time later she saw the same subject pacing in the lobby of the station paying "meticulous" attention to the exits, signage, tenant areas, and areas where large groups of passengers gather. [redacted] continued to watch the subject as he moved to the North end of the station near the restrooms. She then saw [redacted]

[redacted] then left the station and drove away in a White Honda Accord with a license plate of [redacted]. [redacted] documented her observations on a Securitas Incident Report, see attached copy. A records check on the license plate of [redacted] revealed it was currently registered to Tariq RAZAK with an address of [redacted] in Irvine, CA. A records check on RAZAK revealed he matches the description provided by [redacted] as he is 27 years old, 6'-00", with brown hair and brown eyes. A driver's license photo was located for RAZAK, however it was taken in early 2000. [redacted]

b7E

Subjects:

FullName: (U) Tariq , Anjum, Razak
GenderDesc: (U) Male
FileType: (U) PERSON
WhiteUsPersonDesc: (U) Yes
NoDescriptiveText: (U) DOB: [redacted]

FullName: (U) [redacted]
GenderDesc: (U) [redacted]
FileType: (U) [redacted]
WhiteUsPersonDesc: (U) [redacted]
NoDescriptiveText: (U) [redacted]

b6
b7C

b7E

Sources:

SourceName: (U) Ofc [redacted]
SourceTypeDesc: (U) Law Enforcement
SourceGenderCode: (U) M
Protect: (U) N
Credible: (U) YES
Contact: (U) Y
Polygraph: (U) N
SourceContactInfo: (U) [redacted]

b6
b7C

Targets:

Weapons:

Vehicles:

MakeDesc: (U) Honda
ModelText: (U) ACCORD
YearText: (U) 2007
ProvinceDesc: (U) California
CountryDesc: (U) United States

b7E

Tag: (U) [redacted]
Description: (U) 4 door

Leads:

Tasks:

Notes:

AssignmentTypeDesc: (U) Note
StatusDesc: (U) Completed
ToFieldofficedesc: (U) Hq - Counterterrorism
Fromuserdesc: (U) [redacted]
CreatedOn: (U) 2011-05-19 17:41:24
Instruction: (U) Referred to [redacted] per their request.

b7E

AssignmentTypeDesc: (U) Note
StatusDesc: (U) Completed
ToFieldofficedesc: (U) Hq - Counterterrorism
Fromuserdesc: (U) [redacted]
CreatedOn: (U) 2011-05-19 17:44:31
Instruction: (U) Location Name: Santa Ana Train Station
Location Type: OTHER
Location Street: 1000 E. Santa Ana, Blvd
Location
City: Santa Ana
Location State: CA
Location Country: USA

AssignmentTypeDesc: (U) Note
StatusDesc: (U) Completed
ToFieldofficedesc: (U) Hq - Counterterrorism
Fromuserdesc: (U) [redacted]
CreatedOn: (U) 2011-05-19 17:44:31

AssignmentTypeDesc: (U) Note
StatusDesc: (U) Completed
ToFieldofficedesc: (U) Hq - Counterterrorism
Fromuserdesc: (U) [redacted]
CreatedOn: (U) 2011-05-19 17:44:31
Instruction: (U) ORI ID: [redacted]
ORI Name: Los Angeles JRIC
ORI Phone: [redacted]
ORI Email: [redacted]
ORI Street
Number: [redacted]
ORI Street Name: [redacted]
ORI City: [redacted]
ORI State: CA
ORI Country: US
ORI Postal Code: 90650
ORI
Field Office Code: LA

b6
b7C
b7E

AssignmentTypeDesc: (U) Note
StatusDesc: (U) Completed
ToFieldofficedesc: (U) Hq - Counterterrorism
Fromuserdesc: (U) [redacted]

Sentinel Working Copy

Case 3:14-cv-03120-RS Document 118 Filed 09/22/16 Page 25 of 39

b7E

CreatedOn: (U) 2011-05-19 17:44:31

Instruction: (U) [redacted]

b6
b7C
b7E

Police Report Number: 11-0236

Creator

Surname: [redacted]

Creator Given Name: [redacted]

Creator Email: [redacted]

Creator Telephone: [redacted]

AssignmentTypeDesc: (U) Note

StatusDesc: (U) Completed

Tofieldofficedesc: (U) Hq - Counterterrorism

Fromuserdesc: (U) [redacted]

CreatedOn: (U) 2011-05-19 17:44:31

AssignmentTypeDesc: (U) Note

StatusDesc: (U) Completed

Tofieldofficedesc: (U) Hq - Counterterrorism

Fromuserdesc: (U) [redacted]

CreatedOn: (U) 2011-05-19 17:44:31

b7E

AssignmentTypeDesc: (U) Note

StatusDesc: (U) Completed

Tofieldofficedesc: (U) Hq - Counterterrorism

Fromuserdesc: (U) [redacted]

CreatedOn: (U) 2011-05-19 17:44:31

AssignmentTypeDesc: (U) Note

StatusDesc: (U) Completed

Tofieldofficedesc: (U) Hq - Counterterrorism

Fromuserdesc: (U) [redacted]

CreatedOn: (U) 2011-05-19 17:44:31

AssignmentTypeDesc: (U) Note

InvestigativeMethod: (U) Access/examine FBI/DOJ records, and obtain information from FBI/DOJ personnel.

StatusDesc: (U) Completed

Tofieldofficedesc: (U) Los Angeles

Fromuserdesc: (U) [redacted]

CreatedOn: (U) 2011-06-21 15:25:26

Instruction: (U) (U) [redacted]

b6
b7C
b7E

Subject Tariq.

AssignmentTypeDesc: (U) Note

InvestigativeMethod: (U) Access/examine FBI/DOJ records, and obtain information from FBI/DOJ personnel.

StatusDesc: (U) Completed

Tofieldofficedesc: (U) Los Angeles

Fromuserdesc: (U) [redacted]

CreatedOn: (U) 2011-06-21 15:27:30

Instruction: (U) (U) [redacted]

b6
b7C
b7E

AssignmentTypeDesc: (U) Note

Sentinel Working Copy

Case 3:14-cv-03120-RS Document 118 Filed 09/22/16 Page 26 of 39

b7E

InvestigativeMethod: (U) Access/examine FBI/DOJ records, and obtain information from FBI/DOJ personnel.
 StatusDesc: (U) Completed
 Tofieldofficedesc: (U) Los Angeles
 Fromuserdesc: (U) [redacted]
 CreatedOn: (U) 2011-06-21 16:03:33
 Instruction: (U) (U) [redacted]

b6
b7C
b7E

[redacted]

AssignmentTypeDesc: (U) Note
 InvestigativeMethod: (U) Access/examine FBI/DOJ records, and obtain information from FBI/DOJ personnel.
 StatusDesc: (U) Completed
 Tofieldofficedesc: (U) Los Angeles
 Fromuserdesc: (U) [redacted]
 CreatedOn: (U) 2011-06-21 16:30:03
 Instruction: (U) (U) [redacted]

b6
b7C
b7E

[redacted]

AssignmentTypeDesc: (U) Note
 InvestigativeMethod: (U) Access/examine FBI/DOJ records, and obtain information from FBI/DOJ personnel.
 StatusDesc: (U) Completed
 Tofieldofficedesc: (U) Los Angeles
 Fromuserdesc: (U) [redacted]
 CreatedOn: (U) 2011-06-21 16:35:49
 Instruction: (U) (U) [redacted]

b6
b7C
b7E

[redacted]

AssignmentTypeDesc: (U) Note
 InvestigativeMethod: (U) Administrative note for informational purposes.
 StatusDesc: (U) Completed
 Tofieldofficedesc: (U) Los Angeles
 Fromuserdesc: (U) [redacted]
 CreatedOn: (U) 2011-06-27 12:58:43
 Instruction: (U) (U) On 06/27/2011, After reviewing the lead and information obtained from data checks. Writer has found no evidence of the Subject's being involved in terrorism or criminal activity. Writer believes the lead was sent only because

b6
b7C

[redacted]

AssignmentTypeDesc: (U) Note
 StatusDesc: (U) Completed
 Tofieldofficedesc: (U) Los Angeles
 Fromuserdesc: (U) [redacted]
 CreatedOn: (U) 2011-06-29 20:36:51

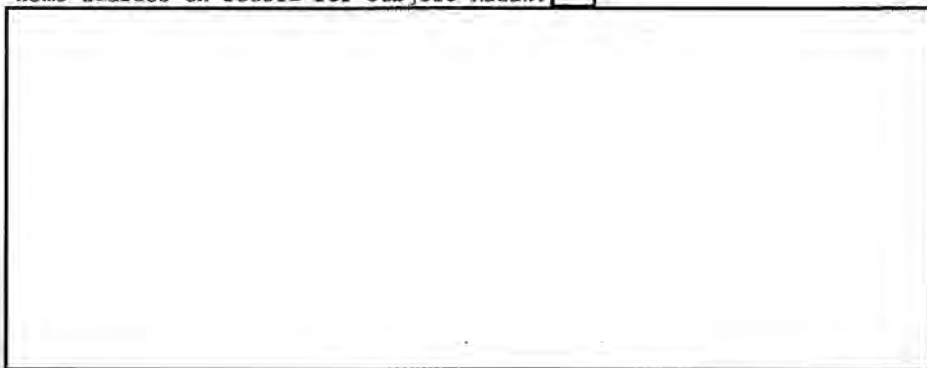
Sentinel Working Copy

Case 3:14-cv-03120-RS Document 118 Filed 09/22/16 Page 27 of 39

Instruction: (U) (U) SSA [redacted] has reviewed this incident and determined it is being worked in accordance to the DIOG and has recently been updated. [redacted]

b7E
b6
b7C
b7E

AssignmentTypeDesc: (U) Note
InvestigativeMethod: (U) Interview or request information from members of the public and private entities.
StatusDesc: (U) Completed
Tofieldofficedesc: (U) Los Angeles
Fromuserdesc: (U) [redacted]
CreatedOn: (U) 2011-07-05 13:48:06
Instruction: (U) (U) On 06/29/2011, Writer and [redacted] drove to [redacted] Irvine, Ca. 92702 this being the home address on record for Subject Razak. [redacted]



b6
b7C

AssignmentTypeDesc: (U) Note
InvestigativeMethod: (U) Interview or request information from members of the public and private entities.
StatusDesc: (U) Completed
Tofieldofficedesc: (U) Los Angeles
Fromuserdesc: (U) [redacted]
CreatedOn: (U) 2011-07-05 14:03:13
Instruction: (U) (U) On 06/29/2011, Writer was contacted via phone by Subject Razak. After identifying myself and the reason for the contact he agreed to talk to me. He said he was at the Santa Ana train station [redacted] on that day. He said he has been out of work for about two months and was at the EDD office located on the second floor above the train station. He said he was waiting [redacted] [redacted] He said he was pacing and looking around the station [redacted] He said he drives [redacted] everyday since he is not working. He provided writer with his cell phone number [redacted] and said to contact him if writer needed.

b6
b7C

b6
b7C

Sentinel Working Copy

Case 3:14-cv-03120-RS Document 118 Filed 09/22/16 Page 28 of 39

b7E

AssignmentTypeDesc: (U) Note
 InvestigativeMethod: (U) Access/examine FBI/DOJ records, and obtain information from FBI/DOJ personnel.
 StatusDesc: (U) Completed
 ToFieldofficedesc: (U) Los Angeles
 Fromuserdesc: (U) [redacted]
 CreatedOn: (U) 2011-07-05 14:55:19
 Instruction: (U) (U) On 07/05/2011, Writer provided SA [redacted] the Subject's information. SA [redacted] will check with his EDD contact to verify the Subject's story about being at the Santa Ana office.

b6
b7C

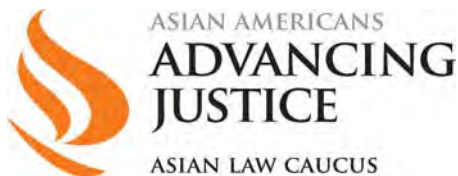
AssignmentTypeDesc: (U) Note
 InvestigativeMethod: (U) Request info/view records from other govt agencies/entities (federal/state/local/tribal/foreign).
 StatusDesc: (U) Completed
 ToFieldofficedesc: (U) Los Angeles
 Fromuserdesc: (U) [redacted]
 CreatedOn: (U) 2011-07-06 17:55:44
 Instruction: (U) (U) On 07/06/2011, Writer was advised by SA [redacted] that the Subject was still getting Unemployment Insurance benefits from the Santa Ana office of the EDD. SA [redacted] received the information from his contact, EDD Investigator [redacted]

b6
b7C

Groups:

Unclassified

EXHIBIT 3



April 9, 2015

VIA FEDEX NEXT DAY AIR

Director
Office of Information Policy
U.S. Department of Justice
1425 New York Ave., NW, Suite 11050
Washington, D.C. 20530-0001

Re: Freedom of Information Act Appeal on Behalf of Tariq Razak; FOIPA Request No. 1253741-000

Dear Director:

We write to appeal the U.S. Department of Justice's (the "Department") February 13, 2015 letter exempting large portions of a production responsive to FOIPA Request Number 1253741-000, which we filed on behalf of Tariq Razak on February 18, 2014.¹ The Department produced thirteen highly redacted pages in response to Mr. Razak's request. For the reasons set forth below, we appeal all of the exemptions upon which the Department declined to disclose responsive information, and respectfully request reconsideration of the Department's initial exemption determinations.

I. The Department Has Failed to Substantiate Use of Exemptions

The Department cites sections (b)(6), (b)(7)(c), (b)(7)(e), and (j)(2) to justify withholding significant portions of the 13-page production. Review of the production, however, reveals that these exemptions were not properly asserted and that redactions were over broadly applied.

The Department asserts (b)(6), which relates to personnel and medical files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. 5 U.S.C. § 552(b)(6). This exemption is intended to protect an individual's private information from disclosure to third parties. Here, however, the Department invoked (b)(6) to justify denying Mr. Razak access to records that have no plausible nexus to a third party's personnel and medical files. For example, page six of the production states: "After reviewing the lead and

¹ Copies of our February 18, 2014 request and the Department's February 13, 2015 response are attached hereto as Exhibits A and B, respectively.

information obtained from data checks[,] Writer has found no evidence of the Subject's being involved in terrorism or criminal activity. Writer believes the lead was sent only because [REDACTED (b)(6) and (b)(7)(c)]." The Writer's conclusion as to why a lead was sent on Mr. Razak has no connection to a third party's personnel and medical files and, thus, this information was improperly redacted. See *Local 598 v. Dept. of Army Corps of Eng'rs*, 841 F.2d 1459, 1463 (9th Cir. 1988) ("In the Act generally, and particularly under Exemption (6), there is a strong presumption in favor of disclosure.") (emphasis added).

The Department also improperly asserts (b)(7)(c) and (b)(7)(e). Exemption (b)(7)(c) applies to records or information compiled for law enforcement purposes, the disclosure of which could be reasonably expected to constitute an unwarranted invasion of personal privacy. 5 U.S.C. § 552(b)(7)(c). Exemption (b)(7)(e), in turn, protects from disclosure law enforcement guidelines or techniques. *Id.* at § 552(b)(7)(c). The Department, however, invoked these exemptions to justify redacting materials related to incidents at which Mr. Razak was present. For example, on page seven of the production, the Department redacted the entire narrative regarding the Writer's visit to Mr. Razak's home based on (b)(6) and (b)(7)(e). Also on page seven, the Department redacted portions of statements that Mr. Razak himself made to the Writer based on the same exemptions. See, e.g., p. 7 ("He said he was at the Santa Ana train station [REDACTED] on that day. . . . He said he was waiting [REDACTED]. He said he was pacing and looking around the station [REDACTED]. He said he drives [REDACTED] everyday since he is not working.") None of this information risks invading a third party's personal privacy, nor does it relate to law enforcement guidelines or techniques. Accordingly, it was improperly redacted and should have been disclosed. See *Local 598*, 841 F.2d at 1463 (FOIA "embodies a strong policy of disclosure and places a duty to disclose on federal agencies. . . . 'disclosure, not secrecy, is the dominant objective of the Act.'") (internal citation omitted). In addition, the FBI's response fails to cite any federal law the enforcement of which is related to the withheld information. Therefore, redactions based on any of the subsections of exemption 7 would be unsupported here. See *ACLU v. FBI*, Case No. 10-03759 RS, Dkt. 128 (N.D. Cal. Mar. 23, 2015).

II. The Department Has Failed to Produce All Segregable Portions

FOIA requires that "[a]ny reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection." 5 U.S.C. § 552(b). Review of the heavily redacted production indicates that the Department overly exempted information and did not produce all segregable portions. For example, on pages 5 through 7 of the production, the "Instruction" specifics are redacted wholesale on five different occasions. In other portions of the production, however, the Department properly segregated non-exempt portions of the "Instruction" information from exempt portions. As an additional example, on page seven of the production, the Department



redacted the entire narrative regarding the Writer's visit to Mr. Razak's home and did not segregate any non-exempt portions.

These are just a few examples of the overly redacted nature of the production. Thus, to the extent the Department stands by its reliance on the exemptions, it is nonetheless required to disclose the segregable non-exempt portions of the production.

III. Conclusion

We respectfully request re-consideration of the Department's redaction determinations. We also respectfully request that the Department re-review and ensure that all reasonably segregable portions of the production are released.

Thank you for your attention to this appeal. Please do not hesitate to contact me at (415) 848-7711 or by email at yamans@advancingjustice-alc.org if you have any questions. We look forward to your prompt response.

Sincerely,



Yaman Salahi
Staff Attorney

Enclosures



EXHIBIT 4



U.S. Department of Justice
Office of Information Policy
Suite 11050
1425 New York Avenue, NW
Washington, DC 20530-0001

Telephone: (202) 514-3642

Yaman Salahi, Esq.
Advancing Justice - Asian Law Caucus
55 Columbus Avenue
San Francisco, CA 94111
yamans@advancingjustice-alc.org

Re: Appeal No. AP-2015-03075
Request No. 1253741
MWH:JMB

VIA: E-mail

Dear Mr. Salahi:

You appealed on behalf of your client, Tariq Razak, from the action of the Federal Bureau of Investigation on his request for access to records concerning himself. I note that your appeal concerns only the withholdings made by the FBI.

After carefully considering your appeal, I am affirming the FBI's action on your client's request. In order to provide you with the greatest possible access to responsive records, your request was reviewed under both the Privacy Act of 1974 and the Freedom of Information Act. I have determined that the records responsive to your client's request are exempt from the access provision of the Privacy Act. See 5 U.S.C. § 552a(j)(2); see also 28 C.F.R. § 16.96 (2014). For this reason, I have reviewed your appeal under the FOIA.

The FOIA provides for disclosure of many agency records. At the same time, Congress included in the FOIA nine exemptions from disclosure that provide protection for important interests such as personal privacy, privileged communications, and certain law enforcement activities. The FBI properly withheld certain information because it is protected from disclosure under the FOIA pursuant to:

5 U.S.C. § 552(b)(6), which concerns material the release of which would constitute a clearly unwarranted invasion of the personal privacy of third parties;

5 U.S.C. § 552(b)(7)(C), which concerns records or information compiled for law enforcement purposes the release of which could reasonably be expected to constitute an unwarranted invasion of the personal privacy of third parties; and

5 U.S.C. § 552(b)(7)(E), which concerns records or information compiled for law enforcement purposes the release of which would disclose techniques and procedures for law enforcement investigations or prosecutions.

- 2 -

Additionally, to the extent that your client's request seeks access to records that would either confirm or deny an individual's placement on any government watch list, the FBI properly refused to confirm or deny the existence of any records responsive to your client's request because the existence of such records is protected from disclosure pursuant to 5 U.S.C. § 552(b)(7)(E). FOIA Exemption 7(E) concerns records or information compiled for law enforcement purposes the release of which would disclose techniques and procedures for law enforcement investigations or prosecutions. This response should not be taken as an indication that records do or do not exist. Rather, this is the standard response made by the FBI.

Please be advised that this Office's decision was made only after a full review of this matter. Your appeal was assigned to an attorney with this Office who thoroughly reviewed and analyzed your appeal, your client's underlying request, and the action of the FBI in response to your client's request.

If your client is dissatisfied with my action on your appeal, the FOIA permits him to file a lawsuit in federal district court in accordance with 5 U.S.C. § 552(a)(4)(B).

For your information, the Office of Government Information Services (OGIS) offers mediation services to resolve disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. Using OGIS services does not affect your client's right to pursue litigation. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, Room 2510, 8601 Adelphi Road, College Park, Maryland 20740-6001; e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

Sincerely,

5/21/2015

X 

Sean R. O'Neill
Chief, Administrative Appeals Staff
Signed by: O'Neill, Sean (OIP)

EXHIBIT 5



June 25, 2014

Via Certified U.S. Mail, Return Receipt Requested

Federal Bureau of Investigation
Attn: Privacy Act Request
Record/Information Dissemination Section
170 Marcel Drive
Winchester, VA 22602-4843

Federal Bureau of Investigation – Los Angeles Field Office
Attn: Privacy Act Request
Record/Information Dissemination Section
Suite 1700, FOB 11000 Wilshire Blvd
Los Angeles, CA 90024-3672

Mr. Kshemendra Paul
Program Manager, Information Sharing Environment
Office of the Director of National Intelligence
Attn: Program Manager, Information Sharing Environment
Washington DC, 20511

Orange County Intelligence Assessment Center
PO Box 1755
Santa Ana, CA 92702-1755

Re: Privacy Act Request for Expungement of Records for Mr. Tariq Razak

Dear Sir/Madam:

This letter constitutes a request for expungement of records made pursuant to the Privacy Act, 5.U.S.C. § 552a(d)(2), (e)(1), (e)(5), and (e)(7) on behalf Mr. Tariq Razak for all records, including but not limited to Suspicious Activity Reports, pertaining to or referencing Mr. Razak. Mr. Razak is being represented in this matter by attorneys at the American Civil Liberties Union of Northern California (“ACLU-NC”) and Advancing Justice-Asian Law Caucus (“ALC”). Please find his Certification of Identity and Authorization to Release Information enclosed herewith.

We request, based on the Privacy Act, 5 U.S.C. §§ 552a(e)(1), (e)(5), (e)(7), (d)(1) and (d)(2), the opportunity to review any and all records maintained by the Federal Bureau of Investigation (“FBI”), the Orange County Intelligence Assessment Center (“OCIAC”), or the Information Sharing Environment (“ISE”) (collectively, the “Agencies”) containing information pertaining to Mr. Razak, and to amend or expunge all records that describe Mr. Razak’s exercise of rights guaranteed by the First Amendment (including free exercise of religion), describe conduct that does not support reasonable suspicion of criminal activity, or describe conduct that does not implicate criminal conduct in any way. To be clear, this includes, but is not limited to: (i) any such records maintained by the Agencies, whether or not they are in the Agency’s system of records, as the term is defined in 5 U.S.C. § 552a(a)(5), and whether or not they are traceable by Mr. Razak’s name or some other identifying characteristic and (ii) any such records maintained by the Agencies from which records described above are retrievable through a “cross reference” search for files that mention Mr. Razak. *See MacPherson v. IRS*, 803 F.2d 479, 481 (9th Cir. 1986) (“Section (e)(7) requires only that the record be maintained by an agency that keeps a system of records, not that the record be a part of that system”) (emphasis in original).

The following information may assist you in searching for records pertaining to Mr. Razak.

- We have reason to believe a Suspicious Activity Report (SAR) concerning Mr. Razak was filed with the Orange County Intelligence Assessment Center and/or the F.B.I. on or around May 16, 2011 by Officer J. Gallardo, #3203, a Terrorism Liaison Officer at the Santa Ana Police Department. Per records of the Santa Ana Police Department, the report was given Case No. 2011-15770. The factual synopsis is “Male of Middle Eastern descent observed surveying entry/exit points.” The person who filed the report with Santa Ana PD is Karina De La Rosa, a Security Officer at the Santa Ana Train Depot at 1000 E. Santa Ana Boulevard, Santa Ana, CA 92702. Officer Gallardo’s report states, in part, “At approximately 1020 hours, Karina took the elevator from the second floor to the first floor. In the elevator with Karina was a male between male of who Karina believed was of Middle Eastern descent. Karina’s suspicion became aroused because the male appeared observant of his surroundings and was constantly surveying all areas of the facility. The male’s appearance was neat and clean with a closely cropped beard, short hair wearing blue jeans and a blue plaid shirt. Upon exiting the elevator, Karina observed the male meticulously study the entry/exit points, different lobby areas of the train station where large groups of passengers gather. The male then went to the north end of the station where male and female restrooms are located and stood by outside the restrooms. Minutes later, a female wearing a white burka head dress, black pants and a blue shirt exited the restroom. The two individuals then both exited the train station out of the north doors, entered a white 2007 Honda Accord (CA Lic. [redacted]) and left the Train Station in an unknown direction.”



Based on this record, we have reason to believe that the Agencies, or one of the Agencies, maintains records related to Mr. Razak that may describe his protected First Amendment activities. Since Mr. Razak's activities were lawful, we have reason to believe that records maintained by one or more of the Agencies related to Mr. Razak are not based on allegations of criminal conduct, nor supported by reasonable suspicion of criminal conduct. Any such records that bear a title or marking that would tend to suggest Mr. Razak's actions had a potential nexus to terrorism would be inaccurate, irrelevant, and incomplete and unnecessary to any legitimate law enforcement purpose. Therefore, we request all such records be expunged or amended to omit all references to Mr. Razak, any identifying characteristics, and his activities, pursuant to §§ 552a(e)(1), (e)(5), (e)(7), and (d)(2) of the Privacy Act.

If this request is denied in whole or in part, we request that you justify any refusals to expunge the records by reference to specific provisions of the Privacy Act. We reserve the right to appeal a decision to deny Mr. Razak's request.

Mr. Razak has also filed a FOIA/Privacy Act requesting disclosure of similar records, under FOIPA Request No. 1253741-000.

Please direct all correspondence regarding this request to:

Yaman Salahi
Advancing Justice—Asian Law Caucus
55 Columbus Ave.
San Francisco, CA 94111

If you have any questions, I can be reached by phone at (415) 848-7711.

Sincerely,

Yaman Salahi
Staff Attorney

Enclosures



1 MORGAN, LEWIS & BOCKIUS LLP
 2 Stephen Scotch-Marmo (admitted *pro hac vice*)
 3 stephen.scotch-marmo@morganlewis.com
 4 Michael James Ableson (admitted *pro hac vice*)
 5 michael.ableson@morganlewis.com
 6 101 Park Avenue
 7 New York, NY 10178
 8 Telephone: (212) 309-6000; Facsimile: (212) 309-6001

9 AMERICAN CIVIL LIBERTIES UNION
 10 FOUNDATION OF NORTHERN CALIFORNIA
 11 Linda Lye (SBN 215584), llye@aclunc.org
 12 Julia Harumi Mass (SBN 189649), jmass@aclunc.org
 13 39 Drumm Street
 14 San Francisco, CA 94111
 15 Telephone: (415) 621-2493; Facsimile: (415) 255-8437

16 ASIAN AMERICANS ADVANCING
 17 JUSTICE - ASIAN LAW CAUCUS
 18 Christina Sinha (SBN 278893), christinas@advancingjustice-alc.org
 19 55 Columbus Avenue
 20 San Francisco, CA 94111
 21 Telephone: (415) 848-7711; Facsimile: (415) 896-1702

22 *Attorneys for Plaintiffs*

23 UNITED STATES DISTRICT COURT
 24 NORTHERN DISTRICT OF CALIFORNIA
 25 SAN FRANCISCO DIVISION

26 WILEY GILL; JAMES PRIGOFF; TARIQ
 27 RAZAK; KHALID IBRAHIM; and AARON
 28 CONKLIN,

Plaintiffs,

v.

DEPARTMENT OF JUSTICE; LORETTA
 LYNCH, in her official capacity as the
 Attorney General of the United States;
 PROGRAM MANAGER – INFORMATION
 SHARING ENVIRONMENT;
 KSHEMENDRA PAUL, in his official
 capacity as the Program Manager of the
 Information Sharing Environment,

Defendants.

Case No. 3:14-cv-03120-RS-KAW

**DECLARATION OF JAMES PRIGOFF
 IN SUPPORT OF PLAINTIFFS’
 MOTION FOR SUMMARY
 JUDGMENT AND PLAINTIFFS’
 OPPOSITION TO DEFENDANTS’
 MOTION FOR SUMMARY
 JUDGMENT**

Hearing Date: December 8, 2016
 Time: 1:30 pm
 Judge: Hon. Richard Seeborg
 Courtroom: 3, 17th Floor
 Date of Filing: July 10, 2014
 Trial Date: None Set

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

I, James Prigoff, declare as follows:

1. I am one of the Plaintiffs in the above-titled action. I make this Declaration in support of Plaintiffs’ Motion for Summary Judgment and Plaintiffs’ Opposition to Defendants’ Motion for Summary Judgment. I make this Declaration of my own personal knowledge, and if called to testify, I could and would testify competently to the matters stated herein.

2. I am a United States citizen and I reside in Sacramento, California. I am 88 years old.

3. I am a retired business executive. I served as Senior Vice President of the Sara Lee Corporation and President of a division of Levi Strauss & Co.

4. I am also a professional photographer. I have been a photographer for most of my life. My specialty is photographing murals, graffiti and other public art. I have published several books of photographs and have been included in a dozen more. I have a collection of over 80,000 photographic slides. My work has been exhibited at the Smithsonian and in galleries from Berlin to Vancouver; I have lectured on photography and public art all over the world. In 2012, based on my 40 years of documenting public art, the Estria Foundation named me an “Urban Legend.”

5. It has been my experience that some of my principal photographic subjects (public art and graffiti) are frequently located on infrastructure (i.e., bridges, tunnels, electrical grids, and so forth).

6. In early June 2004, I was the keynote speaker at the National Conference on Mural Art in Philadelphia, Pennsylvania. While in Philadelphia, I updated my photographic collection of that city’s public art. After speaking at the conference, I drove to New York to see my son and also to update my photographic collection of that city’s public art. Then I drove to Boston, Massachusetts, where I made a presentation at a show of my work in Cambridge. While in Boston, I also took the opportunity to document the public art of Boston.

7. As part of this documentation effort, I sought to photograph a famous piece of public art known as the “Rainbow Swash.” The Rainbow Swash is located in the Dorchester

1 neighborhood of Boston. The artwork is painted on a natural gas storage tank, which is
2 surrounded by a chain link fence. The Rainbow Swash is highly visible to commuters from the
3 local expressway.

4 8. In order to photograph the Rainbow Swash, I drove my rental car to a public area
5 outside the fence surrounding the artwork, and set up my equipment. I chose this location in part
6 because of favorable lighting conditions. From this location, the sun was behind me and casting
7 its light on the Rainbow Swash. Before I could take any photographs, two private security guards
8 came out from inside the fenced area and told me I was not allowed to photograph the Rainbow
9 Swash. The guards claimed the area was private property. When I pointed out to the guards that I
10 was not on private property, they still insisted that I could not take any photographs.

11 9. To avoid a confrontation with the guards, I did not take any photographs of the
12 Rainbow Swash from this public area and stopped attempting to do so. I got back in my car and
13 drove to another public location outside the fenced area. However, the guards followed me to this
14 new location, so I left this location as well without taking any photographs. I did not provide any
15 identifying information to the guards at any point.

16 10. I drove to the other side of the Rainbow Swash, and this time, the guards did not
17 follow me. I was able to take some photographs of the Rainbow Swash from this third vantage
18 point. However, the lighting conditions were significantly inferior to the conditions at the first
19 two locations, as I now had to take the photograph into the sunlight. The resulting photographs
20 were of notably poorer aesthetic quality than if I had been able to photograph from either of the
21 first two sites.

22 11. I subsequently discovered several excellent photographs of the Rainbow Swash
23 online, including on the Wikipedia entry for the Rainbow Swash. These widely available
24 photographs of this national landmark were taken from vantage points closer than the two
25 locations from which I attempted to take, and the third location from which I actually took,
26 photographs of the Rainbow Swash.

27
28

1 12. After my trip to Boston, I returned to my home in Sacramento, California. A few
2 months later, on or about August 19, 2004, I came home one day to find a business card affixed to
3 my door. It was the business card of Agent A. Ayaz of the Joint Terrorism Task Force. On the
4 back of the card was a handwritten note, stating, “Mr. Prigoff, please call me. Thanks.” A true
5 and correct copy of the front and back of the business card I found on my door is attached as
6 Exhibit 1 to this declaration.

7 13. Later, I learned from a neighbor across the street that two agents had knocked on
8 her door and asked about me.

9 14. I called Mr. Ayaz, who asked if I had been to Boston. I realized that Mr. Ayaz was
10 referring to my efforts to photograph the Rainbow Swash, and I explained what happened on that
11 occasion.

12 15. I believed that the security guards at the Rainbow Swash site had submitted a
13 report about me that included my rental car information, and that is how I was traced from Boston
14 to my home in Sacramento.

15 16. My beliefs were confirmed when I submitted a Freedom of Information Act
16 (“FOIA”) and Privacy Act request to the FBI on July 9, 2014, and received redacted versions of
17 three reports, each titled “SUSPICIOUS ACTIVITY,” concerning my attempt to photograph the
18 Rainbow Swash. True and correct copies of the documents I received from the FBI in response to
19 my FOIA and Privacy Act request (with personal identifying information about me redacted), and
20 which I have personally reviewed, are attached as Exhibits 2, 3, and 4 to this declaration. *See Exs.*
21 2 (“SUSPICIOUS ACTIVITY” report on James Burt Prigoff, dated June 21, 2004), 3
22 (“SUSPICIOUS ACTIVITY” report on James Burt Prigoff, dated October 18, 2004) & 4
23 (“SUSPICIOUS ACTIVITY” report on James Burt Prigoff, dated November 8, 2004).

24 17. Note that, despite my repeated efforts, even the redacted “SUSPICIOUS
25 ACTIVITY” reports I received in response to my FOIA and Privacy Act request do not constitute
26 my entire FBI file.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

(a) I received a response from the FBI regarding my FOIA and Privacy Act request, dated March 24, 2015, which provides the three “SUSPICIOUS ACTIVITY” reports discussed above, and also noted that deletions had been made in the reports. A true and correct copy of the letter I received from the FBI, and which I have personally reviewed, is attached as Exhibit 5 to this declaration. *See* Ex. 5 (letter from David M. Hardy, FBI, to Yaman Salahi, Asian Americans Advancing Justice, dated March 24, 2015).

(b) The numerous redactions to my “SUSPICIOUS ACTIVITY” reports include a paragraph that states:

An ACS check of JAMES PRIGOFF revealed the following references:

- [REDACTED] in 1983
- [REDACTED] in 1991
- [REDACTED] in 1992
- [REDACTED] in 1992

Ex. 2 at 2; *see also* Ex. 4 at 2. Thus, according to the redacted reports that were provided to me, at least four other FBI files exist that refer to me.

(c) The ground provided by the FBI for its failure to produce these other four files is 5 U.S.C. § 552(b)(7)(E):

records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information . . . would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

See Ex. 2 at 2 (redactions annotated b7e).

(d) On May 19, 2015, I appealed the incomplete production of my FBI files. A true and correct copy of the letter I sent to the DOJ’s Office of Information Policy, and

1 which I have personally reviewed, is attached as Exhibit 6 to this declaration. *See* Ex. 6
2 (letter from Yaman Salahi to Director, Office of Information Policy, DOJ, dated May 19,
3 2015). In that letter, I cited the redacted passage quoted in the previous paragraph and
4 noted that the missing reports “clearly fall within the parameters of [my FOIA]
5 request” *Id.* at 1-2. I also challenged the exemption based on § 552(b)(7)(E):

6 Here, the Department invoked (b)(7)(E) to justify redacting materials related to
7 incidents that occurred *over two to three decades ago*, specifically, all information
8 relating to ACS references for Mr. Prigoff from 1983, 1991, and 1992. Such
9 information cannot plausibly be the subject of law enforcement investigations or
10 prosecutions. In addition, given that Mr. Prigoff has not engaged in any criminal
11 activity, it is highly unlikely that the Department is able to meet its burden of
12 showing that the redacted material relates to enforcement of a particular federal
13 law.

14 *Id.* at 2-3 (original emphasis).

15 (e) On January 27, 2016, I received a response from the DOJ’s Office of
16 Information Policy denying my appeal of the incomplete production of my FBI files. A
17 true and correct copy of the letter I received from the DOJ’s Office of Information Policy,
18 and which I have personally reviewed, is attached as Exhibit 7 to this declaration. *See* Ex.
19 7 (letter from Sean R. O’Neill, Office of Information Policy, DOJ, to Yaman Salahi, dated
20 January 27, 2016).

21 18. My FOIA and Privacy Act request to the FBI, dated July 9, 2014, was also
22 addressed to the Office of the Director of National Intelligence (“ODNI”).

23 (a) The ODNI responded to me by letter dated January 8, 2015. A true and
24 correct copy of the ODNI’s response, which I have personally reviewed, is attached as
25 Exhibit 8. *See* Ex. 8 (letter from Jennifer Hudson, Director, Information Management
26 Division, ODNI, to Yaman Salahi, dated January 8, 2015). In its letter, the ODNI stated
27
28

1 that “it could neither confirm nor deny the existence or nonexistence [in its classified
2 files] of any information responsive to your request.” *Id.*

3 (b) I appealed the ODNI’s determination on February 20, 2015. On September
4 15, 2015, the ODNI denied that appeal. A true and correct copy of the ODNI’s appeal
5 denial, which I have personally reviewed, is attached as Exhibit 9. *See* Ex. 9 (letter from
6 Mark W. Ewing, Office of the Director of National Intelligence, to Yaman Salahi, dated
7 September 15, 2015).

8 19. I am very upset that I was tracked cross-country from Boston to Sacramento, and
9 contacted by law enforcement agents at my home, over my effort to engage in photography from
10 a public location. Indeed, one of the “SUSPICIOUS ACTIVITY” reports notes that I rented the
11 car (that I was using when trying to photograph the Rainbow Swash) “in downtown Philadelphia
12 on 6/3/2004 and returned to the Philadelphia airport on 6/13/2004 with an accumulation of 1,280
13 miles.” Ex. 1. This shows that the FBI was carefully monitoring my whereabouts.

14 20. I am also very upset that law enforcement agents questioned at least one of my
15 neighbors about me. I believe this questioning created a negative and strong implication that I
16 must have engaged in some type of misconduct. *See also* Ex. 3 at 3 (“PRIGOFF was also upset
17 when he learned, through his neighbors, that investigators visited his residence.”).

18 21. The FBI has maintained the “SUSPICIOUS ACTIVITY” reports about me for
19 over a decade now. These three reports, dated June 21, 2004, October 18, 2004, and November 8,
20 2004, all pertain to activity in the spring of 2004. Yet the FBI produced them to me by letter dated
21 March 24, 2015. *See* Ex. 5. Thus, the FBI has clearly maintained these reports in some kind of
22 database for over ten years. This is so even though the second and third SARs state that the matter
23 is concluded. *See* Ex. 3 at 4 (“Absent the development of additional derogatory information
24 attributed to PRIGOFF, Sacramento views no basis for further investigation, and therefore
25 considers this lead covered.) & Ex. 4 at 2 (“In view of the explanation provided this, Boston
26 considers this lead covered.”).

1 22. As a result of the “SUSPICIOUS ACTIVITY” reports about me, and their
2 inclusion in the FBI’s database, my reputation has been injured because I have been branded as a
3 person who has engaged in some type of misconduct, even though I was simply attempting to
4 take photographs from a public area. Note that the October 18, 2004 “SUSPICIOUS
5 ACTIVITY” report concludes: “Absent the development of additional derogatory information
6 attributed to PRIGOFF, Sacramento . . . considers this lead covered.” Ex. 4 at 3 (emphasis added)

7 23. In addition, as a result of the inclusion of this information about me in the FBI’s
8 database, my privacy has been invaded because any person with access to the database has access
9 to information about me, even though I was simply attempting to take photographs from a public
10 area.

11 24. I have reviewed the “Criteria Guidance” contained in each of the three versions of
12 the “Functional Standard” for Suspicious Activity Reporting issued by the Program Manager for
13 the Information Sharing Environment (“PM-ISE”), and attached as Exhibit 10 to this declaration.
14 The “Criteria Guidance” lists categories of behavior that presumably satisfies the PM-ISE’s
15 definition of what constitutes suspicious activity. Photography of infrastructure is listed in each of
16 the three versions. I have also reviewed a document that is titled “Potential Indicators of Terrorist
17 Activities Related to the General Public” with the seal of the Bureau of Justice Assistance and
18 that is attached as Exhibit 11 to this declaration. This document lists as one potential indicator of
19 terrorist activity “people acting suspiciously.”

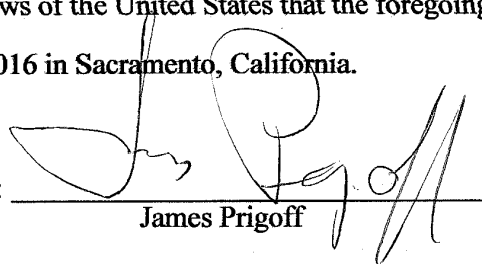
20 25. I continue to be an active photographer and often take pictures of architectural
21 structures and post offices, among other sites that could be described as infrastructure. Taking
22 photographs of infrastructure falls under one or more of the behavioral categories identified by
23 the PM-ISE. Although I do not view taking photographs as suspicious, the security guards at the
24 Rainbow Swash apparently did and so my activities as a photographer could, in the eyes of at
25 least some people, fall under the label “people acting suspiciously.” As a result, I fear that I am
26 likely to be the subject of yet another SAR in the future. I further fear that my efforts to take
27 photographs of architectural structures, post offices (which frequently contain murals from the
28

1 WPA period) or other sites that could be described as infrastructure will be hindered again in the
2 future, and I will be either prevented from taking photographs or forced to take photographs of
3 lesser quality, as occurred to me at the Rainbow Swash.

4 26. I remain deeply troubled by what may result from the collection, maintenance, and
5 dissemination in a database of reports describing me as engaging in suspicious activity.

6 27. I believe that the defendants in this case would have benefited from input from the
7 public on the standard for suspicious activity reporting. I would have wanted the defendants to
8 know when they adopted their standard for suspicious activity reporting that a standard that does
9 not require reasonable suspicion of criminal activity harms innocent people, like me, who have
10 not engaged in any wrongdoing: It makes us the targets of law enforcement scrutiny, puts our
11 information in government databases, and adversely affects our reputations by identifying us as
12 individuals who have engaged in conduct with a potential nexus to terrorism. I would also have
13 wanted defendants to know the specific facts of my case so that they could understand the factual
14 basis for my concerns. I was not aware that defendants sought input on the standard for
15 suspicious activity reporting. As a result, I did not have an opportunity to share my perspective or
16 the factual basis for my concerns.

17
18 I declare under penalty of perjury under the laws of the United States that the foregoing is
19 true and correct. Executed this 15 day of Sept 2016 in Sacramento, California.

20
21 By: 
22 James Prigoff

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

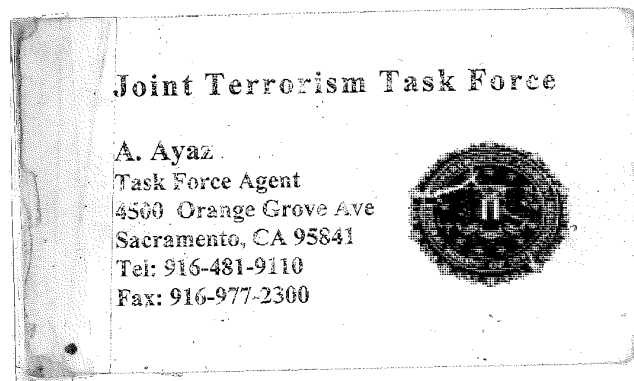
FILER'S ATTESTATION

I, Phillip J. Wiese, am the ECF user whose identification and password are being used to file this DECLARATION OF JAMES PRIGOFF IN SUPPORT OF PLAINTIFFS' MOTION FOR SUMMARY JUDGMENT AND PLAINTIFFS' OPPOSITION TO DEFENDANTS' MOTION FOR SUMMARY JUDGMENT. Pursuant to L.R. 5-1(i)(3), I hereby attest that concurrence in the electronic filing of this document has been obtained from each of the other signatories.

Dated: September 22, 2016

By /s/ Phillip J. Wiese
Phillip J. Wiese

EXHIBIT 1



8-19-04
1:30 PM

MR. PRIGOFF, PLEASE
CALL ME. THANKS

EXHIBIT 2

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-25-2014 BY NSICG/T97M74K90

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 06/21/2004

To: Boston
Sacramento

From: Boston

CT-3

Contact: [Redacted]

b6
b7C

Approved By: [Redacted]

Drafted By: [Redacted]

Case ID #: [Redacted]

(Pending) -2924
(Pending) -144

b7E

Title: SUSPICIOUS ACTIVITY
JAMES BURT PRIGOFF

DEMOCRATIC NATIONAL CONVENTION
BOSTON, MA. JULY 2004
00: BOSTON

✓ pw

Synopsis: On 6/11/2004 the male operator of a rental car stopped his vehicle near a natural gas tank in Boston and began taking photographs of the facility.

Enclosure(s): a BOSTON POLICE DEPARTMENT (BPD) report form (CC#040-3006167) dated 6/11/2004

a PENNSYLVANIA BUREAU OF MOTOR VEHICLES vehicle registration check on PENNSYLVANIA registration EZX-9873

a copy of California Drivers' License [Redacted], with Image of JAMES BURT PRIGOFF

Details: On 6/11/2004 the BOSTON POLICE DEPARTMENT (BPD) notified the writer of an incident reported to that Department relative to the following incident:

On 6/11/2004 members of the KEYSpan SECURITY reported that about 10:10 AM that date, a white, non-Hispanic male, late 50's or early 60's, 5'9" - 5'10", weight in proportion to height, dark hair, mustache drove a vehicle up onto a private road which was marked No Trespassing, leading

[Redacted]

2924

b7E

173 pwo. cc

To: Boston From: Boston
Re: [redacted] 06/21/2004

b7E

to a natural gas storage tank facility at 200 Victory Road, Dorchester, Massachusetts and began taking photographs of the facility.

As the security staff advised this male that he was not allowed to take photographs of the facility he became extremely belligerent telling them that he could take photos of anything he wanted. This male then drove to another road on this facility and was again told that he was trespassing. He again became belligerent and finally left the scene.

The vehicle the subject drove, a 2004 Chevrolet sedan, grey in color, Pennsylvania Registration EZX-9873 is registered to the AVIS RAC SYS INC. PV Holding Company, 300 Cente Pointe Drive, Virginia Beach, Va. 23462.

Further inquiry revealed that this vehicle had been rented in downtown Philadelphia on 6/3/2004 and returned to the Philadelphia airport on 6/13/2004 with an accumulation of 1,280 miles. The vehicle had been rented by one JAMES PRIGOFF D.O.B. [redacted] of [redacted], Sacramento, California 95835 under California Operator's License [redacted].

An ACS check of JAMES PRIGOFF revealed the following references:

- [redacted] in 1983
- [redacted] in 1991
- [redacted] in 1992
- [redacted] in 1992

b7E

To: Boston From: Boston
Re: [redacted] 06/21/2004

b7E

LEAD(s) :

Set Lead 1: (Action)

SACRAMENTO

AT AT SACRAMENTO

Sacramento Field Office is requested to conduct an interview of JAMES PRIGOFF born [redacted] of [redacted] Drive, Sacramento, California 95825 as to the purpose of his trip to Massachusetts and in particular his presence in BOSTON and in the area of the natural gas storage tanks.

♦♦

EXHIBIT 3

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 10/18/2004

To: Boston

Attn: CT-3

SSA [redacted]
SA [redacted]

b6
b7C

From: Sacramento

JTF

Contact: TFA [redacted]

Approved By: [redacted]

Drafted By: [redacted] 292aa04.ec

Case ID #: [redacted] (Pending)
[redacted] (Pending)

b7E

Title: SUSPICIOUS ACTIVITY
JAMES BURT PRIGOFF

Synopsis: To report results of [redacted] investigation.

Reference: [redacted]

b7E

Details: After interviewing captioned subject, Sacramento has determined that captioned subject is not [redacted]
[redacted]

By way of background, on 6/11/2004, the BOSTON POLICE DEPARTMENT (BPD) notified the Boston FBI division of an incident reported to that Department relative to the following incident:

On 6/11/2004 members of the KEYSpan SECURITY reported that about 10:10 AM that date, a white, non-Hispanic male, late 50's or early 60's, 5'9" - 5'10", weight in proportion to height, dark hair, mustache drove a vehicle up onto a private road which was marked No Trespassing, leading to a natural gas storage tank facility at 200 Victory Road, Dorchester, Massachusetts and began taking photographs of the facility.

As the security staff advised this male that he was not allowed to take photographs of the facility he became extremely belligerent telling them that he could take photos of anything he wanted. This male then drove to another road on this facility and was again told that he was trespassing. He again became belligerent and finally left the scene.

To: Boston From: Sacramento
Re: [redacted] 10/18/2004

b7E

The vehicle the subject drove, a 2004 Chevrolet sedan, grey in color, Pennsylvania Registration EZX-9873 is registered to the AVIS RAC SYS INC. PV Holding Company, 300 Cente Pointe Drive, Virginia Beach, Va. 23462.

Further inquiry revealed that this vehicle had been rented in downtown Philadelphia on 6/3/2004 and returned to the Philadelphia airport on 6/13/2004 with an accumulation of 1,280 miles. The vehicle had been rented by one JAMES PRIGOFF D.O.B. [redacted] of [redacted], Sacramento, California 95835 under California Operator's License [redacted].

An ACS check of JAMES PRIGOFF revealed the following references:

- [redacted] in 1983
- [redacted] in 1991
- [redacted] in 1992
- [redacted] in 1992

b7E

Set forth below is the telephonic interview that Writer conducted with PRIGOFF.

On 08/23/2004, James PRIGOFF, DOB [redacted], California DL# [redacted], residence address [redacted], Sacramento, CA 95825, residence telephone [redacted], was telephonically interviewed by Writer. Writer contacted PRIGOFF to determine PRIGOFF'S possible involvement [redacted]. After being advised of the nature of the interview and the identity of the interviewing agent, PRIGOFF provided the following information:

b7E

PRIGOFF is an artist who was attending the National Conference for Mural Art in Philadelphia, PA, and identified himself as the keynote speaker at this event. From Philadelphia, PRIGOFF drove to New York to visit his son. PRIGOFF then drove to Boston, MA, to attend what he described as his own art show at the Cambridge Art Gallery, where his collection of art is known as "The Walls of Heritage and the Walls of Pride." PRIGOFF was also a guest speaker at that event. Just prior to arriving in Boston from New York, PRIGOFF noticed a tower, presumably a water tower, with public art displayed on it. PRIGOFF intended to get a closer view of the art but was denied access by the towers security officers, which greatly irritated him. PRIGOFF stated that he simply desired to take a photo of the art work on the tower.

To: Boston From: Sacramento
Re: 10/18/2004

b7E

PRIGOFF stated that he is known internationally as an artist and has photographed a number of tanks and towers throughout the country.

Note: PRIGOFF spoke in a generally agitated tone during his conversation with Writer. PRIGOFF stated that he normally does not communicate with Federal Agents but would make an exception during this occasion, since he found the topic of the inquiry to be "amusing." PRIGOFF was also upset when he learned, through his neighbors, that investigators visited his residence. (Prior to the telephonic conversation with PRIGOFF, investigators attempted to contact him at his residence without success). PRIGOFF stated that investigators inquiry of him was a "waste of taxpayers money."

Absent the development of additional derogatory information attributed to PRIGOFF, Sacramento views no basis for further investigation, and therefore, considers this lead covered.

To: Boston From: Sacramento
Re: 10/18/2004

b7E

LEAD(s) :

Set Lead 1: (Info)

BOSTON

AT BOSTON

Provided for information.

◆◆

EXHIBIT 4

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-25-2014 BY NSICG/F97M7AK9D
(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 11/08/2004

To: Boston

From: Boston

CT-3

Contact: [Redacted]

b6
b7C

Approved By: [Redacted]

Drafted By: [Redacted]

Case ID #:

[Redacted]

(Pending) - 3402

b7E

Title: SUSPICIOUS ACTIVITY

Synopsis: Results of [Redacted] of an incident on 6/11/2004 where JAMES PRIGOFF took photographs of the Dorchester Gas Tank.

Details: On 6/11/2004 a male, later identified as JAMES PRIGOFF DOB [Redacted] of [Redacted], Sacramento, California 95835, has stopped the vehicle he was operating, on a private road, marked with No Trespassing signs, at the Dorchester Gas Tank facility at 200 Victory Road, Boston, Massachusetts, and began taking photographs of the facility.

At Boston's request, on 8/23/2004 an agent of the FEDERAL BUREAU OF INVESTIGATION'S (FBI) Sacramento Office conducted an interview of JAMES PRIGOFF, during which PRIGOFF described himself as being an internationally known artist who was attending the National Conference for Mural Art in Philadelphia where he was a keynote speaker. From Philadelphia, PRIGOFF drove to New York to visit his son and then drove to Boston, Massachusetts to attend what he described as his "own art show" at the Cambridge Art Gallery where his collection of art is known as "The Walls of Heritage and the Walls of Pride". He advised that he was also a guest speaker at that event.

Just prior to arriving in Boston from New York, PRIGOFF noticed a tower (presumably the Dorchester Gas Tank) with public art displayed on it. He intended to get a closer view of the art but was denied access by facility's security officers. PRIGOFF advised that he was greatly irritated because he simply desired to take a photo of the art work on

[Redacted]

3402

b7E

To: Boston From: Boston
Re: 11/08/2004

b7E

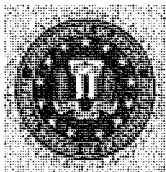
the tower. He has photographed a number of tanks and towers throughout the country.

In view of the explanation provided this, Boston considers this lead covered.

◆◆

EXHIBIT 5

U.S. Department of Justice



Federal Bureau of Investigation
Washington, D.C. 20535

March 24, 2015

MR. YAMAN SALAHI
ASIAN AMERICANS ADVANCING JUSTICE
ASIAN LAW CAUCUS
55 COLUMBUS AVENUE
SAN FRANCISCO, CA 94111

FOIPA Request No.: 1280493-000
Subject: PRIGOFF, JAMES

Dear Mr. Salahi:

The enclosed documents were reviewed under the Freedom of Information/Privacy Acts (FOIPA), Title 5, United States Code, Section 552/552a. Deletions have been made to protect information which is exempt from disclosure, with the appropriate exemptions noted on the page next to the excision. In addition, a deleted page information sheet was inserted in the file to indicate where pages were withheld entirely. The exemptions used to withhold information are marked below and explained on the enclosed Explanation of Exemptions:

Section 552		Section 552a
<input type="checkbox"/> (b)(1)	<input type="checkbox"/> (b)(7)(A)	<input type="checkbox"/> (d)(5)
<input type="checkbox"/> (b)(2)	<input type="checkbox"/> (b)(7)(B)	<input type="checkbox"/> (j)(2)
<input type="checkbox"/> (b)(3)	<input checked="" type="checkbox"/> (b)(7)(C)	<input type="checkbox"/> (k)(1)
_____	<input type="checkbox"/> (b)(7)(D)	<input type="checkbox"/> (k)(2)
_____	<input checked="" type="checkbox"/> (b)(7)(E)	<input type="checkbox"/> (k)(3)
_____	<input type="checkbox"/> (b)(7)(F)	<input type="checkbox"/> (k)(4)
<input type="checkbox"/> (b)(4)	<input type="checkbox"/> (b)(8)	<input type="checkbox"/> (k)(5)
<input type="checkbox"/> (b)(5)	<input type="checkbox"/> (b)(9)	<input type="checkbox"/> (k)(6)
<input checked="" type="checkbox"/> (b)(6)		<input type="checkbox"/> (k)(7)

9 pages were reviewed and 9 pages are being released.

Document(s) were located which originated with, or contained information concerning, other Government agency(ies) [OGA].

This information has been referred to the OGA(s) for review and direct response to you.

We are consulting with OGA(s). The FBI will correspond with you regarding this information when the consultation is finished.

In accordance with standard FBI practice and pursuant to FOIA exemption (b)(7)(E) and Privacy Act exemption (j)(2) [5 U.S.C. § 552/552a (b)(7)(E)/(j)(2)], this response neither confirms nor denies the existence of your subject's name on any watch lists.


For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S.C. § 552(c) (2006 & Supp. IV (2010)). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist. Enclosed for your information is a copy of the Explanation of Exemptions.

You have the right to appeal any denials in this release. Appeals should be directed in writing to the Director, Office of Information Policy (OIP), U.S. Department of Justice, 1425 New York Ave., NW, Suite 11050, Washington, D.C. 20530-0001, or you may submit an appeal through OIP's eFOIA portal at <http://www.justice.gov/oip/efoia-portal.html>. Your appeal must be received by OIP within sixty (60) days from the date of this letter in order to be considered timely. The envelope and the letter should be clearly marked "Freedom of Information Appeal." Please cite the FOIPA Request Number assigned to your request so that it may be easily identified.

The enclosed material is from the main investigative file(s) in which the subject(s) of your request was the focus of the investigation. Our search located additional references, in files relating to other individuals, or matters, which may or may not be about your subject(s). Our experience has shown when ident, references usually contain information similar to the information processed in the main file(s). Because of our significant backlog, we have given priority to processing only the main investigative file(s). If you want the references, you must submit a separate request for them in writing, and they will be reviewed at a later date, as time and resources permit.

See additional information which follows.

Sincerely,



David M. Hardy
Section Chief
Record/Information
Dissemination Section
Records Management Division

Enclosures

This is in reference to your Freedom of Information Privacy Acts request submitted to the Records Management Division in Winchester, Virginia. Enclosed is a processed copy of records responsive to this FOIPA. These records represent the final release of information related to this request.

The enclosure is being provided at no charge.

Regarding your request for expungement of records concerning James Prigoff, we have determined that the records in question consist of investigatory materials compiled for law enforcement purposes contained in the FBI Central Records System. Therefore, consistent with the system of records notice contained in 28 C.F.R. § 16.96, these records are exempt from the amendment provisions of the Privacy Act. See 5 U.S.C. § 552a (j)(2).

You may file an appeal regarding the request for expungement by writing to the Director, Office of Privacy and Civil Liberties (OPCL), U.S. Department of Justice, 1331 Pennsylvania Ave. NW, Suite 1000, Washington, D.C. 20530-0001. Your appeal must be received by OPCL within sixty (60) days from the date of this letter in order to be considered timely. The envelope and the letter should be clearly marked "Privacy Amendment Appeal." Please cite the FOIPA Request Number in any correspondence to us for proper identification of your request.

EXPLANATION OF EXEMPTIONS**SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552**

- (b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;
- (b)(2) related solely to the internal personnel rules and practices of an agency;
- (b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;
- (b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

- (d)(5) information compiled in reasonable anticipation of a civil action proceeding;
- (j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
- (k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;
- (k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;
- (k)(4) required by statute to be maintained and used solely as statistical records;
- (k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;
- (k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

FBI/DOJ

EXHIBIT 6



May 19, 2015

VIA FEDEX AIR

Director, Office of Information Policy
U.S. Department of Justice
1425 New York Avenue, NW, Suite 11050
Washington, D.C. 20530-0001

**Re: Freedom of Information Act and Privacy Act Appeal on Behalf of James Prigoff;
FOIPA Request No. 1280493-000**

Dear Sir/Madam:

We write to appeal the U.S. Department of Justice's (the "Department") March 24, 2015 letter exempting portions of a production responsive to FOIPA Request Number 1280493-000, which we filed on behalf of James Prigoff on July 9, 2014.¹ The Department produced nine redacted pages in response to Mr. Prigoff's request. The production, however, makes clear that (1) the Department did not produce all records relating to Mr. Prigoff, as requested, and (2) the Department improperly applied exemptions under FOIA as the basis for withholding information responsive to Mr. Prigoff's request. For these reasons, and as set forth in detail below, we appeal certain of the exemptions upon which the Department withheld responsive information, and respectfully request that the Department produce all documents referencing Mr. Prigoff.

I. The Department Failed to Produce All Responsive Documents

In our July 9, 2014 request, we sought "*all records, including but not limited to Suspicious Activity Reports, pertaining to or referencing Mr. Prigoff.*" (Ex. A, at p. 1 (emphasis added).) We did not limit the scope of our request by subject matter or by date. By way of example, we included information about an incident in 2004 involving Mr. Prigoff about which we believed the Department contained records. (*See id.*, at p. 2.) The Department's production, however, did not produce all documents pertaining to or referencing Mr. Prigoff. Instead, the Department produced *only* records relating to that particular 2004 incident. The production,

¹ Copies of our July 9, 2014 request and the FBI's March 24, 2015 response are attached hereto as Exhibits A and B, respectively.

however, reveals that other responsive documents exist, but were not included. Specifically, page two of the report dated June 21, 2004, states:

An ACS check of JAMES PRIGOFF revealed the following references:

[REDACTED] in 1983

[REDACTED] in 1991

[REDACTED] in 1992

[REDACTED] in 1992

(Ex. B.) Page two of the FBI's report dated October 18, 2004 contains the same information. (*See id.*)

The Department did not include in the production any records relating to these references in its ACS system, even though they clearly fall within the parameters of our request for "all records . . . pertaining to or referencing Mr. Prigoff." (Ex. A, at p. 1.) The Department thus has not met its burden of making "a good-faith effort to conduct a search for the requested records, using methods which can be reasonably expected to produce the information requested." *Nation Magazine v. U.S. Customs Serv.*, 71 F.3d 885, 890 (D.C. Cir. 1995) (internal quotation omitted). Accordingly, we hereby reiterate our request that the FBI produce any and all documents pertaining to or referencing Mr. Prigoff, including but not limited to, all documents related to the above-listed references in the FBI's ACS system.

II. The Department Failed to Substantiate Use of Exemptions

The Department cites sections (b)(6), (b)(7)(C), and (b)(7)(E) to justify withholding portions of the nine-page production. Review of the production, however, reveals that the (b)(7)(E) exemption was not properly asserted and that redactions based thereon were over broadly applied.

Exemption (b)(7)(E) applies to records or information compiled for law enforcement purposes that would disclose techniques, procedures, and/or guidelines for law enforcement investigations or prosecutions. 5 U.S.C. § 552(b)(7)(E). Here, the Department invoked (b)(7)(E) to justify redacting materials related to incidents that occurred *over two to three decades ago*, specifically, all information relating to ACS references for Mr. Prigoff from 1983, 1991, and 1992. Such information cannot plausibly be the subject of law enforcement investigations or prosecutions. In addition, given that Mr. Prigoff has not engaged in any criminal activity, it is highly unlikely that the Department is able to meet its burden of showing that the redacted material relates to enforcement of a particular federal law. *See ACLU v. FBI*, Case No. 10-cv-03759-RS (N.D. Cal. March 23, 2015) (holding FBI could not assert exemption 7 where it did



not show a rational basis between the enforcement of a federal law and withheld information). In any event, the Department's blanket cite to (b)(7)(E) fails to justify its withholding of responsive information. As such, the (b)(7)(E) exemption was improperly asserted and information that was redacted based thereon should have been disclosed. *See Local 598 v. Dept. of Army Corps of Eng'rs*, 841 F.2d 1459, 1463 (9th Cir. 1988) (FOIA "embodies a strong policy of disclosure and places a duty to disclose on federal agencies. . . . 'disclosure, not secrecy, is the dominant objective of the Act.'") (internal citation omitted).

Thank you for your attention to this appeal. Please do not hesitate to contact me at (415) 848-7711 or by email at yamans@advancingjustice-alc.org if you have any questions. We look forward to your prompt response.

Sincerely,



Yaman Salahi
Staff Attorney

Enclosures



EXHIBIT 7



U.S. Department of Justice
Office of Information Policy
Suite 11050
1425 New York Avenue, NW
Washington, DC 20530-0001

Telephone: (202) 514-3642

Yaman Salahi, Esq.
Asian Americans Advancing Justice
Asian Law Caucus
55 Columbus Avenue
San Francisco, CA 94111
yamans@advancingjustice-alc.org

Re: Appeal No. AP-2015-03904
Request No. 1280493
RRK:TAZ

VIA: E-mail

Dear Mr. Salahi:

You appealed on behalf of your client, James Prigoff, from the action of the Federal Bureau of Investigation on his Freedom of Information Act request for access to records concerning himself. I note that your appeal is limited to challenging the adequacy of the FBI's search for records, and the FBI's assertions of Exemption (b)(7)(E) to withhold certain information.

After carefully considering your appeal, I am affirming the FBI's action on your client's request. In order to provide your client with the greatest possible access to responsive records, your client's request was reviewed under both the Privacy Act of 1974 and the FOIA. I have determined that the records responsive to your client's request are exempt from the access provision of the Privacy Act. See 5 U.S.C. § 552a(j)(2); see also 28 C.F.R. § 16.96 (2015). For this reason, I have reviewed your appeal under the FOIA.

The FOIA provides for disclosure of many agency records. At the same time, Congress included in the FOIA nine exemptions from disclosure that provide protection for important interests such as personal privacy, privileged communications, and certain law enforcement activities. The FBI properly withheld certain information because it is protected from disclosure under the FOIA pursuant to 5 U.S.C. § 552(b)(7)(E). This provision concerns records or information compiled for law enforcement purposes the release of which would disclose techniques and procedures for law enforcement investigations or prosecutions.

To the extent that your client's request seeks access to records that would either confirm or deny an individual's placement on any government watch list, the FBI properly refused to confirm or deny the existence of any records responsive to your client's request because the existence of such records is protected from disclosure pursuant to 5 U.S.C. § 552a(j)(2) & 5 U.S.C. § 552(b)(7)(E). FOIA Exemption 7(E) concerns records or information compiled for law enforcement purposes the release of which would disclose techniques and procedures for law

- 2 -

enforcement investigations or prosecutions. This response should not be taken as an indication that records do or do not exist. Rather, this is the standard response made by the FBI.

As to your appeal concerning the adequacy of the FBI's search for responsive records subject to the FOIA, I have determined that the FBI's response was correct and that it conducted an adequate, reasonable search for such records. The FBI searched for both main files and cross references in its Headquarters Office and in its Boston, New York, San Francisco, and Washington Field Offices.

Please be advised that this Office's decision was made only after a full review of this matter. Your appeal was assigned to an attorney with this Office who thoroughly reviewed and analyzed your appeal, your client's underlying request, and the action of the FBI in response to your client's request.

If your client is dissatisfied with my action on your appeal, the FOIA permits him to file a lawsuit in federal district court in accordance with 5 U.S.C. § 552(a)(4)(B).

For your information, the Office of Government Information Services (OGIS) offers mediation services to resolve disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. Using OGIS services does not affect your client's right to pursue litigation. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, Room 2510, 8601 Adelphi Road, College Park, Maryland 20740-6001; e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

Sincerely,

1/27/2016

X



Sean R. O'Neill
Chief, Administrative Appeals Staff
Signed by: SEAN O'NEILL

EXHIBIT 8

Office of the Director of National Intelligence
Washington, DC 20511

JAN - 8 2015

Yaman Salahi
Asian Americans Advancing Justice - Asian Law Caucus
55 Columbus Avenue
San Francisco, CA 94111

Reference: ODNI Case #DP-2015-00003

Dear Mr. Salahi:

This is in response to your letter dated 9 July 2014 (Enclosure) received in the Information Management Division of the Office of the Director of National Intelligence (ODNI) on 20 October 2014, in which you requested records pertaining to James Prigoff under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and the Privacy Act (PA), 5 U.S.C. §552a.

Your request has been processed in accordance with both the FOIA and the PA. The ODNI conducted a search of its Security, Personnel, and Human Resources files for records responsive to your request, and no records were located.

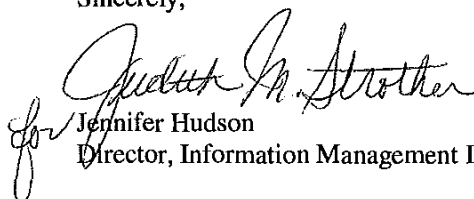
With regard to its classified files, in accordance with Section 3.6(a) of Executive Order 13526, the ODNI can neither confirm nor deny the existence or nonexistence in those files of any information responsive to your request. The fact of the existence or nonexistence of the requested records is currently and properly classified pursuant to FOIA exemption (b)(1) and PA exemption (k)(1). Any information within those files that would reveal intelligence sources and methods information is protected from disclosure by the National Security Act of 1947, as amended, and by FOIA exemption (b)(3), 50 U.S.C. 3024(i).

If you wish to appeal our determination on this request, please explain the basis of your appeal and forward to the address below within 45 days of the date of this letter.

Office of the Director of National Intelligence
Information Management Office
Washington D.C. 20511

If you have any questions, email our Requester Service Center at DNI-FOIA@dni.gov or call us at (703) 874-8500.

Sincerely,


Jennifer Hudson
Director, Information Management Division

Enclosure

EXHIBIT 9

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
CHIEF MANAGEMENT OFFICER
WASHINGTON, DC 20511

SEP 15 2015

Mr. Yaman Salahi
Asian Americans Advancing Justice
Asian Law Caucus
55 Columbus Avenue
San Francisco, CA 94111

Reference: ODNI Case DP-2015-00003

Dear Mr. Salahi:

This is in response to your letter dated 20 February 2015 (Enclosure), wherein you appealed our 8 January 2015 determination in response to your 9 July 2014 request for all records pertaining to your client, Mr. James Prigoff.

Your appeal was processed in accordance with the FOIA, 5 U.S.C § 552, as amended, and Privacy Act, 5 U.S.C. § 552a. The Office of the Director of National Intelligence (ODNI) conducted an additional search for unclassified records responsive to your request and no records were located. Expungement of records will not apply in this case, since no responsive records were located.

Regarding classified holdings, in accordance with Section 3.6(a) of Executive Order 13526, the ODNI can neither confirm nor deny the existence or nonexistence in its files of any information responsive to your request. The fact of the existence or nonexistence of requested records is currently and properly classified and is intelligence sources and methods information that is protected from disclosure by the National Security Act of 1947, as amended. Therefore your request is denied pursuant to FOIA exemptions (b)(1) and (k)(1). By this statement, the ODNI neither confirms nor denies that such records may or may not exist.

Therefore, after careful consideration of your appeal, we have determined that the decision of the Director, Information Management Office should be affirmed.

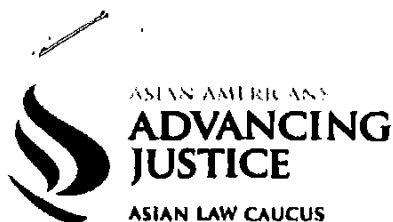
In accordance with the provisions of the FOIA, you have the right to seek judicial review of this determination in a United States district court. Alternatively, the Office of Government Information Services (OGIS) offers mediation services to resolve disputes between FOIA requesters and federal agencies. Using services offered by OGIS does not affect your right to pursue litigation. For more information, including how to contact OGIS, please consult this website, <http://ogis.archives.gov>.

Sincerely,


Mark W. Ewing

Enclosure:
Appeal Request

REC'D SEP 29

**FEB 23 2015**

February 20, 2015

VIA EMAIL AND UPS NEXT DAY AIR

Office of the Director of National Intelligence
Information Management Office
Washington, D.C. 20511

**Re: Freedom of Information Act and Privacy Act Appeal on Behalf of James Prigoff;
ODNI Case #DP-2015-00003**

Dear Sir/Madam:

We write to appeal the Office of the Director of National Intelligence's (the "ODNI") response to our request, dated July 9, 2014, on behalf of James Prigoff to disclose, amend, and/or expunge any and all records, including but not limited to Suspicious Activity Reports ("SARs"), pertaining to or referencing Mr. Prigoff. By way of letter dated January 8, 2015, the ODNI stated that it "conducted a search of its Security, Personnel, and Human Resources files for records responsive to your request, and no records were located." The ODNI further stated that it could neither confirm nor deny the existence or non-existence of any information responsive to our request in its classified files.¹ There are several grounds for this appeal.

First, the ODNI's January 8, 2015 letter makes clear that it only searched its "Security, Personnel, and Human Resources" files for records responsive to our request. We did not, however, limit our request to such files, but instead requested that the ODNI provide *all* records in the Information Sharing Environment's possession that refer or relate to Mr. Prigoff. (*See Ex. A, at p. 2.*) The ODNI has not met its burden of making "a good-faith effort to conduct a search for the requested records, using methods which can be reasonably expected to produce the information requested." *Nation Magazine v. U.S. Customs Serv.*, 71 F.3d 885, 890 (D.C. Cir. 1995) (internal quotation omitted). Accordingly, we hereby reiterate our request that the ODNI search all databases and files to which it has access, including any databases and files containing SARs, for records concerning Mr. Prigoff. We also request that, in its subsequent response, the ODNI identify the databases and files that it searched, and indicate whether those databases and files contain SAR information within the ODNI's possession, access, or control.

¹ Copies of our July 9, 2014 request and the ODNI's January 8, 2015 response are attached hereto as Exhibits A and B, respectively.

Second, in declining to confirm or deny the existence or non-existence of responsive information, the ODNI invoked 5 U.S.C. § 552(b)(1). It is not clear whether the ODNI applied this exemption to eGuardian or other databases containing SAR reports or information derived from SAR reports. If so, the ODNI's reliance is improper because the type of information that is the subject of our request, and which we believe is in the ODNI's possession, has already been publicly disclosed with regard to three other individuals. Specifically, SARs have been disclosed to Mr. Wiley Gill, Mr. Khaled Ibrahim, and Mr. Tariq Razak, all of whom we represent and all of whom filed similar FOIA and Privacy Act requests with the ODNI. (Mr. Gill's ODNI case number is DP-2015-00006, Mr. Ibrahim's ODNI case number is DP-2015-00005, and Mr. Razak's ODNI case number is DP-2015-00004.) Thus, there is no reason under FOIA or the Privacy Act to justify the ODNI's refusal to confirm or deny the existence or non-existence of similar information with regard to Mr. Prigoff.

Third, the ODNI's January 8, 2015 letter did not address our request pursuant to the Privacy Act for an opportunity to amend and/or expunge all records maintained by the ODNI that describe (i) Mr. Prigoff's exercise of rights guaranteed by the First Amendment, (ii) conduct that does not support reasonable suspicion of criminal activity, and (iii) conduct that does not implicate criminal conduct in any way. (*See Ex. A*, at pp. 2-3.) As such, it appears that the ODNI did not process this portion of our request. We hereby reiterate our request for amendment and/or expungement as set forth in our July 9, 2014 letter. To the extent that documents responsive to our request exist, but have been designated classified, the ODNI is not precluded from expunging records based on this classification.

Thank you for your attention to this appeal. Please do not hesitate to contact me at (415) 848-7711 or by email at yamans@advancingjustice-alc.org if you have any questions. We look forward to your prompt response.

Sincerely,



Yaman Salahi
Staff Attorney

Enclosures

www.advancingjustice-alc.org

EXHIBIT 10

PART B – ISE-SAR CRITERIA GUIDANCE

Category	Description
Eliciting Information	Questioning facility personnel about facility/infrastructure/personnel; this includes individuals probing employees in person on or off-site, over the phone, or via the Internet about particular structures, functions, and personnel procedures at the facility/infrastructure.
Breach/Attempted Intrusion	Unauthorized personnel attempting to or actually entering a restricted area or protected site. Impersonation of authorized personnel (e.g. police/security, janitor).
Misrepresentation	Presenting false or misusing insignia, documents, and/or identification, to misrepresent one's affiliation to cover possible illicit activity.
Photography	Taking pictures/video of facility/infrastructure/personnel or surrounding environment.
Observation	Showing unusual interest in facility/infrastructure/personnel; for example, observing it through binoculars, taking notes, drawing maps, or drawing structures of the facility.
Surveillance	Monitoring the activity of people, facilities, processes or systems.
Theft/Loss/Diversion	Stealing or diverting something associated with a facility/infrastructure (e.g., badges, uniforms, identification, emergency vehicles, technology or documents (classified or unclassified), which are proprietary to the facility).
Sabotage/Tampering/ Vandalism	Damaging, manipulating, or defacing part of a facility/infrastructure or protected site.
Testing of Security	Interactions with, or challenges to installations, personnel, or systems that reveal physical, personnel or cyber security capabilities.
Cyber Attack	Compromising, or attempting to compromise or disrupt an organization's information technology infrastructure.
Expressed or Implied Threat	Communicating a spoken or written threat to damage or compromise a facility/infrastructure.
Flyover	Suspected over flight of a facility/infrastructure; this includes any type of flying vehicle (e.g., airplanes, helicopters, unmanned aerial vehicles, hang gliders).
Materials Acquisition/Storage	Acquisition of unusual quantities of precursor material (e.g., cell phones, pagers, fuel, timers), unauthorized/unlicensed individual/group attempts to obtain precursor chemicals/agents, or toxic materials, and rental of storage units for the purpose of storing chemicals or mixing apparatus.
Acquisition Of Expertise	Attempts to obtain or conduct training in security concepts; military weapons or tactics; or other, unusual, capabilities, such as specialized transport or handling capabilities.
Weapons Discovery	Discovery of weapons or explosives.
Sector-Specific Incident	Actions associated with a characteristic of unique concern to specific sectors (such as the public health sector), with regard to their personnel, facilities, systems or functions.
Recruiting	Building of operations teams and contacts, personnel data, banking data or travel data.
Other	Incidents not fitting any of the above categories.

UNCLASSIFIED

ISE-FS-200

PART B – ISE-SAR CRITERIA GUIDANCE

Category	Description
DEFINED CRIMINAL ACTIVITY AND POTENTIAL TERRORISM NEXUS ACTIVITY	
Breach/Attempted Intrusion	Unauthorized personnel attempting to or actually entering a restricted area or protected site. Impersonation of authorized personnel (e.g. police/security, janitor).
Misrepresentation	Presenting false or misusing insignia, documents, and/or identification, to misrepresent one's affiliation to cover possible illicit activity.
Theft/Loss/Diversion	Stealing or diverting something associated with a facility/infrastructure (e.g., badges, uniforms, identification, emergency vehicles, technology or documents (classified or unclassified), which are proprietary to the facility).
Sabotage/Tampering/Vandalism	Damaging, manipulating, or defacing part of a facility/infrastructure or protected site.
Cyber Attack	Compromising, or attempting to compromise or disrupt an organization's information technology infrastructure.
Expressed or Implied Threat	Communicating a spoken or written threat to damage or compromise a facility/infrastructure.
Aviation Activity	Operation of an aircraft in a manner that reasonably may be interpreted as suspicious, or posing a threat to people or property. Such operation may or may not be a violation of Federal Aviation Regulations.
POTENTIAL CRIMINAL OR NON-CRIMINAL ACTIVITY REQUIRING ADDITIONAL FACT INFORMATION DURING INVESTIGATION¹¹	
Eliciting Information	Questioning individuals at a level beyond mere curiosity about particular facets of a facility's or building's purpose, operations, security procedures, etc., that would arouse suspicion in a reasonable person.
Testing or Probing of Security	Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel or cyber security capabilities.
Photography	Taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person. Examples include taking pictures or video of infrequently used access points, personnel performing security functions (patrols, badge/vehicle checking), security-related equipment (perimeter fencing, security cameras), etc.

¹¹ Note: These activities are generally First Amendment-protected activities and should not be reported in a SAR or ISE-SAR absent articulable facts and circumstances that support the source agency's suspicion that the behavior observed is not innocent, but rather reasonably indicative of criminal activity associated with terrorism, including evidence of pre-operational planning related to terrorism. Race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion (although these factors may be used as specific suspect descriptions).

UNCLASSIFIED

ISE-FS-200

Category	Description
Observation/Surveillance	Demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional (e.g. engineers) interest such that a reasonable person would consider the activity suspicious. Examples include observation through binoculars, taking notes, attempting to measure distances, etc.
Materials Acquisition/Storage	Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, fuel, chemicals, toxic materials, and timers, such that a reasonable person would suspect possible criminal activity.
Acquisition of Expertise	Attempts to obtain or conduct training in security concepts; military weapons or tactics; or other unusual capabilities that would arouse suspicion in a reasonable person.
Weapons Discovery	Discovery of unusual amounts of weapons or explosives that would arouse suspicion in a reasonable person.
Sector-Specific Incident	Actions associated with a characteristic of unique concern to specific sectors (such as the public health sector), with regard to their personnel, facilities, systems or functions.

PART B—ISE-SAR CRITERIA GUIDANCE

Part B provides a more thorough explanation of ISE-SAR pre-operational behavioral categories and criteria. This guidance highlights the importance of having a trained analyst or investigator take into account the context, facts, and circumstances in reviewing suspicious behaviors to identify those SARs with a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism). It is important to understand, however, that the behavioral categories and criteria listed below reflect studies of prior terrorism incidents and are not intended to be limited in any way by the descriptive examples.¹⁹ The descriptive examples outlined below in the third column do not represent all possible examples that relate to ISE-SAR submissions. They are provided as a nonexhaustive list of illustrations of pre-operational behaviors that may support the documentation and submission of an ISE-SAR based on the contextual assessment of the reviewing analyst or investigator.

In order to ensure that Part B is responsive to changes in the threat environment, the ISA IPC will establish a formal process for reviewing and updating the behavioral categories in the first column and the behavioral criteria set forth in the second column. (*See the chart below.*) The process will involve coordination and consultation between and among NSI participants and other stakeholders, who will examine the current body of knowledge regarding terrorism and other criminal activity. This process will result in the issuance of an update to the *ISE-SAR Functional Standard* when revisions are made to either or both of the first or second columns.

As needed, the DHS, in conjunction with the FBI, will guide a *separate* process to allow for interim updates to the descriptive examples contained in the third column of Part B. Updates to the third column will be based on field experience (e.g., emerging threats, trip wire reports, and other intelligence) and will be documented in the change management chart²⁰ of the *ISE-SAR Functional Standard*, rather than reissuance of the *ISE-SAR Functional Standard* by the PM-ISE.

The nine behaviors identified below as “Potential Criminal or Non-criminal Activity Requiring Additional Information During Vetting” are not inherently criminal behaviors and may include constitutionally protected activities that must not be documented in an ISE-SAR that contains PII unless there are articulable facts or circumstances that clearly support the determination that the behavior observed is not innocent, but rather reasonably indicative of pre-operational planning associated with terrorism. Race, ethnicity, gender, national origin, religion, sexual orientation, or

¹⁹ In addition to the descriptive examples listed in Part B and in order to further enhance NSI participants’ understanding of the Part B behavioral categories and criteria, the DHS, in conjunction with the FBI, may develop additional examples to be included in implementation materials (e.g., the *Vetting ISE-SAR Data* guidance) or delivered through training. Additionally, relevant federal and SLTT law enforcement agencies may identify and report additional examples of terrorism behavior within the 16 behavioral categories to the DHS or the FBI.

²⁰ This chart is included on page 6 of this *Functional Standard*.

gender identity must not be considered as factors creating suspicion (but attributes may be documented in specific suspect descriptions for identification purposes).²¹ The activities listed as “Potential Criminal or Non-Criminal Activity” are not inherently criminal behaviors and are potentially constitutionally protected; thus, additional facts or circumstances must be articulated in the incident. For example, the trained analyst or investigator should document specific additional facts or circumstances indicating that the behavior is suspicious, such as steps to conceal one's location and avoid detection while taking pictures.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
DEFINED CRIMINAL ACTIVITY AND POTENTIAL TERRORISM NEXUS ACTIVITY		
Breach/ Attempted Intrusion	Unauthorized personnel attempting to enter or actually entering a restricted area, secured protected site, or nonpublic area. Impersonation of authorized personnel (e.g., police/security officers, janitor, or other personnel).	<ul style="list-style-type: none"> • At 1:30 a m., an individual breached a security perimeter of a hydroelectric dam complex. Security personnel were alerted by an electronic alarm and observed the subject on CCTV, taking photos of himself in front of a “No Trespassing” sign and of other parts of the complex. The subject departed prior to the arrival of security personnel. • A railroad company reported to police officers that video surveillance had captured images of three individuals illegally entering a train station to gain access to a restricted-access tunnel and taking photos of the tunnel.

²¹ See footnote 9 for additional guidance.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
Misrepresentation	Presenting false information or misusing insignia, documents, and/or identification to misrepresent one's affiliation as a means of concealing possible illegal activity.	<ul style="list-style-type: none"> • A state bureau of motor vehicles employee discovered a fraudulent driver's license in the possession of an individual applying to renew the license. A criminal investigator determined that the individual had also fraudulently acquired a passport in the same name and used it to make several extended trips to countries where terrorist training has been documented. • An individual used a stolen uniform from a private security company to gain access to the video monitoring control room of a shopping mall. Once inside the room, the subject was caught trying to identify the locations of surveillance cameras throughout the entire mall.
Theft/Loss/ Diversion	Stealing or diverting something associated with a facility/infrastructure or secured protected site (e.g., badges, uniforms, identification, emergency vehicles, technology, or documents {classified or unclassified}), which are proprietary to the facility/infrastructure or secured protected site.	<ul style="list-style-type: none"> • A federal aerospace facility reported a vehicle burglary and the theft of an employee's identification credential, a secure ID token, and an encrypted thumb drive. • An explosives ordnance company reported a burglary of a storage trailer. Items stolen included electric initiators, radios, and other items that could be used in connection with explosives.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
Sabotage/ Tampering/ Vandalism	Damaging, manipulating, defacing, or destroying part of a facility/infrastructure or secured protected site.	<ul style="list-style-type: none"> • A light-rail authority reported the discovery of a track switch that had been wrapped in a length of chain in a possible attempt to derail a passenger train car. • A natural gas company reported the deliberate removal of gas meter plugs on the “customer side” in two separate locations approximately a quarter of a mile apart. One location was a government facility. The discovery was made as the government facility’s sensor detected the threat of an explosion.
Cyberattack	Compromising or attempting to compromise or disrupt an organization’s information technology infrastructure.	<ul style="list-style-type: none"> • A federal credit union reported it was taken down for two and a half hours through a cyberattack, and the attacker was self-identified as a member of a terrorist organization. • A state’s chief information officer reported the attempted intrusion of the state’s computer network by a group that has claimed responsibility for a series of hacks and distributed denial-of-service attacks on government and corporate targets.
Expressed or Implied Threat	Communicating a spoken or written threat to commit a crime that will result in death or bodily injury to another person or persons or to damage or compromise a facility/infrastructure or secured protected site.	<ul style="list-style-type: none"> • A customer-experience feedback agency received a call from a watchlisted individual stating, “Wait till they see what we do to the ATF, IRS, NSA.” • A military museum received a threatening letter containing a white powder. The letter claimed a full-scale anthrax attack had been launched in retaliation for crimes committed by the U.S. Armed Forces.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
Aviation Activity	Learning to operate, or operating an aircraft, or interfering with the operation of an aircraft in a manner that poses a threat of harm to people or property and that would arouse suspicion of terrorism or other criminality in a reasonable person. Such activity may or may not be a violation of Federal Aviation Regulations.	<ul style="list-style-type: none"> • Federal air traffic control personnel reported two separate laser beam cockpit illumination incidents involving different commercial airliners occurring at night and during the take-off phase of flight. The reports revealed that the laser beam in both incidents originated from the same general geographic area, near a major airport on the East Coast. These findings indicate the likelihood of purposeful acts by the same individual. • A chemical facility representative reported an unauthorized helicopter hovering within 50 feet of a chemical tank located in a posted restricted area. An FAA registry search of the tail number was negative, indicating use of an unregistered number, which suggests an attempt to conceal the identity of the plane's owner and/or its place of origin.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
POTENTIAL CRIMINAL OR NON-CRIMINAL ACTIVITY REQUIRING ADDITIONAL INFORMATION DURING VETTING		
Eliciting Information	Questioning individuals or otherwise soliciting information at a level beyond mere curiosity about a public or private event or particular facets of a facility's or building's purpose, operations, security procedures, etc., in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.	<ul style="list-style-type: none"> • A tour bus company servicing one of the nation's national monuments reported that a male subject asked a driver many unusual and probing questions about fuel capacity, fueling locations, and fueling frequency such that the driver became very concerned about the intent of the questioning. The male subject was not a passenger. • A guest services employee at a shopping center was questioned by an individual about how much security was on the property. The employee contacted security personnel, who confronted the individual. When questioned by security personnel, the individual quickly changed his questions to renting a wheelchair and then left without being identified. Security personnel reported that the individual seemed very nervous and that his explanations were not credible.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
Testing or Probing of Security	Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel, or cybersecurity capabilities in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.	<ul style="list-style-type: none"> • An individual who refused to identify himself to facility personnel at a shipping port reported that he was representing the governor's office and wanted to access the secure area of a steel manufacturer's space. He was inquiring about the presence of foreign military personnel. The individual fled when he realized that personnel were contacting the security office about his activities. He ran through the lobby and departed in a vehicle with an out-of-state license plate and containing two other individuals. • An individual discharged a fire extinguisher in a stairwell of a hotel and set off the building's fire alarm. This individual was observed entering the hotel approximately two minutes before the alarm sounded, was observed exiting from the stairwell at about the same time as the alarm, and then was observed in the lobby area before leaving the hotel.
Recruiting/Financing	Providing direct financial support to operations teams and contacts or building operations teams and contacts; compiling personnel data, banking data, or travel data in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.	<ul style="list-style-type: none"> • A prison inmate reported an effort to radicalize inmates nearing release toward violence. According to the plan, released inmates would go to a particular location for the purpose of obtaining information about attending an overseas terrorist training camp. • An individual reported that a former friend and business associate (a chemist) had recently asked him to participate in a terrorist-cell operation by providing funding to purchase needed equipment. The funding for the operation was reportedly linked to the illegal production of drugs.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
Photography	Taking pictures or video of persons, facilities, buildings, or infrastructure in an unusual or surreptitious manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include taking pictures or video of infrequently used access points, the superstructure of a bridge, personnel performing security functions (e.g., patrols, badge/vehicle checking), security-related equipment (e.g., perimeter fencing, security cameras), etc.	<ul style="list-style-type: none"> • A citizen reported to local police that she saw an unknown male crouched down in the back of an SUV with the hatchback open half-way. The subject was videotaping a National Guard readiness center. The vehicle was parked on the side of the road but sped away when the citizen began to approach the vehicle. The citizen could not provide a license tag number. • A citizen observed a female subject taking photographs of a collection of chemical storage containers in the vicinity of the port. The subject was hiding in some bushes while taking photographs of the storage tanks. The citizen reported this information to the city's port police. When the port police officer arrived and approached the subject, she ran to a nearby vehicle and sped off.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
Observation/ Surveillance	Demonstrating unusual or prolonged interest in facilities, buildings, or infrastructure beyond mere casual (e.g., tourists) or professional (e.g., engineers) interest and in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include observation through binoculars, taking notes, attempting to mark off or measure distances, etc.	<ul style="list-style-type: none"> • A mall security officer observed a person walking through the mall, filming at waist level, and stopping at least twice to film his complete surroundings, floor to ceiling. The subject became nervous when he detected security personnel observing his behavior. Once detained, the subject explained that he came to the mall to walk around and was simply videotaping the mall for his brother. The camera contained 15 minutes of mall coverage and footage of a public train system, along with zoomed photos of a bus. • Military pilots reported that occupants of multiple vehicles were observing and photographing in the area of residences of the military pilots. The pilots are responsible for the transport of special forces units. The report was made once the pilots realized that they had been individually surveyed by occupants of multiple vehicles during the same time period.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
Materials Acquisition/ Storage	Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, radio control toy servos or controllers; fuel, chemicals, or toxic materials; and timers or other triggering devices, in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.	<ul style="list-style-type: none"> • A garden center owner reported an individual in his twenties seeking to purchase 40 pounds of urea and 30 pounds of ammonium sulfate. The owner does not carry these items and became suspicious when the individual said he was purchasing the items for his mother and then abruptly departed the business. • A female reported that a man wanted to borrow her car to purchase fertilizer to add to the 3,000 pounds he had already acquired. When asked why he was acquiring fertilizer, he responded that he was going to "make something go boom." The subject lives in a storage unit and utilizes several other storage units at the location.
Acquisition of Expertise	Attempts to obtain or conduct training or otherwise obtain knowledge or skills in security concepts, military weapons or tactics, or other unusual capabilities in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.	<ul style="list-style-type: none"> • A fusion center received information on a watch-listed individual who was making repeated attempts to gain a hazardous materials endorsement for his commercial driver's license even though his immigration status made him ineligible. • A complaint was received from a gun shop about an individual under the age of 21 who had brought multiple groups of students into the gun shop to rent weapons to shoot. They desired to shoot assault rifles and handguns and asked questions about how to get around state and federal laws on weapon possession and transport.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
Weapons Collection/Discovery	Collection or discovery of unusual amounts or types of weapons, including explosives, chemicals, and other destructive materials, or evidence, detonations or other residue, wounds, or chemical burns, that would arouse suspicion of terrorism or other criminality in a reasonable person.	<ul style="list-style-type: none"> • A city employee discovered a backpack near a park bench along the route of a planned Martin Luther King Day march in the city. The backpack contained an improvised explosive device. • A suspicious person call resulted in the discovery of three individuals possessing hand-held radios, a military-grade periscope, a 7mm Magnum scoped rifle, an AK-74 assault rifle, a pistol-gripped shotgun, a semi-automatic handgun, a bandolier of shotgun ammunition, dozens of loaded handgun magazines, dozens of AK-74 magazines, Ghillie suits, several homemade explosive devices constructed of pill bottles, blast simulators, and military clothing.
Sector-Specific Incident	Actions associated with a characteristic of unique concern to specific sectors (e.g., the public health sector), with regard to their personnel, facilities, systems, or functions in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.	<ul style="list-style-type: none"> • A water company reported that it had security footage of an unknown person breaking into the premises. At 5 a.m., the individual cut through a fence and used a tool to breach a door. Once inside the building, the person took photos of the chlorination system, including the chlorine tank. A pump failure occurred, but it was not certain that this was related to the break-in. • A vehicle containing two individuals was discovered in a secure area of a loading dock at a facility that stores officially designated sensitive chemicals. The vehicle sped off upon discovery by security personnel. Surveillance footage revealed that the individuals gained entry by manually lifting a security gate to the compound.

EXHIBIT 11



BJA Bureau of Justice Assistance

Communities Against Terrorism

Potential Indicators of Terrorist Activities Related to the General Public

What Should I Consider Suspicious?

What Should I Do?

People involved in terrorist activity often exhibit indicators that if observed could identify a potential impending crime or terrorist attack. The following is a list of some of the characteristics of such persons that you should be aware of .

- Unusual requests for information –
 - questions regarding sensitive information such as security procedures or systems
 - questions regarding facility operations

- Unusual interest in high risk or symbolic targets
 - surveillance
 - note taking
 - drawing of diagrams
 - annotating maps
 - inappropriate photographs or videos

- people over dressed for the weather
- Unusual activity –
 - people acting suspiciously
 - people departing quickly when seen or approached
 - people in places where they do not belong
 - vehicles that appear to be overloaded



It is important to give a thorough report when notifying law enforcement. Keep in mind the responding officer may only have the information you gave at the time of your call. Providing a detailed description of persons or vehicles is imperative for a successful follow up by law enforcement personnel.

If something seems wrong, notify law enforcement authorities.

Do not jeopardize your safety or the safety of others.

**Columbus, Ohio Division of Police
Homeland Security Section
Terrorism Early Warning Unit
614-645-5410
1-866-759-8005**

Case: 17-16107-031201-RSS Document ID: 71011 Filed: 09/27/2015 Page 62 of 81

Help Protect Your Community

Be Part of the Solution



Terrorism may be national or international in scope, but terrorist incidents occur locally and are preceded by a number of pre-incident activities. Individuals in the community are key to identifying these pre-incident activities. By learning what to look for, **you** can aid law enforcement officials in protecting the homeland.

By being aware of what to look for and knowing how to report suspicious behavior, **you** can make a positive contribution in the fight against terrorism. The **partnership between the community and law enforcement** is essential to the success of anti-terrorism efforts.

It is important to remember that just because someone's speech, actions, beliefs, appearance, or way of life is different, it does not mean that he or she is suspicious. Instead, focus on behavior and activities that are unusual or out of place for the situation and that appear to be suspicious.

The activities outlined on this handout are by no means all-inclusive but have been compiled from a review of terrorist events over several years. Some of the activities, taken individually, could be innocent and must be examined by law enforcement professionals in a larger context to determine whether there is a basis to investigate.

This project was supported by Grant Number 2007-MU-BX-K002, awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Potential Indicators of Terrorist Activities Related to the General Public



Columbus, Ohio Division of Police
Homeland Security Section
Terrorism Early Warning Unit
614-645-5410
1-866-759-8005

Case 1:14-cv-00312-RSS Document 17-071 Filed 09/22/15 Page 63 of 81

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

MORGAN, LEWIS & BOCKIUS LLP
Stephen Scotch-Marmo (admitted *pro hac vice*)
stephen.scotch-marmo@morganlewis.com
Michael James Ableson (admitted *pro hac vice*)
michael.ableson@morganlewis.com
101 Park Avenue
New York, NY 10178
Telephone: (212) 309-6000; Facsimile: (212) 309-6001

AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN CALIFORNIA
Linda Lye (SBN 215584), llye@aclunc.org
Julia Harumi Mass (SBN 189649), jmass@aclunc.org
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 621-2493; Facsimile: (415) 255-8437

ASIAN AMERICANS ADVANCING
JUSTICE - ASIAN LAW CAUCUS
Christina Sinha (SBN 278893)
christinas@advancingjustice-alc.org
55 Columbus Avenue
San Francisco, CA 94111
Telephone: (415) 848-7711; Facsimile: (415) 896-1702

Attorneys for Plaintiffs
Additional counsel listed on signature page of Plaintiffs' Motions

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

WILEY GILL; JAMES PRIGOFF; TARIQ
RAZAK; KHALID IBRAHIM; and AARON
CONKLIN,

Plaintiffs,

v.

DEPARTMENT OF JUSTICE; LORETTA
LYNCH, in her official capacity as the
Attorney General of the United States;
PROGRAM MANAGER – INFORMATION
SHARING ENVIRONMENT;
KSEMENDRA PAUL, in his official
capacity as the Program Manager of the
Information Sharing Environment,

Defendants.

Case No. 3:14-cv-03120-RS-KAW

**DECLARATION OF LINDA LYE IN
SUPPORT OF PLAINTIFFS'
OPPOSITION TO DEFENDANTS'
MOTION FOR SUMMARY
JUDGMENT AND CROSS-MOTION
FOR SUMMARY JUDGMENT**

Hearing Date: December 8, 2016
Time: 1:30 p.m.
Judge: Hon. Richard Seeborg
Courtroom: 3, 17th Floor
Date Of Filing: July 10, 2014
Trial Date: None Set

1 I, Linda Lye, declare as follows:

2 1. I am counsel for Plaintiffs in this matter. The information in this declaration is
3 based upon my personal knowledge, except as otherwise indicated. If called upon to testify, I
4 would competently testify thereto.

5 2. In July 2013, I submitted a California Public Records Act (“PRA”) request to the
6 fusion center in Northern California, which is known as the National California Regional
7 Intelligence Center (“NCRIC”). A true and correct copy of the letter I sent is attached as Exhibit
8 1 to this declaration. My request asked for, among other things: “Records regarding sources of
9 funding used to support information systems containing suspicious activity reports, in particular,
10 name and amount of funding sources.”

11 3. On August 2, 2013, NCRIC responded to my request and stated: “The NCRIC
12 spent \$690,125 on the information systems containing SAR information. The funding source was
13 from 2009 ARRA funding.” A true and correct copy of NCRIC’s to me is attached as Exhibit 2
14 to this declaration.

15 4. On March 7, 2016, I submitted a follow-up PRA request to NCRIC requesting
16 “[d]ocuments reflecting funding sources – and identifying the federal entities that administered
17 any such sources – relating to information systems containing Suspicious Activity Reports.” In
18 particular, I requested documents related to the \$690,125 expended on information systems
19 containing SAR information, funded from 2009 ARRA funding, and referenced in NCRIC’s
20 August 2, 2013 response to my prior PRA request. A true and correct copy of my March 7, 2016
21 PRA request to NCRIC is attached as Exhibit 3 to this declaration.

22 5. On March 21, 2016, NCRIC responded to my request and provided multiple
23 documents in response. Only one of the documents pertained to a 2009 funding award. A true
24 and correct copy of NCRIC’s March 21, 2016 response letter and the 2009 funding award
25 document are attached as Exhibit 4 to this declaration.

26 6. NCRIC’s 2009 funding award involves funds from the “BJA FY 09 Recovery
27 Act” and provides funding to enhance Intelligence-led Policing capabilities through the
28 implementation of a Regional Intelligence Management System (IMS)...Grant funds

1 will...complete initial system implements, provide training, and incrementally add data sources.”
2 Exhibit 4 at 16. The document states that the grant award is subject to various “Special
3 Conditions,” including that “any information technology system funded or supported by OJP
4 funds will comply with 28 C.F.R. Part 23, Criminal Intelligence Systems Operating Policies.”
5 Exhibit 4 at 2 and 14.

6 7. In short, NCRIC’s August 2, 2013 and March 21, 2016 response to my PRA
7 requests indicate that NCRIC used funds from a federal grant that was administered by the Office
8 of Justice Programs to support information systems containing SAR information. The documents
9 produced by NCRIC further indicate that the Office of Justice Programs specifically attached a
10 special condition requiring any information system funded or supported by that grant to comply
11 with 28 C.F.R. Part 23.

12 8. The Office of Justice Programs maintains a website on which it posts, among other
13 things, information about the programs it funds. One such program is the Regional Information
14 Sharing System, also known as RISS. A true and correct copy of a description of the program
15 that I obtained from the Office of Justice Program’s website
16 (http://ojp.gov/about/pdfs/BJA_RISS%20Prog%20Summary_For%20FY%2017%20PresBud.pdf
17) on August 25, 2016 is attached as Exhibit 5 to this declaration. The document states that the
18 purpose of RISS is “[t]o enable multi-jurisdictional information sharing across law enforcement
19 and criminal justice agencies at all levels to resolve criminal cases while promoting officer
20 safety.” The document further states that it “supports federal, state, local, territorial, and tribal
21 law enforcement agencies and other criminal justice agencies through the six regional RISS
22 centers by providing,” among other things, “[a] secure online information and intelligence sharing
23 network.” The document identifies the program’s “Authorizing Legislation” as “Omnibus Crime
24 Control and Safe Streets Act of 1968 (42 USC 3796h(d)) as amended.” In addition, the document
25 states that additional information about RISS can be obtained on the following website:
26 “<http://www.riss.net/>.”

27 9. I visited the website www.riss.net on August 25, 2016, and it contains a page titled
28 “28 CFR Part 23 Frequently Asked Questions.” A true and correct copy of that page

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

FILER’S ATTESTATION

I, Phillip J. Wiese, am the ECF user whose identification and password are being used to file this DECLARATION OF LINDA LYE IN SUPPORT OF PLAINTIFFS’ OPPOSITION TO DEFENDANTS’ MOTION FOR SUMMARY JUDGMENT AND CROSS-MOTION FOR SUMMARY JUDGMENT. Pursuant to L.R. 5-1(i)(3), I hereby attest that concurrence in the electronic filing of this document has been obtained from each of the other signatories.

Dated: September 22, 2016 By /s/ Phillip J. Wiese
Phillip J. Wiese

EXHIBIT 1



July 12, 2013

Via U.S. Mail and Email

Mike Sena, Deputy Director
 Northern California Regional Intelligence Center
 P.O. Box 36102
 San Francisco, CA 94102
info@ncric.org

Re: Public Records Act Request Regarding Intelligence Gathering

Dear Public Records Coordinator:

I am writing on behalf of the American Civil Liberties Union of Northern California to request records pursuant to the California Public Records Act (Government Code §§ 6250, et. seq.) and Article I § 3(b) of the California Constitution for the following records¹:

- 1) Records regarding sources of funding used to support information systems containing automated license plate records, in particular, name and amount of funding sources.
- 2) Records regarding sources of funding used to support information systems containing suspicious activity reports, in particular, name and amount of funding sources.
- 3) Records reflecting the amount of financial support received by the Central California Intelligence Center through the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. §3711, *et seq.*, and the purpose(s) for which such funds are allocated or used.

Please provide the foregoing information for Fiscal Year 2011-12, FY 2012-13, and FY 2013-14.

¹“Records” covered by this request include but are not limited to: internal and external correspondence (including email), memoranda, drafts, notes, outlines, policies, procedures, regulations, directives, instructions, orders, bulletins, pamphlets or brochures, scripts, handouts, analyses, evaluations, reports, summaries, writings, logs and other written records or records by any other means, including but not limited to records kept on computers, computer source and object code, electronic communications, computer disks, CD-ROM, video tapes or digital video disks.

MICHELLE A. WELSH, CHAIRPERSON | DENNIS MCNALLY, AJAY KRISHNAN, FARAH BRELVI, ALLEN ASCH, VICE CHAIRPERSONS | KENNETH J. SUGARMAN, SECRETARY/TREASURER
 ABDI SOLTANI, EXECUTIVE DIRECTOR | CHERI BRYANT, DEVELOPMENT DIRECTOR | SHAYNA GELENDER, ORGANIZING & COMMUNITY ENGAGEMENT DIRECTOR | REBECCA FARMER, COMMUNICATIONS DIRECTOR
 ALAN SCHLOSSER, LEGAL DIRECTOR | MARGARET C. CROSBY, ELIZABETH O'ILL, LINDA LYE, JULIA HARUMI MASS, LINNEA NELSON, MICHAEL RISHER, JORY STEELE, STAFF ATTORNEYS
 PHYLLIDA BURLINGAME, ALLEN HOPPER, NATASHA MINSKER, NICOLE A. OZER, POLICY DIRECTORS | STEPHEN V. BOMSE, GENERAL COUNSEL

Case 3:14-cv-03120-RS Document 116 Filed 09/22/16 Page 8 of 39

Public Records Coordinator

July 12, 2013

Page 2

The California Public Records Act requires within ten (10) days either production of the requested documents and/or notice of the specific reasons why the materials requested (or portions thereof) are exempt from disclosure. Further, we request a summary of the information contained within any records you claim to be exempt under Government Code § 6254(f), as required by Government Code § 6254(f)(2).

Please send copies of the requested records to me at the address shown above, or email them to me at llye@aclunc.org. If necessary, we will reimburse you for reasonable copying costs.

If you have any questions regarding this request, please feel free to contact me at (415) 621-2493. Thank you in advance for your timely cooperation.

Sincerely,



Linda Lye
Staff Attorney

cc: David A. Silberman (via United States mail and email)
Office of County Counsel
County of San Mateo
Hall of Justice and Records, 6th Floor
400 County Center
Redwood City, CA 94063-1662
dsilberman@smcgov.org

EXHIBIT 2

Linda Lye

From: Hugh A. Cotton <hcotton@ncric.org>
Sent: Friday, August 02, 2013 2:38 PM
To: Linda Lye
Cc: PrivacyOfficer
Subject: RE: Public Records Act Request Regarding Intelligence Gathering

Dear Ms. Lye,

I am writing in response to your July 24, 2013 correspondence which was in response to my July 22, 2013 answer to your original Public Records Act request. In your most recent letter, you clarify the intent of some of your initial questions and seek additional information. I understand your questions as follows and have attempted to answer them in good faith as set forth below.

Question 1: What are the funding sources for ALPR's?

- The NCRIC spent \$163,660 from the FY08 UASI Grant (referenced below) on ALPR systems in November – December of 2010.

Question 2: What are the funding sources relating to information systems containing SAR information?

- The NCRIC spent \$690,125 on the information systems containing SAR information. The funding source was from 2009 ARRA funding. The NCRIC entered into an agreement with Palantir in January of 2012. There are ongoing maintenance costs, however, the NCRIC has yet to expend such funds. Maintenance costs will likely be funded out of the UASI or SHSP funding.

Question 3: Are there any *other* sources of funding, not listed below, that NCRIC received for FY 11, 12 and 13 and if so, in what amounts?

- The NCRIC previously disclosed the following funding sources in response to your initial request:
 - FY2011 State Homeland Security Grant (DHS grant passed through to Cal OES) \$2,011,000
 - FY12 State Homeland Security Grant (DHS grant passed through to Cal OES) \$1,761,000
 - FY11 Urban Area Security Initiative Grant (DHS passed through to Cal OES then to the Bay Area UASI as a sub-recipient) \$3,393,158
 - FY12 Urban Area Security Initiative Grant (DHS passed through to Cal OES then to the Bay Area UASI as a sub-recipient) \$3,393,158
 - Southwest Border Grant - FY09 Recovery Act - JAG (US DOJ-BJA) \$800,700
- The previously disclosed funding sources were DHS grants that included the title "FY11, FY12, and FY13." However, if you are requesting information for all NCRIC grants **active** during the actual fiscal year periods of FY11, FY12, and FY13, then below is a more accurate and comprehensive accounting:
 - 2010 Anti-Terrorism Funding (Direct from Cal OES) \$200,000
 - FY2008 State Homeland Security Grant (DHS passed through to Cal OES) \$1,000,000
 - FY2009 State Homeland Security Grant (DHS passed through to Cal OES) \$1,000,000
 - FY2010 State Homeland Security Grant (DHS passed through to Cal OES) \$1,150,000
 - FY2008 Urban Area Security Initiative(DHS passed through to Cal OES then to the Bay Area UASI as a sub-recipient) \$2,267,252

- FY2009 Urban Area Security Initiative(DHS passed through to Cal OES then to the Bay Area UASI as a sub-recipient) \$2,909,951
- FY2010 Urban Area Security Initiative(DHS passed through to Cal OES then to the Bay Area UASI as a sub-recipient) \$3,718,623
- 2011 National Justice Information Sharing Initiative (Direct from DHS BJA) \$90,240
- 2009 ARRA Funding US DOJ BJA/OJP, \$800,700

• Fiscal year periods for the NCRIC are as follows:

- FY11: 7/1/10-6/30/11
- FY12: 7/1/11-6/30/12
- FY13: 7/1/12-6/30/13
- FY14: 7/1/13-6/30/14

Additionally, for clarification, the NCRIC has not received funding yet for FY 13.

I will assume that by this letter I have satisfied your request. However, if you have any further questions or concerns please do not hesitate to contact me at your convenience.

Sincerely,

Hugh A. Cotton
Northern California Regional Intelligence Center
Privacy Officer
P.O. Box 36102
San Francisco, California 94102
HCotton@ncric.org



24/7: (866) 367-8847

Unclassified//Law Enforcement Sensitive

******* NOTICE: This e-mail message and any attached files are intended solely for the use of the addressee(s) named above in connection with official business. This communication may contain Sensitive But Unclassified information that may be statutorily or otherwise prohibited from being released without appropriate approval. Any review, use, or dissemination of this e-mail message and any attached file(s) in any form outside of the Northern California Regional Intelligence Center or the Department of Justice without express authorization is strictly prohibited.**

From: Linda Lye [mailto:llye@aclunc.org]
Sent: Tuesday, July 23, 2013 6:16 PM
To: Hugh A. Cotton
Cc: PrivacyOfficer
Subject: RE: Public Records Act Request Regarding Intelligence Gathering

Dear Mr. Cotton,

Thank you for the response and apologies for my typographical error. I did intend the third request to seek records reflecting the amount of financial support received by the Northern, not Central, California Intelligence Center. To follow up, the information I sought was somewhat different from that which you have provided. In requests 1 and 2, I sought information about the sources of funding used to support systems containing data received from automated license plate readers and suspicious activity reports, respectively. You have instead provided more general information about sources of funding received by NCRIC in general. Can you please provide information about the funding sources for the two systems referenced in requests 1 and 2. Separately, you have now provided information about NCRIC funding in FY 09, 11, and 12. Are there any *other* sources of funding, not listed below, that NCRIC received in FY 11, 12 and 13 and if so, in what amounts and for what purposes? Thanks so much for your assistance.

Best, Linda

Linda Lye
Staff Attorney, ACLU-NC

From: Hugh A. Cotton [<mailto:hcotton@ncric.org>]
Sent: Monday, July 22, 2013 4:19 PM
To: Linda Lye
Cc: PrivacyOfficer
Subject: Re: Public Records Act Request Regarding Intelligence Gathering

Dear Ms. Lye,

I am writing in response to your attached July 12, 2013 letter in which you requested information relating to the funding sources of the Northern California Regional Intelligence Center (NCRIC) for the Fiscal years 2011-12, FY 2012-13, and FY 2013-14. The NCRIC received funding for the fiscal years in question from each of the following sources:

- FY2011 State Homeland Security Grant (DHS grant passed through to Cal OES) \$2,011,000
- FY12 State Homeland Security Grant (DHS grant passed through to Cal OES) \$1,761,000
- FY11 Urban Area Security Initiative Grant (DHS passed through to Cal OES then to the Bay Area UASI as a sub-recipient) \$3,393,158
- FY12 Urban Area Security Initiative Grant (DHS passed through to Cal OES then to the Bay Area UASI as a sub-recipient) \$3,393,158
- Southwest Border Grant - FY09 Recovery Act - JAG (US DOJ-BJA) \$800,700

Additionally, you requested information related to the amount of financial support received by the Central California Intelligence Center through the Omnibus Crime Control and Safe Streets Act of 1968. The NCRIC did not receive any financial support from the Central California Intelligence Center or the Omnibus Crime Control and Safe Streets Act of 1968. I suspect this portion of your request to be a typographical error, but I have answered your question to the best of my ability based upon my understanding the question.

I will assume that by this letter I have satisfied your request. However, if you disagree or otherwise have any questions or concerns please do not hesitate to contact me at your convenience.

Hugh A. Cotton
Northern California Regional Intelligence Center
Privacy Officer
P.O. Box 36102
San Francisco, California 94102
HCotton@ncric.org



24/7: (866) 367-8847

Unclassified//Law Enforcement Sensitive

******* NOTICE: This e-mail message and any attached files are intended solely for the use of the addressee(s) named above in connection with official business. This communication may contain Sensitive But Unclassified information that may be statutorily or otherwise prohibited from being released without appropriate approval. Any review, use, or dissemination of this e-mail message and any attached file(s) in any form outside of the Northern California Regional Intelligence Center or the Department of Justice without express authorization is strictly prohibited.**

EXHIBIT 3



March 7, 2016

VIA EMAIL AND U.S. MAIL

Northern California Regional Intelligence Center

Attn: Privacy Officer

P.O. Box 36102

San Francisco, CA 94102

privacyofficer@ncric.ca.gov

re: Public Records Act request regarding Suspicious Activity Reporting Program

Dear Privacy Officer,

I am writing on behalf of the American Civil Liberties Union of Northern California to request records of the Northern California Regional Intelligence Center regarding funding for the Nationwide Suspicious Activity Reporting Initiative (“NSI”). This request is made pursuant to the California Public Records Act (Government Code §§ 6250, et. seq.) and Article I § 3(b) of the California Constitution for the following records¹:

- 1) Documents reflecting funding sources -- and identifying the federal entities that administered any such sources -- relating to information systems containing Suspicious Activity Reports.

An August 2, 2013 response by your office to a prior Public Records Act request from my office stated: “The NCRIC spent \$690,125 on the information systems containing SAR information. The funding source was from 2009 ARRA funding. The NCRIC entered into an agreement with Palantir in January of 2012. There are ongoing maintenance costs, however, the NCRIC has yet to expend such funds. Maintenance costs will likely be funded out of the UASI or SHSP funding.”

¹“Records” covered by this request include but are not limited to: internal and external correspondence (including email), memoranda, drafts, notes, outlines, policies, procedures, regulations, directives, instructions, orders, bulletins, pamphlets or brochures, scripts, handouts, analyses, evaluations, reports, summaries, writings, logs and other written records or records by any other means, including but not limited to records kept on computers, computer source and object code, electronic communications, computer disks, CD-ROM, video tapes or digital video disks.

March 7, 2016
Page 2

My current request seeks documents that reflect the funding sources for the \$690,125 expended on information systems containing SAR information, as well as documents that identify that federal entity or entities that administered such funding.

It also seeks documents that reflect any subsequent expenditures related to the information system(s) containing SAR information – in particular, the funding sources and federal entity or entities that administer such funding.

- 2) Grant documents (including grant applications as well as documentation reflecting approvals/acceptance of such grants) pertaining to any grant administered by the Office of Justice Programs from 2013 to present.

The California Public Records Act requires within ten (10) days either production of the requested documents and/or notice of the specific reasons why the materials requested (or portions thereof) are exempt from disclosure. Further, we request a summary of the information contained within any records you claim to be exempt under Government Code § 6254(f), as required by Government Code § 6254(f)(2).

Please send copies of the requested records to me at the address shown above, or email them to me at llye@aclunc.org. We request that you waive any fees that would be normally applicable to a Public Records Act request. In addition, if you have the records in electronic form you can simply email them to me without incurring any copying costs. *See Gov't. Code § 6253.9.* However, should you be unable to do so, the ACLU will reimburse your agency for the direct costs of copying these records plus postage. *See Gov't. Code § 6253(b).* If you have any questions regarding this request, please feel free to contact me at (415) 621-2493. Thank you in advance for your timely cooperation.

Sincerely,



Linda Lye
Senior Staff Attorney

Enclosure

cc: Mike Sena (msena@ncric.org)

EXHIBIT 4



Daniel J. Mahoney
Deputy Director & Privacy Officer
Northern California Regional Intelligence Center
450 Golden Gate Avenue, 14th Floor
San Francisco, CA 94102

Sent via E-Mail to:

March 21, 2016

Linda Lye - llye@aclunc.org

Ms. Lye,

In response to your California Public Records Act requests (dated March 7, 2016):

1) Documents reflecting funding sources -- and identifying the federal entities that administered any such sources -- relating to information systems containing Suspicious Activity Reports.

An August 2, 2013 response by your office to a prior Public Records Act request from my office stated: "The NCRIC spent \$690,125 on the information systems containing SAR information. The funding source was from 2009 ARRA funding. The NCRIC entered into an agreement with Palantir in January of 2012. There are ongoing maintenance costs, however, the NCRIC has yet to expend such funds. Maintenance costs will likely be funded out of the UASI or SHSP funding."

My current request seeks documents that reflect the funding sources for the \$690,125 expended on information systems containing SAR information, as well as documents that identify that federal entity or entities that administered such funding.

It also seeks documents that reflect any subsequent expenditures related to the information system(s) containing SAR information – in particular, the funding sources and federal entity or entities that administer such funding.

2) Grant documents (including grant applications as well as documentation reflecting approvals/acceptance of such grants) pertaining to any grant administered by the Office of Justice Programs from 2013 to present.

Attached in 4 separate e-mails (due to the size of the files) are documents responsive to this request.

Most Cordially,

NORTHERN CALIFORNIA REGIONAL INTELLIGENCE CENTER

Daniel J. Mahoney

Deputy Director & Privacy Officer



Department of Justice
Office of Justice Programs

Office of the Assistant Attorney General

Washington, D.C. 20531

July 15, 2009

Sheriff Greg Munks
San Mateo County
400 County Center
1st Floor
Redwood City, CA 94063-1662

Dear Sheriff Munks:

On behalf of Attorney General Eric Holder, it is my pleasure to inform you that the Office of Justice Programs has approved your application for funding under the FY 09 Recovery Act Combating Criminal Narcotics Activity Stemming from the Southern Border of the United States: Facilitating Justice Information Sharing, Collaboration and Problem Solving in the amount of \$800,700 for San Mateo County.

Enclosed you will find the Grant Award and Special Conditions documents. This award is subject to all administrative and financial requirements, including the timely submission of all financial and programmatic reports, resolution of all interim audit findings, and the maintenance of a minimum level of cash-on-hand. Should you not adhere to these requirements, you will be in violation of the terms of this agreement and the award will be subject to termination for cause or other administrative action as appropriate.

If you have questions regarding this award, please contact:

- Program Questions, Kerri Vitalo Logan, Program Manager at (202) 353-9074; and
- Financial Questions, the Office of the Chief Financial Officer, Customer Service Center (CSC) at (800) 458-0786, or you may contact the CSC at ask.ocfo@usdoj.gov.

Congratulations, and we look forward to working with you.

Sincerely,

Laurie Robinson
Acting Assistant Attorney General

Enclosures



Department of Justice
Office of Justice Programs
Office for Civil Rights

Washington, D.C. 20531

July 15, 2009

Sheriff Greg Munks
San Mateo County
400 County Center
1st Floor
Redwood City, CA 94063-1662

Dear Sheriff Munks:

Congratulations on your recent award. In establishing financial assistance programs, Congress linked the receipt of Federal funding to compliance with Federal civil rights laws. The Office for Civil Rights (OCR), Office of Justice Programs (OJP), U.S. Department of Justice is responsible for ensuring that recipients of financial aid from OJP, its component offices and bureaus, the Office on Violence Against Women (OVW), and the Office of Community Oriented Policing Services (COPS) comply with applicable Federal civil rights statutes and regulations. We at OCR are available to help you and your organization meet the civil rights requirements that come with Justice Department funding.

Ensuring Access to Federally Assisted Programs

As you know, Federal laws prohibit recipients of financial assistance from discriminating on the basis of race, color, national origin, religion, sex, or disability in funded programs or activities, not only in respect to employment practices but also in the delivery of services or benefits. Federal law also prohibits funded programs or activities from discriminating on the basis of age in the delivery of services or benefits.

Providing Services to Limited English Proficiency (LEP) Individuals

In accordance with Department of Justice Guidance pertaining to Title VI of the Civil Rights Act of 1964, 42 U.S.C. § 2000d, recipients of Federal financial assistance must take reasonable steps to provide meaningful access to their programs and activities for persons with limited English proficiency (LEP). For more information on the civil rights responsibilities that recipients have in providing language services to LEP individuals, please see the website at <http://www.lep.gov>.

Ensuring Equal Treatment for Faith-Based Organizations

The Department of Justice has published a regulation specifically pertaining to the funding of faith-based organizations. In general, the regulation, Participation in Justice Department Programs by Religious Organizations; Providing for Equal Treatment of all Justice Department Program Participants, and known as the Equal Treatment Regulation 28 C.F.R. part 38, requires State Administering Agencies to treat these organizations the same as any other applicant or recipient. The regulation prohibits State Administering Agencies from making award or grant administration decisions on the basis of an organization's religious character or affiliation, religious name, or the religious composition of its board of directors.

The regulation also prohibits faith-based organizations from using financial assistance from the Department of Justice to fund inherently religious activities. While faith-based organizations can engage in non-funded inherently religious activities, they must be held separately from the Department of Justice funded program, and customers or beneficiaries cannot be compelled to participate in them. The Equal Treatment Regulation also makes clear that organizations participating in programs funded by the Department of Justice are not permitted to discriminate in the provision of services on the basis of a beneficiary's religion. For more information on the regulation, please see OCR's website at <http://www.ojp.usdoj.gov/ocr/etfbo.htm>.

State Administering Agencies and faith-based organizations should also note that the Safe Streets Act, as amended; the Victims of Crime Act, as amended; and the Juvenile Justice and Delinquency Prevention Act, as amended, contain prohibitions against discrimination on the basis of religion in employment. Despite these nondiscrimination provisions, the Justice Department has concluded that the Religious Freedom Restoration Act (RFRA) is reasonably construed, on a case-by-case basis, to require that its funding agencies permit faith-based organizations applying for funding under the applicable program statutes both to receive DOJ funds and to continue considering religion when hiring staff, even if the statute that authorizes the funding program generally forbids considering of religion in employment decisions by grantees.

Questions about the regulation or the application of RFRA to the statutes that prohibit discrimination in employment may be directed to this Office.

Enforcing Civil Rights Laws

All recipients of Federal financial assistance, regardless of the particular funding source, the amount of the grant award, or the number of employees in the workforce, are subject to the prohibitions against unlawful discrimination. Accordingly, OCR investigates recipients that are the subject of discrimination complaints from both individuals and groups. In addition, based on regulatory criteria, OCR selects a number of recipients each year for compliance reviews, audits that require recipients to submit data showing that they are providing services equitably to all segments of their service population and that their employment practices meet equal employment opportunity standards.

Complying with the Safe Streets Act or Program Requirements

In addition to these general prohibitions, an organization which is a recipient of financial assistance subject to the nondiscrimination provisions of the Omnibus Crime Control and Safe Streets Act (Safe Streets Act) of 1968, 42 U.S.C. § 3789d(c), or other Federal grant program requirements, must meet two additional requirements: (1) complying with Federal regulations pertaining to the development of an Equal Employment Opportunity Plan (EEOP), 28 C.F.R. § 42.301-.308, and (2) submitting to OCR Findings of Discrimination (see 28 C.F.R. §§ 42.205(5) or 31.202(5)).

1) Meeting the EEOP Requirement

In accordance with Federal regulations, Assurance No. 6 in the Standard Assurances, COPS Assurance No. 8.B, or certain Federal grant program requirements, your organization must comply with the following EEOP reporting requirements:

If your organization has received an award for \$500,000 or more and has 50 or more employees (counting both full- and part-time employees but excluding political appointees), then it has to prepare an EEOP and submit it to OCR for review **within 60 days from the date of this letter**. For assistance in developing an EEOP, please consult OCR's website at <http://www.ojp.usdoj.gov/ocr/eeop.htm>. You may also request technical assistance from an EEOP specialist at OCR by dialing (202) 616-3208.

If your organization received an award between \$25,000 and \$500,000 and has 50 or more employees, your organization still has to prepare an EEOP, but it does not have to submit the EEOP to OCR for review. Instead, your organization has to maintain the EEOP on file and make it available for review on request. In addition, your organization has to complete Section B of the Certification Form and return it to OCR. The Certification Form can be found at <http://www.ojp.usdoj.gov/ocr/eeop.htm>.

If your organization received an award for less than \$25,000; or if your organization has less than 50 employees, regardless of the amount of the award; or if your organization is a medical institution, educational institution, nonprofit organization or Indian tribe, then your organization is exempt from the EEOP requirement. However, your organization must complete Section A of the Certification Form and return it to OCR. The Certification Form can be found at <http://www.ojp.usdoj.gov/ocr/eeop.htm>.

2) Submitting Findings of Discrimination

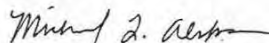
In the event a Federal or State court or Federal or State administrative agency makes an adverse finding of discrimination against your organization after a due process hearing, on the ground of race, color, religion, national origin, or sex, your organization must submit a copy of the finding to OCR for review.

Ensuring the Compliance of Subrecipients

If your organization makes subawards to other agencies, you are responsible for assuring that subrecipients also comply with all of the applicable Federal civil rights laws, including the requirements pertaining to developing and submitting an EEOP, reporting Findings of Discrimination, and providing language services to LEP persons. State agencies that make subawards must have in place standard grant assurances and review procedures to demonstrate that they are effectively monitoring the civil rights compliance of subrecipients.

If we can assist you in any way in fulfilling your civil rights responsibilities as a recipient of Federal funding, please call OCR at (202) 307-0690 or visit our website at <http://www.ojp.usdoj.gov/ocr/>.

Sincerely,



Michael L. Alston
Director

cc: Grant Manager
Financial Analyst



Department of Justice
Office of Justice Programs
Office of the Chief Financial Officer

Washington, D.C. 20531

July 15, 2009

Sheriff Greg Munks
San Mateo County
400 County Center
1st Floor
Redwood City, CA 94063 - 1662

Reference Grant Number: 2009-SS-B9-0029

Dear Sheriff Munks:

I am pleased to inform you that my office has approved the following budget categories for the aforementioned grant award in the cost categories identified below:

Category	Budget
Personnel	\$0
Fringe Benefits	\$0
Travel	\$4,300
Equipment	\$649,000
Supplies	\$0
Construction	\$0
Contractual	\$147,400
Other	\$0
Total Direct Cost	\$800,700
Indirect Cost	\$0
Total Project Cost	\$800,700
Federal Funds Approved:	\$800,700
Non-Federal Share:	\$0
Program Income:	\$0

Match is not required for this grant program.

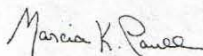
All Sole Source procurement in excess of \$100,000 requires written justification and the prior approval of OJP.

If you have questions regarding this award, please contact:

- Program Questions, Kerri Vitalo Logan, Program Manager at (202) 353-9074
- Financial Questions, the Office of Chief Financial Officer, Customer Service Center(CSC) at (800) 458-0786, or you may contact the CSC at ask.ocfo@usdoj.gov.

Congratulations, and we look forward to working with you.

Sincerely,



Marcia K. Paull
Chief Financial Officer



Department of Justice
Office of Justice Programs
Bureau of Justice Assistance

Grant

PAGE 1 OF 9

1. RECIPIENT NAME AND ADDRESS (Including Zip Code) San Mateo County 400 County Center 1st Floor Redwood City, CA 94063-1662		4. AWARD NUMBER: 2009-SS-B9-0029	
		5. PROJECT PERIOD: FROM 07/01/2009 TO 06/30/2011 BUDGET PERIOD: FROM 07/01/2009 TO 06/30/2011	
		6. AWARD DATE 07/15/2009	7. ACTION
1A. GRANTEE IRS/VENDOR NO. 946000563		8. SUPPLEMENT NUMBER 00	Initial
		9. PREVIOUS AWARD AMOUNT	\$ 0
3. PROJECT TITLE Enhancing Intelligence-Led Policing (ILP) Capabilities in the Area of Responsibility of the NCHIDTA and Northern California Regional Intelligence Center through Implementation of a Regional Intelligen		10. AMOUNT OF THIS AWARD	\$ 800,700
		11. TOTAL AWARD	\$ 800,700
12. SPECIAL CONDITIONS THE ABOVE GRANT PROJECT IS APPROVED SUBJECT TO SUCH CONDITIONS OR LIMITATIONS AS ARE SET FORTH ON THE ATTACHED PAGE(S).			
13. STATUTORY AUTHORITY FOR GRANT This project is supported under FY09 Recovery Act (BJA – Southern Border/HIDTA (Criminal Narcotics Activity)) Pub. L. No. 111-5, 123 Stat. 115, 130			
15. METHOD OF PAYMENT PAPRS			
AGENCY APPROVAL		GRANTEE ACCEPTANCE	
16. TYPED NAME AND TITLE OF APPROVING OFFICIAL Laurie Robinson Acting Assistant Attorney General		18. TYPED NAME AND TITLE OF AUTHORIZED GRANTEE OFFICIAL Greg Munks Sheriff County of San Mateo	
17. SIGNATURE OF APPROVING OFFICIAL 		19. SIGNATURE OF AUTHORIZED RECIPIENT OFFICIAL 	19A. DATE 7/21/09
AGENCY USE ONLY			
20. ACCOUNTING CLASSIFICATION CODES FISCAL YEAR FUND CODE BUD. ACT. DIV. OFC. REG. SUB. POMS AMOUNT 9 B SS 80 00 00 800700		21. ISSUGT1901	

OJP FORM 4000/2 (REV. 5-87) PREVIOUS EDITIONS ARE OBSOLETE.

OJP FORM 4000/2 (REV. 4-88)



Department of Justice
Office of Justice Programs
Bureau of Justice Assistance

**AWARD CONTINUATION
SHEET
Grant**

PAGE 2 OF 9

PROJECT NUMBER 2009-SS-B9-0029 AWARD DATE 07/15/2009

SPECIAL CONDITIONS

1. The recipient agrees to comply with the financial and administrative requirements set forth in the current edition of the Office of Justice Programs (OJP) Financial Guide.
2. The recipient acknowledges that failure to submit an acceptable Equal Employment Opportunity Plan (if recipient is required to submit one pursuant to 28 C.F.R. Section 42.302), that is approved by the Office for Civil Rights, is a violation of its Certified Assurances and may result in suspension or termination of funding, until such time as the recipient is in compliance.
3. The recipient agrees to comply with the organizational audit requirements of OMB Circular A-133, Audits of States, Local Governments, and Non-Profit Organizations, and further understands and agrees that funds may be withheld, or other related requirements may be imposed, if outstanding audit issues (if any) from OMB Circular A-133 audits (and any other audits of OJP grant funds) are not satisfactorily and promptly addressed, as further described in the current edition of the OJP Financial Guide, Chapter 19.
4. Recipient understands and agrees that it cannot use any federal funds, either directly or indirectly, in support of the enactment, repeal, modification or adoption of any law, regulation or policy, at any level of government, without the express prior written approval of OJP.
5. The recipient must promptly refer to the DOJ OIG any credible evidence that a principal, employee, agent, contractor, subgrantee, subcontractor, or other person has either 1) submitted a false claim for grant funds under the False Claims Act; or 2) committed a criminal or civil violation of laws pertaining to fraud, conflict of interest, bribery, gratuity, or similar misconduct involving grant funds. This condition also applies to any subrecipients. Potential fraud, waste, abuse, or misconduct should be reported to the OIG by -

mail:

Office of the Inspector General
U.S. Department of Justice
Investigations Division
950 Pennsylvania Avenue, N.W.
Room 4706
Washington, DC 20530

e-mail: oig.hotline@usdoj.gov

hotline: (contact information in English and Spanish): (800) 869-4499

or hotline fax: (202) 616-9881

Additional information is available from the DOJ OIG website at www.usdoj.gov/oig.

6. **RECOVERY ACT – Conflict with Other Standard Terms and Conditions**
The recipient understands and agrees that all other terms and conditions contained in this award, or in applicable OJP grant policy statements or guidance, apply unless they conflict or are superseded by the terms and conditions included here that specifically implement the American Recovery and Reinvestment Act of 2009, Public Law 111-5 (“ARRA” or “Recovery Act”) requirements. Recipients are responsible for contacting their grant managers for any needed clarifications.

Car



Department of Justice
Office of Justice Programs
Bureau of Justice Assistance

**AWARD CONTINUATION
SHEET
Grant**

PAGE 3 OF 9

PROJECT NUMBER 2009-SS-B9-0029 AWARD DATE 07/15/2009

SPECIAL CONDITIONS

- 7. **RECOVERY ACT – Access to Records; Interviews**
The recipient understands and agrees that DOJ (including OJP and the Office of the Inspector General (OIG)), and its representatives, and the Government Accountability Office (GAO), shall have access to and the right to examine all records (including, but not limited to, books, papers, and documents) related to this Recovery Act award, including such records of any subrecipient, contractor, or subcontractor.

The recipient also understands and agrees that DOJ and the GAO are authorized to interview any officer or employee of the recipient (or of any subrecipient, contractor, or subcontractor) regarding transactions related to this Recovery Act award.
- 8. **RECOVERY ACT – One-time funding**
The recipient understands and agrees that awards under the Recovery Act will be one-time awards and accordingly that its proposed project activities and deliverables are to be accomplished without additional DOJ funding.
- 9. **RECOVERY ACT – Separate Tracking and Reporting of Recovery Act Funds and Outcomes**
The recipient agrees to track, account for, and report on all funds from this Recovery Act award (including specific outcomes and benefits attributable to Recovery Act funds) separately from all other funds, including DOJ award funds from non-Recovery Act awards awarded for the same or similar purposes or programs. (Recovery Act funds may be used in conjunction with other funding as necessary to complete projects, but tracking and reporting of Recovery Act funds must be separate.)

Accordingly, the accounting systems of the recipient and all subrecipients must ensure that funds from this Recovery Act award are not commingled with funds from any other source.

The recipient further agrees that all personnel (including subrecipient personnel) whose activities are to be charged to the award will maintain timesheets to document hours worked for activities related to this award and non-award-related activities.
- 10. **RECOVERY ACT – Subawards – DUNS and CCR for Reporting**
The recipient agrees to work with its first-tier subrecipients (if any) to ensure that, no later than the due date of the recipient's first quarterly report after a subaward is made, the subrecipient has a valid DUNS profile and has an active registration with the Central Contractor Registration (CCR) database.
- 11. **RECOVERY ACT – Subawards – Monitoring**
The recipient agrees to monitor subawards under this Recovery Act award in accordance with all applicable statutes, regulations, OMB circulars, and guidelines, including the OJP Financial Guide, and to include the applicable conditions of this award in any subaward. The recipient is responsible for oversight of subrecipient spending and monitoring of specific outcomes and benefits attributable to use of Recovery Act funds by subrecipients. The recipient agrees to submit, upon request, documentation of its policies and procedures for monitoring of subawards under this award.

Car



Department of Justice
Office of Justice Programs
Bureau of Justice Assistance

**AWARD CONTINUATION
SHEET
Grant**

PAGE 4 OF 9

PROJECT NUMBER 2009-SS-B9-0029 AWARD DATE 07/15/2009

SPECIAL CONDITIONS

12. RECOVERY ACT – Recovery Act Transactions Listed in Schedule of Expenditures of Federal Awards and Recipient Responsibilities for Informing Subrecipients
(a) The recipient agrees to maintain records that identify adequately the source and application of Recovery Act funds, to maximize the transparency and accountability of funds authorized under the Recovery Act as required by the Act and in accordance with 2 CFR 215.21, "Uniform Administrative Requirements for Grants and Agreements with Institutions of Higher Education, Hospitals, and Other Non-profit Organizations" and OMB A-102 Common Rules provisions (relating to Grants and Cooperative Agreements with State and Local Governments).

(b) The recipient agrees to separately identify the expenditures for Federal awards under the Recovery Act on the Schedule of Expenditures of Federal Awards (SEFA) and the Data Collection Form (SF-SAC) required by OMB Circular A-133. This condition only applies if the recipient is covered by the Single Audit Act Amendments of 1996 and OMB Circular A-133, "Audits of States, Local Governments, and Non-Profit Organizations." This shall be accomplished by identifying expenditures for Federal awards made under the Recovery Act separately on the SEFA, and as separate rows under Item 9 of Part III on the SF-SAC by CFDA number, and inclusion of the prefix "ARRA-" in identifying the name of the Federal program on the SEFA and as the first characters in Item 9d of Part III on the SF-SAC.

(c) The recipient agrees to separately identify to each subrecipient the Federal award number, CFDA number, and amount of Recovery Act funds, and to document this identification both at the time of subaward and at the time of disbursement of funds. When a recipient awards Recovery Act funds for an existing program, the information furnished to subrecipients shall distinguish the subawards of incremental Recovery Act funds from regular subawards under the existing program.

(d) The recipient agrees to require its subrecipients to specifically identify Recovery Act funding on their SEFA information, similar to the requirements for the recipient SEFA described above. This information is needed to allow the recipient to properly monitor subrecipient expenditure of Recovery Act funds as well as facilitate oversight by the Federal awarding agencies, the DOJ OIG, and the GAO.

13. RECOVERY ACT – Reporting and Registration Requirements under Section 1512 of the Recovery Act.
(a) This award requires the recipient to complete projects or activities which are funded under the Recovery Act and to report on use of Recovery Act funds provided through this award. Information from these reports will be made available to the public.

(b) The reports are due no later than ten calendar days after each calendar quarter in which the recipient receives the assistance award funded in whole or in part by the Recovery Act.

(c) Recipients and their first-tier recipients must maintain current registrations in the Central Contractor Registration (www.ccr.gov) at all times during which they have active federal awards funded with Recovery Act funds. A Dun and Bradstreet Data Universal Numbering System (DUNS) Number (www.dnb.com) is one of the requirements for registration in the Central Contractor Registration.

(d) The recipient shall report the information described in section 1512(c) of the Recovery Act using the reporting instructions and data elements that will be provided online at www.FederalReporting.gov and ensure that any information that is pre-filled is corrected or updated as needed.

(e) The recipient shall notify the OJP program manager of submission of its section 1512(c) report at the time the report is submitted per (d) above. Notification to OJP may be either by submission of a copy of the section 1512(c) data report, or (if not practicable) by electronic notification to the OJP program manager confirming submission of the report. Failure to provide the required notification to OJP will be deemed a failure to report under section 1512(c).

REMINDEES: EARLY





Department of Justice
Office of Justice Programs
Bureau of Justice Assistance

**AWARD CONTINUATION
SHEET
Grant**

PAGE 5 OF 9

PROJECT NUMBER 2009-SS-B9-0029 AWARD DATE 07/15/2009

SPECIAL CONDITIONS

14. RECOVERY ACT – Reporting Potential Fraud, Waste, and Abuse, and Similar Misconduct

The recipient must promptly refer to the DOJ OIG any credible evidence that a principal, employee, agent, contractor, subgrantee, subcontractor, or other person has either 1) submitted a false claim for Recovery Act funds under the False Claims Act; or 2) committed a criminal or civil violation of laws pertaining to fraud, conflict of interest, bribery, gratuity, or similar misconduct involving Recovery Act funds. This condition also applies to any subrecipients. Potential fraud, waste, abuse, or misconduct should be reported to the OIG by –

mail:
Office of the Inspector General
U.S. Department of Justice
Investigations Division
950 Pennsylvania Avenue, N.W.
Room 4706
Washington, DC 20530

e-mail: oig.hotline@usdoj.gov

hotline: (contact information in English and Spanish): (800) 869-4499

or hotline fax: (202) 616-9881

Additional information is available from the DOJ OIG website at www.usdoj.gov/oig.

15. RECOVERY ACT – Protecting State and Local Government and Contractor Whistleblowers (Recovery Act, section 1553)

The recipient recognizes that the Recovery Act provides certain protections against reprisals for employees of non-Federal employers who disclose information reasonably believed to be evidence of gross mismanagement, gross waste, substantial and specific danger to public health or safety, abuse of authority, or violations of law related to contracts or grants using Recovery Act funds. For additional information, refer to section 1553 of the Recovery Act. The text of Recovery Act is available at www.ojp.usdoj.gov/recovery.

16. RECOVERY ACT – Limit on Funds (Recovery Act, section 1604)

The recipient agrees that none of the funds under this award may be used by any State or local government, or any private entity, for construction costs or any other support of any casino or other gambling establishment, aquarium, zoo, golf course, or swimming pool.

17. RECOVERY ACT – Infrastructure Investment (Recovery Act, sections 1511 and 1602)

The recipient agrees that it may not use any funds made available under this Recovery Act award for infrastructure investment absent submission of a satisfactory certification under section 1511 of the Recovery Act. Should the recipient decide to use funds for infrastructure investment subsequent to award, the recipient must submit appropriate certifications under section 1511 of the Recovery Act and receive prior approval from OJP. In seeking such approval, the recipient shall give preference to activities that can be started and completed expeditiously, and shall use award funds in a manner that maximizes job creation and economic benefits. The text of the Recovery Act (including sections 1511 and 1602) is available at www.ojp.usdoj.gov/recovery.



Department of Justice
Office of Justice Programs
Bureau of Justice Assistance

**AWARD CONTINUATION
SHEET
Grant**

PAGE 6 OF 9

PROJECT NUMBER 2009-SS-B9-0029

AWARD DATE 07/15/2009

SPECIAL CONDITIONS

18. RECOVERY ACT – Buy American Notification (Recovery Act, section 1605)

The recipient understands that this award is subject to the provisions of section 1605 of the Recovery Act (“Buy American”). No award funds may be used for iron, steel, or manufactured goods for a project for the construction, alteration, maintenance, or repair of a public building or public work, unless the recipient provides advance written notification to the OJP program office, and a Grant Adjustment Notice is issued that modifies this special condition to add government-wide standard conditions (anticipated to be published in subpart B of 2 C.F.R. part 176) that further implement the specific requirements or exceptions of section 1605.

Section 1605 of the Recovery Act prohibits use of any Recovery Act funds for a project for the construction, alteration, maintenance, or repair of a public building or public work unless all of the iron, steel, and manufactured goods used in the project are produced in the United States, subject to certain exceptions, including United States obligations under international agreements.

For purposes of this special condition, the following definitions apply:

“Public building” and “public work” means a public building of, and a public work of, a governmental entity (the United States; the District of Columbia; commonwealths, territories, and minor outlying islands of the United States; State and local governments; and multi-State, regional, or interstate entities which have governmental functions). These buildings and works may include, without limitation, bridges, dams, plants, highways, parkways, streets, subways, tunnels, sewers, mains, power lines, pumping stations, heavy generators, railways, airports, terminals, docks, piers, wharves, ways, lighthouses, buoys, jetties, breakwaters, levees, and canals, and the construction, alteration, maintenance, or repair of such buildings and works.

“Manufactured good” means a good brought to the construction site for incorporation into the building or work that has been--

- (1) Processed into a specific form and shape; or
- (2) Combined with other raw material to create a material that has different properties than the properties of the individual raw materials.

“Steel” means an alloy that includes at least 50 percent iron, between .02 and 2 percent carbon, and may include other elements.

For purposes of OJP grants, projects involving construction, alteration, maintenance, or repair of jails, detention facilities, prisons, public crime victims’ shelters, police facilities, or other similar projects will likely trigger this provision.

NOTE: The recipient is encouraged to contact the OJP program manager – in advance – with any questions concerning this condition, including its applicability to particular circumstances.



Department of Justice
Office of Justice Programs
Bureau of Justice Assistance

**AWARD CONTINUATION
SHEET
Grant**

PAGE 7 OF 9

PROJECT NUMBER 2009-SS-B9-0029 AWARD DATE 07/15/2009

SPECIAL CONDITIONS

- 19. RECOVERY ACT – Wage Rate Requirements under Section 1606 of the Recovery Act
 (a) Section 1606 of the Recovery Act requires that all laborers and mechanics employed by contractors and subcontractors on projects funded directly by or assisted in whole or in part by and through the Federal Government pursuant to the Recovery Act shall be paid wages at rates not less than those prevailing on projects of a character similar in the locality as determined by the Secretary of Labor in accordance with subchapter IV of chapter 31 of title 40, United States Code.

 Pursuant to Reorganization Plan No. 14 and the Copeland Act, 40 U.S.C. 3145, the Department of Labor has issued regulations at 29 CFR Parts 1, 3, and 5 to implement the Davis-Bacon and related Acts. Regulations in 29 CFR 5.5 instruct agencies concerning application of the standard Davis-Bacon contract clauses set forth in that section. The standard Davis-Bacon contract clauses found in 29 CFR 5.5(a) are to be incorporated in any covered contracts made under this award that are in excess of \$2,000 for construction, alteration or repair (including painting and decorating).

 (b) For additional guidance on the wage rate requirements of section 1606, contact your awarding agency. Recipients of grants, cooperative agreements and loans should direct their initial inquiries concerning the application of Davis-Bacon requirements to a particular federally assisted project to the Federal agency funding the project. The Secretary of Labor retains final coverage authority under Reorganization Plan Number 14.
- 20. RECOVERY ACT – Misuse of award funds
 The recipient understands and agrees that misuse of award funds may result in a range of penalties, including suspension of current and future funds, suspension or debarment from federal grants, recoupment of monies provided under an award, and civil and/or criminal penalties.
- 21. RECOVERY ACT – Additional Requirements and Guidance
 The recipient agrees to comply with any modifications or additional requirements that may be imposed by law and future OJP (including government-wide) guidance and clarifications of Recovery Act requirements.
- 22. RECOVERY ACT - Quarterly Financial Reports
 The recipient agrees to submit quarterly financial status reports to OJP. At present, these reports are to be submitted on-line (at [https:// grants.ojp.usdoj.gov](https://grants.ojp.usdoj.gov)) using Standard Form SF 269A, not later than 45 days after the end of each calendar quarter. The recipient understands that after October 15, 2009, OJP will discontinue its use of the SF 269A, and will require award recipients to submit quarterly financial status reports within 30 days after the end of each calendar quarter, using the government-wide Standard Form 425 Federal Financial Report form (available for viewing at [www.whitehouse.gov/ omb/ grants/ standard_forms/ ffr.pdf](http://www.whitehouse.gov/omb/grants/standard_forms/ffr.pdf)). Beginning with the report for the fourth calendar quarter of 2009 (and continuing thereafter), the recipient agrees that it will submit quarterly financial status reports to OJP on-line (at [https:// grants.ojp.usdoj.gov](https://grants.ojp.usdoj.gov)) using the SF 425 Federal Financial Report form, not later than 30 days after the end of each calendar quarter. The final report shall be submitted not later than 90 days following the end of the grant period.

inform
B. ADLER



Department of Justice
Office of Justice Programs
Bureau of Justice Assistance

**AWARD CONTINUATION
SHEET
Grant**

PAGE 8 OF 9

PROJECT NUMBER 2009-SS-B9-0029 AWARD DATE 07/15/2009

SPECIAL CONDITIONS

- 23. RECOVERY ACT – Provisions of Section 1512(c)
The recipient understands that section 1512(c) of the Recovery Act provides as follows:

Recipient Reports- Not later than 10 days after the end of each calendar quarter, each recipient that received recovery funds from a Federal agency shall submit a report to that agency that contains--
(1) the total amount of recovery funds received from that agency;
(2) the amount of recovery funds received that were expended or obligated to projects or activities; and
(3) a detailed list of all projects or activities for which recovery funds were expended or obligated, including--
(A) the name of the project or activity;
(B) a description of the project or activity;
(C) an evaluation of the completion status of the project or activity;
(D) an estimate of the number of jobs created and the number of jobs retained by the project or activity; and
(E) for infrastructure investments made by state and local governments, the purpose, total cost, and rationale of the agency for funding the infrastructure investment with funds made available under this Act, and name of the person to contact at the agency if there are concerns with the infrastructure investment.
(4) Detailed information on any subcontracts or subgrants awarded by the recipient to include the data elements required to comply with the Federal Funding Accountability and Transparency Act of 2006 (Public Law 109-282), allowing aggregate reporting on awards below \$25,000 or to individuals, as prescribed by the Director of the Office of Management and Budget.
- 24. RECOVERY ACT – Inapplicability of General Non-supplanting Requirement to this Award
The recipient understands that, for purposes of this award, the general non-supplanting requirement of the OJP Financial Guide (Part II, Chapter 3) does not apply.
- 25. The recipient agrees that any information technology system funded or supported by OJP funds will comply with 28 C.F.R. Part 23, Criminal Intelligence Systems Operating Policies, if OJP determines this regulation to be applicable. Should OJP determine 28 C.F.R. Part 23 to be applicable, OJP may, at its discretion, perform audits of the system, as per the regulation. Should any violation of 28 C.F.R. Part 23 occur, the recipient may be fined as per 42 U.S.C. 3789g(c)-(d). Recipient may not satisfy such a fine with federal funds.
- 26. To support public safety and justice information sharing, OJP requires the grantee to use the National Information Exchange Model (NIEM) specifications and guidelines for this particular grant. Grantee shall publish and make available without restriction all schemas generated as a result of this grant to the component registry as specified in the guidelines. For more information on compliance with this special condition, visit <http://www.niem.gov/implementationguide.php>.
- 27. To avoid duplicating existing networks or IT systems in any initiatives funded by BJA for law enforcement information sharing systems which involve interstate connectivity between jurisdiction, such systems shall employ, to the extent possible, existing networks as the communication backbone to achieve interstate connectivity, unless the grantee can demonstrate to the satisfaction of BJA that this requirement would not be cost effective or would impair the functionality of an existing or proposed IT system.
- 28. The grantee agrees that within 120 days of award, for any law enforcement task force funded with these funds, the task force commander, agency executive, task force officers, and other task force members of equivalent rank, will complete required online (internet-based) task force training to be provided free of charge through BJA's Center for Task Force Integrity and Leadership. This training will address task force effectiveness as well as other key issues including privacy and civil liberties/rights, task force performance measurement, personnel selection, and task force oversight and accountability. Additional information will be provided by BJA regarding the required training and access methods via BJA's web site and the Center for Task Force Integrity and Leadership (www.ctfli.org).

IMPORTANT
CALENDAR



Department of Justice
Office of Justice Programs
Bureau of Justice Assistance

**AWARD CONTINUATION
SHEET
Grant**

PAGE 9 OF 9

PROJECT NUMBER 2009-SS-B9-0029


AWARD DATE 07/15/2009

SPECIAL CONDITIONS

- 29. All contracts under this award should be competitively awarded unless circumstances preclude competition. When a contract amount exceeds \$100,000 and there has been no competition for the award, the recipient must comply with rules governing sole source procurement found in the current edition of the OJP Financial Guide.
- 30. No portion of these federal grant funds shall be used towards any part of the annual cash compensation of any employee of the grantee whose total annual cash compensation exceeds 110% of the maximum salary payable to a member of the Federal government's Senior Executive Service at an agency with a Certified SES Performance Appraisal System for that year.

This prohibition may be waived on an individual basis at the discretion of the Assistant Attorney General for OJP.
- 31. RECOVERY ACT - Active CCR Registration
The recipient agrees expeditiously to obtain active registration with the Central Contractor Registration (CCR) database, and to notify the program office in writing of its registration. Following satisfaction of this requirement, a Grant Adjustment Notice will be issued to remove this special condition.

Alter to take care of

 Department of Justice Office of Justice Programs Bureau of Justice Assistance		GRANT MANAGER'S MEMORANDUM, PT. I: PROJECT SUMMARY Grant	
PROJECT NUMBER		PAGE 1 OF 1	
2009-SS-B9-0029			
This project is supported under FY09 Recovery Act (BJA – Southern Border/HIDTA (Criminal Narcotics Activity)) Pub. L. No. 111-5, 123 Stat. 115, 130			
1. STAFF CONTACT (Name & telephone number)		2. PROJECT DIRECTOR (Name, address & telephone number)	
Kerri Vitalo Logan (202) 353-9074		Michelle Mojas Grant Administrator 400 County Center Third Floor 3rd Floor Redwood City, CA 94063-1662 (650) 363-1974	
3a. TITLE OF THE PROGRAM		3b. POMS CODE (SEE INSTRUCTIONS ON REVERSE)	
BJA FY 09 Recovery Act Combating Criminal Narcotics Activity Stemming from the Southern Border of the United States: Facilitating Justice Information Sharing, Collaboration and Problem Solving			
4. TITLE OF PROJECT			
Enhancing Intelligence-Led Policing (ILP) Capabilities in the Area of Responsibility of the NCHIDTA and Northern California Regional Intelligence Center through Implementation of a Regional Intelligen			
5. NAME & ADDRESS OF GRANTEE		6. NAME & ADDRESS OF SUBGRANTEE	
San Mateo County 400 County Center 1st Floor Redwood City, CA 94063-1662			
7. PROGRAM PERIOD		8. BUDGET PERIOD	
FROM: 07/01/2009 TO: 06/30/2011		FROM: 07/01/2009 TO: 06/30/2011	
9. AMOUNT OF AWARD		10. DATE OF AWARD	
\$ 800,700		07/15/2009	
11. SECOND YEAR'S BUDGET		12. SECOND YEAR'S BUDGET AMOUNT	
13. THIRD YEAR'S BUDGET PERIOD		14. THIRD YEAR'S BUDGET AMOUNT	
15. SUMMARY DESCRIPTION OF PROJECT (See instruction on reverse)			
The State and Local Law Enforcement Assistance Program: Combating Criminal Narcotics Activity Stemming from the Southern border of the United States under the American Recovery and Reinvestment Act of 2009 is designed to provide resources for hiring, retention, assistance, and equipment to local law enforcement along the Southern border and in High-Intensity Drug Trafficking Areas in order to combat criminal narcotics activity stemming from the Southern border of the United States. For the purpose of this solicitation, the term "criminal narcotics activity" includes all drugs controlled by the Controlled Substance Act 21 USC Section 801.			

OJP FORM 4000/2 (REV. 4-88)

Under Category III: Facilitating Justice Information Sharing, Collaboration, and Problem Solving, San Mateo County, in conjunction with the San Mateo Sheriff's Office and the Northern California High-Intensity Drug Trafficking Area (NCHIDTA), will use the grant funds to enhance Intelligence-Led Policing capabilities through the implementation of a Regional Intelligence Management System (IMS). The region's law enforcement agencies currently lack an automated intelligence management system. Mexican drug trafficking organizations facilitate national-level distribution of wholesale quantities of illicit drugs from the San Francisco Bay Area to drug markets throughout the country. San Mateo County will leverage existing partnerships forged through NCHIDTA and the Northern California Regional Intelligence Center to provide the IMS. Grant funds will define Memoranda of Agreement, acquire the IMS, complete initial system implements, provide training, and incrementally add data sources.

CA/NCF



Department of Justice
Office of Justice Programs
Bureau of Justice Assistance

Washington, D.C. 20531

Memorandum To: Official Grant File

From: Maria Berry, Environmental Coordinator

Subject: Categorical Exclusion for San Mateo County

The State and Local Law Enforcement Assistance Program: Combating Criminal Narcotics Activity Stemming from the Southern Border of the United States under the American Recovery and Reinvestment Act of 2009 seeks to address the needs of state, local, and tribal law enforcement agencies engaged in combating the flow of illicit narcotics across the Southern border of the United States with Mexico, while simultaneously preserving and creating jobs and promoting economic recovery. Awards under this program will be used to provide resources for hiring and retention of, and assistance and equipment to local law enforcement along the Southern border and in High-Intensity Drug Trafficking Areas.

None of the following activities will be conducted either under the OJP federal action or a related third party action:

- (1) new construction;
- (2) any renovation or remodeling of a property located in an environmentally or historically sensitive area, including property, (a) listed on or eligible for listing on the National Register of Historic Places, or (b) located within a 100-year flood plain, a wetland, or habitat for an endangered species;
- (3) a renovation that will change the basic prior use of a facility or significantly change its size;
- (4) research and technology whose anticipated and future application could be expected to have an effect on the environment; and
- (5) implementation of a program involving the use of chemicals.

Consequently, an agency-wide analysis has determined that the program meets the Office of Justice Programs' (OJP) criteria for a categorical exclusion under the provisions of 28 CFR, Part 61, Appendix D, paragraph 4(b).

EXHIBIT 5

OFFICE OF JUSTICE PROGRAMS

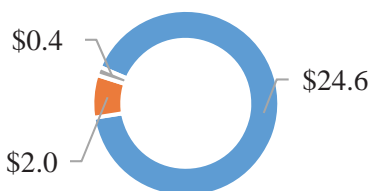
Program Name: Regional Information Sharing Systems (RISS)

FY 2017 Request

Total Funding: \$25.0M
Vs. FY 2016 Enacted: -\$10.0M

FY 2014 Activities Chart

(\$ in millions)



- Awards to the Regional RISS Centers
- RISS Information Sharing and Network Technology Support
- Collaboration Support and Technical Assistance

Program Description

Purpose: To enable multi-jurisdictional information sharing across law enforcement and criminal justice agencies at all levels to resolve criminal cases while promoting officer safety.

This program supports federal, state, local, territorial, and tribal law enforcement agencies and other criminal justice agencies through the six regional RISS centers by providing the following services:

- A secure online information and intelligence sharing network;
- Officer safety information and deconfliction services;
- Investigative and analytical support services;
- Loans of specialized investigative equipment and confidential investigative funds; and
- Training, conferences, and publications designed to assist RISS users in investigating and prosecuting regional, national, and transnational criminal activity.

Authorizing Legislation: Omnibus Crime Control and Safe Streets Act of 1968 (42 USC 3796h(d)) as amended

Administering Agency: Bureau of Justice Assistance (BJA)

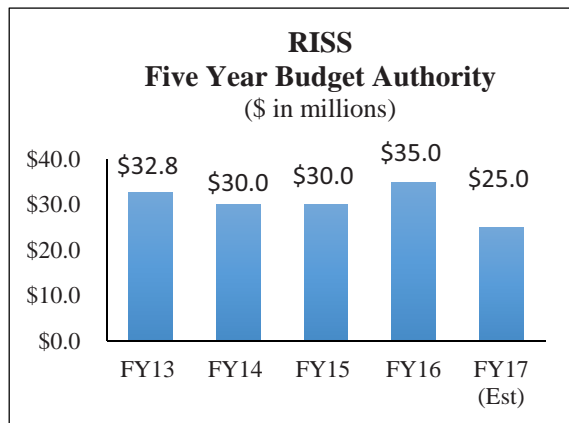
DOJ Strategic Objective 3.1: Promote and strengthen relationships and strategies for the administration of justice with law enforcement agencies, organizations, prosecutors, and defenders through innovative leadership and programs

Who Can Apply for Funding: The six regional RISS Centers and the RISS Technology Support Center

How Funds are Distributed: Discretionary grants are awarded on an annual basis based the number of users each regional center serves, anticipated needs for the coming year, and overall RISS Program funding levels.

Program Goals:

- 1) Recruit more law enforcement agencies – particularly small agencies that would benefit tremendously from the RISS resources such as analysts, equipment, information-sharing, and trainings. Currently, RISS has about 9,000 member agencies but there are over 15,000 agencies in the country.
- 2) Work in conjunction with other national data sources to create a nationwide subject deconfliction search capability to allow law enforcements agencies to know when other agencies are investigating the same subject (individual, type of crime, etc.). Currently, only event deconfliction exists on a nationwide basis which is limited to a particular time, date, and location.
- 3) Annually, RISS aims to increase the number of search requests for information by 3%.



Accomplishments:

- RISS staff responded to over 184,000 requests for intelligence research support.
- Responded to 5.6 million requests through the automated federated search tool.

- Produced over 32,000 analytical products –such as link charts, telephone toll analysis, and crime scene diagrams – to support criminal investigations. RISS also provides computer forensics and video and audio enhancement services at some centers.
- Loans over 4,500 pieces of specialized equipment annually to agencies which could not afford to buy it.
- Increased to 26 (from 19) in FY 2011 the number of RISS Watch Centers where dedicated staff identify conflicts in law enforcement operations and inform officers.
- Sponsored or co-sponsored 952 training opportunities and helped train over 44,000 individuals.
- RISS and partner organizations announced in mid-2015 the integration of the three nationally-recognized event deconfliction systems¹ to create a single nationwide event deconfliction capability for officer safety.

FY 2017 Proposed Policy Changes to the Program: N/A

FY 2017 Proposed Funding Changes to the Program: N/A

Application and Award History

(\$ in millions)	FY 2013	FY 2014	FY 2015	FY 2016	FY 2017
Amount Appropriated	\$32.8	\$30.0	\$30.0	\$35.0	\$25.0 Requested
Total Funding Awarded [^]	\$29.6	\$27.0	\$27.0	TBD	TBD
Awards to Regional RISS Centers:					
1. Mid Atlantic –Great Lakes (MAGLOCLN)	\$4.6	\$4.4	\$4.1	TBD	TBD
2. Mid-States (MOCIC)	\$2.7	\$4.0	\$3.8	TBD	TBD
3. New England (NESPIN)	\$3.2	\$3.1	\$2.9	TBD	TBD
4. Rocky Mountain (RMIN)	\$4.6	\$4.3	\$4.1	TBD	TBD
5. “Regional” Southern States (ROCIC)	\$4.5	\$4.4	\$4.2	TBD	TBD
6. Western States (WSIN)	\$4.6	\$4.4	\$4.3	TBD	TBD
Award to RISS Information Sharing and Network Technology Support Center	\$3.6	\$2.0	\$3.5	TBD	TBD
Award to RISS Collaboration Support and Technical Assistance	\$0.4	\$0.4	\$0.0	TBD	TBD

[^] Total Funding Awarded does not include funds used for management and administration, peer review, or other authorized purposes.

For additional information, please visit: <http://www.riss.net/>.

¹ Case Explorer, SAFETNet*, and RISSafe

EXHIBIT 6

MAGLOCLN MOCIC NESPIN RMIN ROCIC WSIN

Home Contact Us Facebook FAQ Help Logon



A Proven Resource for Law Enforcement™
Regional Information Sharing Systems®



28 CFR Part 23 Frequently Asked Questions

Guidelines

- [28 CFR Part 23 Guideline](#)
- [28 CFR Part 23 Policy Clarification](#)

What is Criminal Intelligence Systems Operating Policies (Federal Regulation 28 CFR Part 23)?

Criminal Intelligence Systems Operating Policies (Federal Regulation 28 CFR Part 23) is a guideline for law enforcement agencies. It contains implementing standards for operating federally grant-funded multijurisdictional criminal intelligence systems. It specifically provides guidance in five primary areas: submission and entry of criminal intelligence information, security, inquiry, dissemination, and review-and-purge process. Criminal Intelligence Systems Operating Policies (Federal Regulation 28 CFR Part 23) does not provide specific, detailed information on how the standards should be implemented by the operating agency but, instead, provides the ability for each agency to develop its own policies and procedures.

What criminal intelligence systems are affected by Criminal Intelligence Systems Operating Policies (Federal Regulation 28 CFR Part 23)?

Criminal Intelligence Systems Operating Policies (Federal Regulation 28 CFR Part 23) standards apply to all multijurisdictional criminal intelligence systems operating under Title I of the Omnibus Crime Control and Safe Streets Act of 1968, as amended. This includes any Office of Justice Programs and Bureau of Justice Assistance programs such as RISS, the Byrne Formula or Discretionary Grants Programs, the Local Law Enforcement Block Grants (LLEBG) Program, and Community Oriented Policing Services (COPS) grants. Many state and local law enforcement agencies have voluntarily adopted, as an agency policy, the operating standards of Criminal Intelligence Systems Operating Policies (Federal Regulation 28 CFR Part 23).

Where can I get more information about 28 CFR Part 23?

The Institute for Intergovernmental Research (IIR) is a Florida-based nonprofit research and training organization specializing in law enforcement, juvenile justice, and criminal justice issues. They provide information, technical assistance, and training on 28 CFR Part 23. For additional information, please visit:

<http://www.iir.com/28CFR>

Policy

- Policy Governance
- Privacy Policy
- Social Media Policy
- RISSProp Policy
- OJP

RISS Centers

- MAGLOCLN
- MOCIC
- NESPIN
- RMIN
- ROCIC
- WSIN

RISS Resources

- RISS Overview
- RISSafe
- RISSIntel
- RISS ATIX
- RISSGang
- Analytical Products
- Confidential Funds
- Equipment Loans
- Field Services Support
- Training and Publications

Miscellaneous

- Federation Partners
- RISS Insider
- RISS Impact Website
- Annual Report
- Help
- Contact Us
- Facebook

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

BENJAMIN C. MIZER
Principal Deputy Attorney General
ANTHONY J. COPPOLINO
Deputy Branch Director
KIERAN G. GOSTIN
Trial Attorney
D.C. Bar No. 1019779

Civil Division, Federal Programs Branch
U.S. Department of Justice
P.O. Box 883
Washington, D.C. 20044
Telephone: (202) 353-4556
Facsimile: (202) 616-8460
E-mail: kieran.g.gostin@usdoj.gov

Attorneys for Federal Defendants

**UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

WILEY GILL; JAMES PRIGOFF; TARIQ
RAZAK; KHALID IBRAHIM; and AARON
CONKLIN,

Plaintiffs,

v.

DEPARTMENT OF JUSTICE, *et al.*,

Defendants.

No. 3:14-cv-03120 (RS)(KAW)

**DEFENDANTS' NOTICE OF MOTION
FOR SUMMARY JUDGMENT AND
MEMORANDUM IN SUPPORT**

Hearing Date: December 8, 2016
Time: 1:30 PM

TABLE OF CONTENTS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

INTRODUCTION..... 1

 I. Statutory and Regulatory Background..... 5

 II. The Nationwide Suspicious Activity Reporting Initiative 6

 III. The Functional Standard for Suspicious Activity Reporting 7

 IV. Criminal Intelligence Systems Funded by the Omnibus Act 10

STANDARD OF REVIEW 12

ARGUMENT..... 13

 I. Plaintiffs’ Notice-and-Comment Claim Fails 13

 A. The Functional Standard is Not a Legislative Rule Subject to Notice-and-Comment Rulemaking..... 14

 B. The PM-ISE’s Process for Formulating the Functional Standard Adequately Protected Plaintiffs’ Substantive and Procedural Interests 18

 II. Plaintiffs’ Arbitrary-and-Capricious Claim Fails 22

 A. Plaintiffs’ Have Brought a Facial Challenge but Are Unable to Satisfy the Requirements Needed to Succeed on Such Challenge 22

 B. Even if Plaintiffs Had Raised an As-Applied Challenge, Such a Challenge Would be Unsuccessful..... 25

 C. The Challenged Decision Was Not Arbitrary or Capricious 28

 1. The APA’s Arbitrary-and-Capricious Standard 28

 2. The Adoption of the “Reasonably Indicative” Operational Concept..... 29

 3. The Rejection of the “Reasonable Suspicion” Standard 31

 III. Remand Without Vacatur Would Be the Only Appropriate Remedy 33

CONCLUSION 35

1 *Brock*, 796 F.2d at 537. The Court further instructed courts to look to the “language and
2 structure” of an agency pronouncement in determining whether it is a legislative rule or a
3 general statement of policy. *Mada-Luna*, 813 F.2d at 1015.

4 Applying this framework, it is clear that the Functional Standard, which is replete
5 with language indicating that it constitutes policy guidance, is not a legislative rule. Among
6 other things, the Functional Standard states that:

- 7
- 8 • The Functional Standard is “limited to *describing* the ISE-SAR process and
associated information exchanges,” A.R. at 414 (emphasis added);
 - 9 • The Functional Standard is intended to promote the “*standardized and consistent*
10 *sharing*” of SARs, *id.* at 422 (emphasis added);
 - 11 • The “ISE-SAR process offers a *standardized means* for identifying and sharing ISE-
12 SARs and applying data analytic tools to the information,” *id.* at 424 (emphasis
added);
 - 13 • “The NSI establishes *standardized processes and policies*,” *id.* at 416 (emphasis added);
14 and
 - 15 • The Functional Standard “*describes the structure, content and products* associated with
16 processing, integrating, and retrieving IS-SARs by ISE agencies participating in
the NSI,” *id.* at 417 (emphasis added).

17 According to its own terms, therefore, the Functional Standard is descriptive in nature: It
18 describes a standardized process (developed through a collaborative effort among NSI
19 participants) for sharing SARs. Consistent with that descriptive purpose, the Functional
20 Standard does not use any imperative terms (*e.g.*, “shall”) when describing the process for
21 sharing SARs within the NSI. Indeed, the Functional Standard explicitly provides that it
22 may be “customized” for “unique communities.” *Id.* at 429.

23 The treatment of the “reasonably indicative” operational concept in the Functional
24 Standard further emphasizes that this agency pronouncement is a statement of policy rather
25 than a binding legislative rule. The first version of the Functional Standard stated that NSI
26 participants may share SARs after determining that they are potentially related to terrorism.
27

1 A.R. at 80. In response to concerns raised by advocacy groups, the subsequent versions of
2 the Functional Standard have explained that a SAR has a potential nexus to terrorism when
3 it is “reasonably indicative of pre-operational planning associated with terrorism.” *Id.* at 193,
4 200, 427. Rather than describing the term “reasonably indicative” as a binding standard or
5 rule, however, the Functional Standard describes it as an “operational concept,” *id.* at 417,
6 that requires the application “professional judgment” in light of the “available context, facts,
7 and circumstances,” *id.* at 427. *See also id.* at 428 (stating that the vetting of SAR is an
8 “analytical process . . . subject to further review and validation,” and that SARs submitted to
9 an information-sharing system used in connection with the NSI remain under the
10 “ownership and control” of the submitting organization).⁷ In sum, the “reasonably
11 indicative” operational concept acts as a guidepost for NSI participants within the
12 Functional Standard’s framework. It is not a strict legal standard or rule with which NSI
13 participants must comply or else face sanction.

14 Indeed, the Functional Standard does not even contemplate the possibility of
15 sanctions being imposed on NSI participants. The regulation on which Plaintiffs’ base their
16 substantive claims in this case, 28 C.F.R. Part 23, provides a useful contrast in this regard.
17 Unlike the Functional Standard, 28 C.F.R. Part 23 explicitly states that the “criminal
18 intelligence systems” subject to its requirements “shall” comply with certain operating
19 principles. 28 C.F.R. § 23.20. And consistent with the mandatory nature of that regulation,
20 the OJP and Congress have both established specific mechanisms for monitoring whether
21

22
23 ⁷ Prior to determining whether a SAR is reasonably indicative of pre-operational planning
24 associated with terrorism, the Functional Standard also instructs analysts to compare the
25 behavior reported in the SAR against to a list of sixteen pre-operational behaviors that may
26 be associated with terrorism. A.R. at 427. The Functional Standard describes this list of
27 behaviors as “criteria guidance,” states that the application of these criteria requires the
analyst to take into account “the context, facts, and circumstances” of the observed
behavior, and emphasizes “the importance of having a trained analyst or investigator”
conduct this analysis. *Id.* at 454–64.

1 *see* 28 C.F.R. §§ 23.30, 23.40, or imposing a fine up to \$10,000 on that entity, *see* 42 U.S.C. §
 2 3789g(d). And the APA itself does not supply a separate cause of action to permit judicial
 3 review of an agency’s decision whether or not to take those sorts of enforcement actions
 4 because any such decision is an inherently discretionary act.¹¹ In short, Congress left it to the
 5 OJP to decide whether the standards in 28 C.F.R. Part 23, which Plaintiffs ask this Court to
 6 impose, are being properly applied and to sanction any violation.

7 Second, even if Plaintiffs were able to overcome the presumption against
 8 reviewability of enforcement decisions, their as-applied APA challenge would fail because
 9 the administrative record does not support a finding that an information-sharing system used
 10 in connection with the NSI is subject to 28 C.F.R. Part 23. As Functional Standard 1.5.5
 11 clarifies, the only NSI information-sharing system that is currently in operation is the NSI
 12 SAR Data Repository, which is operated by the FBI within its eGuardian system. A.R. at
 13 415. The FBI, however, does not receive any Omnibus Act funding for eGuardian or the
 14 NSI SAR Data Repository. The administrative record is devoid of any suggestion that the
 15 FBI receives such funding. And Defendants have further submitted a declaration from the
 16 OJP, which is exclusively responsible for providing federal grants under the Omnibus Act,
 17 establishing that the FBI has not and does not receive Omnibus Act funding for eGuardian
 18 or the NSI SAR Data Repository. *See* Decl. of Marylynn B. Atsatt, attached as Exhibit B.
 19 Accordingly, any attempt to require enforcement of 28 C.F.R. Part 23 against the FBI based
 20 on its operation of eGuardian would be meritless.

21
 22

24 ¹¹ For example, to determine whether to enforce 28 C.F.R. Part 23 against the operator of an
 25 information-sharing system, the OJP must determine whether the information-sharing
 26 system is a “criminal intelligence system” as that term is defined by Part 23, whether the
 27 information-sharing system operates through support of the Omnibus Act, and whether
 enforcement would serve the underlying purposes of the relevant statutory and regulatory
 framework.

28

1 C. The Challenged Decision Was Not Arbitrary or Capricious

2 Aside from the significant threshold problems with Plaintiffs' claim—*i.e.*, that the
3 OJP has discretion to apply 28 C.F.R. Part 23 and that the only NSI information-sharing
4 system currently in operation is not supported by the funding source that is the basis for that
5 regulation—there is also ample support in the administrative record for the PM-ISE's
6 decision to use the “reasonably indicative” operational concept rather than the “reasonable
7 suspicion” standard. The PM-ISE, based in part on a recommendation by an advocacy
8 organization, adopted the “reasonably indicative” operational concept in Functional
9 Standard 1.5 because it determined that this operational concept reflected the appropriate
10 balance between the competing interests of national security, on the one hand, and privacy
11 and civil liberties, on the other hand. The PM-ISE later rejected the recommendation (again
12 by certain advocacy organizations) that it replace the “reasonably indicative” operational
13 concept with the “reasonable suspicion” standard in Functional Standard 1.5.5 because the
14 PM-ISE determined that use of this standard was not feasible in light of the objectives of the
15 NSI. Neither of those decisions was unlawful under APA standards.

16 1. *The APA's Arbitrary-and-Capricious Standard*

17 Judicial review under the APA's arbitrary-and-capricious standard is deferential and
18 narrow. Section 706(2)(A) requires a reviewing court to uphold agency action unless it is
19 “arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law.”
20 5 U.S.C. § 706(2)(A). Under this standard, “[i]t is not the reviewing court's task to make its
21 own judgment about the appropriate outcome. Congress has delegated that responsibility to
22 the agency. The court's responsibility is narrower: to determine whether the agency
23 complied with the procedural requirements of the APA.” *San Luis & Delta-Mendota Water*
24 *Auth. v. Locke*, 776 F.3d 971, 994 (9th Cir. 2014).

25 Accordingly, as the Supreme Court has explained, an agency rule (or in this case,
26 functional standard) may only be deemed unlawful under the APA, if the agency has:

1 [1] relied on factors which Congress has not intended it to consider, [2]
2 entirely failed to consider an important aspect of the problem, [3] offered an
3 explanation for its decision that runs counter to the evidence before the
agency, or [4] is so implausible that it could not be ascribed to a difference in
view or the product of agency expertise.

4 *Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983).

5 Plaintiffs' allegations asserting that the use of the "reasonably indicative" operational
6 concept implicates constitutional concerns under the First Amendment, *see, e.g.*, Am. Compl.,
7 ECF No. 70, ¶¶ 1, 3–4, 29, 38, does not alter this standard of review. *See F.C.C. v. Fox*
8 *Television Stations, Inc.*, 556 U.S. 502, 516 (2009). If Plaintiffs' contention is that the
9 Functional Standard is unconstitutional, they could have asserted that claim. But Plaintiffs
10 did not do so, and they may not alter the deferential arbitrary-and-capricious standard by
11 suggesting that the agency action being reviewed may implicate constitutional concerns.

12 2. *The Adoption of the "Reasonably Indicative" Operational Concept*

13 Applying the deferential APA standard, there is ample evidence in the administrative
14 record supporting the reasonableness of the PM-ISE's determination to adopt the
15 "reasonably indicative" operational concept. Pursuant to its statutory authorization, the PM-
16 ISE was directed to develop a framework for the sharing of SAR information among federal,
17 state, local, tribal, and territorial entities that balanced the need of law enforcement to have
18 access to pertinent SARs and the privacy and civil liberty interests of individuals. The PM-
19 ISE considered these competing factors, as well as the input from NSI stakeholders and
20 advocacy organizations, and selected the "reasonably indicative" operational concept. That
21 decision-making process met the minimal standards of rationality imposed by the APA and
22 should not be disturbed by this Court.

23 Following the release of Functional Standard 1.5, which was the first version of the
24 Functional Standard to use the "reasonably indicative" operational concept, the PM-ISE
25 provided a concise explanation of the reasons for its decision to provide that guidance:

26 The use of the "reasonably indicative" determination process allows
27 supervisors at source agencies and trained analysts and investigators at fusion

1 centers and other agencies to have a uniform process that will result in better
2 quality SARs and the posting of more reliable ISE-SARs to the ISE Shared
3 Spaces, while at the same time enhancing privacy, civil rights, and civil
4 liberties protections. Furthermore, this revision improves mission
5 effectiveness and enables NSI participating agency personnel to identify and
6 address, in a more efficient manner, potential criminal and terrorism threats
7 by using more narrowly targeted language. Finally, better quality SARs
8 should result in a sufficiently high quality of information enabling agencies
9 and analysts to “connect the dots” while not producing so much information
10 as to overwhelm agency analytical capacity.

11 In addition, the “reasonably indicative” determination is an essential privacy,
12 civil rights, and civil liberties protection because it emphasizes a behavior-
13 focused approach to identifying suspicious activity and mitigates the risk of
14 profiling based upon race, ethnicity, national origin, or religious affiliation or
15 activity.

16 A.R. at 281–82. The PM-ISE, in other words, adopted the “reasonably indicative”
17 operational concept based on a determination that it would promote the sharing of useful
18 SAR information across jurisdictional lines while protecting privacy and civil liberties to the
19 greatest extent practicable.

20 That decision was consistent with the PM-ISE’s statutory mandate. Congress, as
21 noted, directed the PM-ISE to issue “procedures, guidelines, instructions, and functional
22 standards, as appropriate, for the management, development, and proper operation of the
23 ISE” that were consistent with guidance provided by the President, the Director of National
24 Intelligence, and the Director of the Office of Management and Budget. 6 U.S.C.
25 § 485(f)(2)(A)(iii). None of these entities instructed the PM-ISE to adopt any particular
26 standard for the sharing of SAR information among federal, state, local, tribal, and territorial
27 entities. Instead, they presented the PM-ISE with the difficult task of developing a
28 framework for the sharing of SARs that balanced two competing factors: (1) the law
enforcement need to have access to SAR information and (2) the protection of privacy
interests and civil liberties. *See* A.R. at 2, 9, 21, 123, 165; Suppl. A.R. at 33–33.

The PM-ISE’s decision reflects a careful balancing of those factors. Consistent with
the collaborative approach to the NSI, the PM-ISE solicited input from NSI participants and

1 advocacy organizations based on their experience with the NSI following the release of
2 Functional Standard 1.0. Based on the input received from those entities, the PM-ISE
3 selected the “reasonably indicative” operational concept because it determined that this
4 operational concept would allow for the effective sharing of SARs while protecting privacy
5 and civil liberties. Indeed, as noted, it was an advocacy organization that recommended
6 inclusion of the “reasonably indicative” operational concept. There is no basis for Plaintiffs’
7 assertion that this decision reflects a failure to consider the factors mandated by statute or is
8 otherwise unlawful.

9 *3. The Rejection of the “Reasonable Suspicion” Standard*

10 The PM-ISE also acted in a manner consistent with its statutory mandate in
11 considering and rejecting a proposal by certain advocacy organizations to replace the
12 “reasonably indicative” operational concept in the Functional Standard with the “reasonable
13 suspicion” standard in 28 C.F.R. Part 23. *See* A.R. at 330-34, 345. The Functional Standard
14 and 28 C.F.R. Part 23 were issued by two separate federal agencies (the PM-ISE and the
15 OJP), pursuant to two separate statutory schemes (the IRTPA and the Omnibus Act), to
16 support two different law enforcement processes (the sharing of tips and leads and the
17 collection of criminal intelligence). Neither the APA nor any other federal law requires these
18 agencies to adopt the same standards for separate and distinct law enforcement mechanisms.

19 The distinction between tips and leads (for SARs) and criminal intelligence is well
20 developed in law enforcement. *See* A.R. at 162–74. Criminal intelligence is the product of
21 an investigation that seeks to identify specific individuals and organizations engaged in
22 criminal activity and to gather information about the criminal conduct in which they are
23 engaged. *See id.* at 164 (defining “Criminal Intelligence Data” as “[i]nformation deemed
24 relevant to the identification of and criminal activity engaged in by an individual or
25 organization reasonably suspected of involvement in criminal activity.”). SARs, in contrast,
26 are reports of the initial tips and leads that law enforcement receive from a variety of sources
27

1 about suspicious activities. *See id.* at 164 (defining “Tips and Leads Data” as an
2 “[u]ncorroborated report or information generated from inside or outside the agency that
3 alleges or indicates some form of criminal activity”); *id.* at 168 (explaining that “SARs” are
4 “tips and leads”). Once collated and analyzed with correlating pieces of data from other
5 sources, this SAR information may lead law enforcement to initiate a criminal investigation
6 seeking to gather information about specific individuals and organizations suspected of
7 being engaged in criminal conduct. *See id.* at 165–66. But this is a distinct law enforcement
8 process that occurs outside the scope of the NSI and is not subject to the Functional
9 Standard.

10 Based on these differences, the PM-ISE declined to follow the recommendation of
11 certain advocacy organizations that the “reasonably indicative” operational concept in the
12 Functional Standard be replaced with the “reasonable suspicion” standard articulated in 28
13 C.F.R. Part 23. *See A.R.* at 345. The PM-ISE, as noted, was directed to develop a
14 framework for the NSI that promoted the broad sharing of SARs across jurisdictional lines
15 while protecting privacy interests and civil liberties to the greatest extent practicable.
16 Because the sharing of SARs occurs prior to the commencement of an investigation, the
17 PM-ISE determined that it would not be feasible to continue to promote the broad sharing
18 of SARs while requiring the establishment of reasonable suspicion before a SAR is shared.
19 *See id.* That decision was based on the factors that the PM-ISE was required to consider by
20 law and was within the bounds of reasonableness. Indeed, though the advocacy
21 organizations’ recommendation that the Functional Standard use the “reasonable suspicion”
22 standard was discussed with NSI participants, no participant endorsed the adoption of that
23 standard. *See id.*

24 In sum, the Functional Standard and 28 C.F.R. Part 23 have different purposes. The
25 express purpose of 28 C.F.R. Part 23 is to impose operating principles on “Criminal
26 Intelligence Systems” funded through support of the Omnibus Act that collect information
27

No. 17-16107

**In the United States Court of Appeals
for the Ninth Circuit**

WILEY GILL; JAMES PRIGOFF; TARIQ RAZAK; KHALED IBRAHIM;
AARON CONKLIN,

Plaintiffs-Appellants,

v.

DEPARTMENT OF JUSTICE; JEFF SESSIONS, Attorney General; PROGRAM
MANAGER – INFORMATION SHARING ENVIRONMENT; KSEMENDRA
PAUL, in his official capacity as Program Manager of the Information Sharing
Environment,

Defendants-Appellees.

EXCERPTS OF RECORD
Volume 3 of 4 – Pages 253 to 375

On Appeal from the United States District Court
for the Northern District of California
No. 3:14-cv-03120-RS
The Honorable Richard Seeborg, District Judge

Stephen Scotch-Marmo
stephen.scotch-
marmo@morganlewis.com
Michael James Ableson
michael.ableson@morganlewis.com
MORGAN, LEWIS & BOCKIUS LLP
101 Park Avenue
New York, NY 10178
T. 212.309.6000
F. 212.309.6001

Linda Lye
llye@aclunc.org
Julia Harumi Mass
jmass@aclunc.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN
CALIFORNIA, INC.
39 Drumm Street
San Francisco, CA 94111
T. 415.921.2493
F. 415.255.8437

Attorneys for Appellants
Wiley Gill, James Prigoff, Tariq Razak, Khaled Ibrahim, and Aaron Conklin

(Additional Counsel on Inside Cover)

Mitra Ebadolahi
mebadolahi@aclusandiego.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF SAN DIEGO AND
IMPERIAL COUNTIES
P.O. Box 87131
San Diego, CA 92138
T. 619.232.2121
F. 619.232.0036

Peter Bibring
pbibring@aclusocal.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF SOUTHERN
CALIFORNIA
1313 West 8th Street
Los Angeles, CA 90017
T. 213.977.9500
F. 213.977.5299

Hugh Handeyside
hhandeyside@aclu.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
T. 212.549.2500
F. 212.549.2654

Jeffrey S. Raskin
jeffrey.raskin@morganlewis.com
Phillip J. Wiese
phillip.wiese@morganlewis.com
MORGAN LEWIS & BOCKIUS LLP
One Market, Spear Street Tower
San Francisco, CA 94105
T. 415.442.1000
F. 415.442.1001

Christina Sinha
christinas@advancingjustice-alc.org
ASIAN AMERICANS ADVANCING
JUSTICE – ASIAN LAW CAUCUS
55 Columbus Avenue
San Francisco, CA 94111
T. 415.848.7711
F. 415.896.1703

Attorneys for Appellants

Wiley Gill, James Prigoff, Tariq Razak, Khaled Ibrahim, and Aaron Conklin

INDEX

Docket No.	Description	Date	Page No.
Volume 1 of 4 – Pages 1 to 10			
134	Order On Cross Motions For Summary Judgment	03/27/17	1
Volume 2 of 4 – Pages 11 to 252			
136	Notice Of Appeal To The United States Court Of Appeals For The Ninth Circuit	05/28/17	11
135	Judgment	03/29/17	16
127	Declaration Of Wiley Gill In Support Of Plaintiffs' Motion For Summary Judgment	11/03/16	17
	Exhibit 1: Letter, Dated January 3, 2014		25
	Exhibit 2: Letter, Dated June 23, 2014		28
	Exhibit 3: Letter, Dated February 29, 2016		48
124	Defendants' Reply In Support Of Motion For Summary Judgment, Opposition To Plaintiffs' Motion For Summary Judgment, And Opposition To Plaintiffs' Motion To Strike Defendants' Declarations And To Supplement The Record With Plaintiffs' Declarations	10/20/16	68
121	Plaintiffs' Motion To Strike Defendants' Declarations And To Supplement The Record With Plaintiffs' Declarations; Memorandum Of Points And Authorities In Support	09/22/16	73
120	Declaration Of Aaron Conklin In Support Of Plaintiffs' Motion For Summary Judgment And Plaintiffs' Opposition To Defendants' Motion For Summary Judgment	09/22/16	88

INDEX
(continued)

Docket No.	Description	Date	Page No.
119	Declaration Of Khaled Ibrahim In Support Of Plaintiffs' Motion For Summary Judgment	09/22/16	94
	Exhibit 1: Suspicious Activity Report		100
118	Declaration Of Tariq Razak In Support Of Plaintiffs' Motion For Summary Judgment	09/22/16	104
	Exhibit 1: Suspicious Activity Report		111
	Exhibit 2: Letter, Dated February 13, 2015		115
	Exhibit 3: Letter, Dated April 9, 2015		132
	Exhibit 4: Letter, Dated May 21, 2015		136
	Exhibit 5: Letter, Dated June 25, 2014		139
117	Declaration Of James Prigoff In Support Of Plaintiffs' Motion For Summary Judgment And Plaintiffs' Opposition To Defendants' Motion For Summary Judgment	09/22/16	143
	Exhibit 1: Business Card With Note, Dated August 19, 2004		153
	Exhibit 2: Suspicious Activity Report On James Burt Prigoff, Dated June 21, 2004		156
	Exhibit 3: Suspicious Activity Report On James Burt Prigoff, Dated October 18, 2004		160
	Exhibit 4: Suspicious Activity Report On James Burt Prigoff, Dated November 8, 2004		165

INDEX
(continued)

Docket No.	Description	Date	Page No.
	Exhibit 5: Letter, Dated March 24, 2015		168
	Exhibit 6: Letter, Dated May 19, 2015		172
	Exhibit 7: Letter, Dated January 27, 2016		176
	Exhibit 8: Letter, Dated January 8, 2015		179
	Exhibit 9: Letter, Dated September 15, 2015		181
	Exhibit 10: ISE-SAR Criteria Guidance		186
	Exhibit 11: Potential Indicators of Terrorist Activities Related to the General Public		201
116	Declaration Of Linda Lye In Support Of Plaintiffs' Opposition To Defendants' Motion For Summary Judgment And Cross-Motion For Summary Judgment	09/22/16	204
	Exhibit 1: Letter, Dated July 12, 2013		209
	Exhibit 2: Emails, Dated July 22, 2013, July 23, 2013 and August 2, 2013		212
	Exhibit 3: Letter, Dated March 7, 2016		217
	Exhibit 4: Letter, Dated March 21, 2016		220
	Exhibit 5: Regional Information Sharing Systems (RISS)		238
	Exhibit 6: 28 CFR Part 23 Frequently Asked Questions		241

INDEX
(continued)

Docket No.	Description	Date	Page No.
113	Defendants' Notice Of Motion For Summary Judgment And Memorandum In Support	08/18/16	243
Volume 3 of 4 – Pages 253 to 375			
107	Defendants' Notice Of Filing Of Supplemental Administrative Record	05/10/16	253
	Amended Certification Of Administrative Record And Supplemental Administrative Record		255
	Document 1: ISE Privacy Guidelines (December 4, 2006)		265
	Document 3: National Strategy for Information Sharing (October 2007)		268
	Document 5: Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project (October 1, 2008)		272
	Document 6: ISE Suspicious Activity Reporting Evaluation Environment Segment Architecture (December 2008)		290
	Document 7: ISE SAR Evaluation Environment Implementation Guide, Version 1.0 (January 9, 2009)		293
	Document 8: Final Report: Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Evaluation Environment (January 2010)		296

INDEX
(continued)

Docket No.	Description	Date	Page No.
	Document 9: Review of Advocate Websites for Concerns and Issues on ISE-Related Activities (2012)		306
94	Notice Of Motion And Memorandum Of Law In Support Of Defendants' Motion For Relief From Nondispositive Pretrial Order Of Magistrate Judge	01/15/16	310
79	Defendants' Opposition To Plaintiffs' Motion To Complete The Administrative Record	10/22/15	322
56	Defendants' Opposition To Plaintiffs' Special Motion To Establish Right To Discovery On The Department Of Justice's Standard For Suspicious Activity Reporting	07/10/15	374
Volume 4 of 4 – Pages 376 to 656			
52	Defendants' Notice Of Filing Of Administrative Record	06/16/15	376
	Certification of Administrative Record		380
53	Administrative Record	06/16/15	—
	Exhibit 1: White House Memorandum on Guidelines and Requirements in Support of the Information Sharing Environment (December 16, 2005) (wh121605- memo .pdf)		390

INDEX
(continued)

Docket No.	Description	Date	Page No.
	Exhibit 3: The Information Sharing Environment Suspicious Activity Reporting (SAR) Working Group's Business Process Analysis (February 13, 2007) (SAR_BusinessAnalysis_final20070215.doc)		395
	Exhibit 6: PM-ISE Memorandum, Release of the Information Sharing Environment (ISE) Functional Standard for Suspicious Activity Reporting (SAR) Version 1.0 (ISE-FS-200) (January 25, 2008) (Transmittal_Memorandum_ISE-FS-200.pdf)		397
	Exhibit 7: Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.0 ISE-FS-200 (January 25, 2008) (Functional Standard_Issuance_Version_1.0_Final_Signed).pdf)		401
	Exhibit 15: Information Sharing Environment – Suspicious Activity Reporting Functional Standard And Evaluation Environment Initial Privacy and Civil Liberties Analysis September 2008— Version 1 (September 2008) (ISE-SAR FS and EE Initial Privacy and Civil Liberties Analysis_090508.pdf)		433

INDEX
(continued)

Docket No.	Description	Date	Page No.
	Exhibit 20: Feedback Session with Privacy and Civil Liberties Advocates: Suspicious Activity Reporting (SAR) Line-Officer Training and the ISE-SAR Functional Standard—Agenda (February 13, 2009) (Agenda February 18, 2009 - SAR Feedback Session.doc)		447
	Exhibit 26: Memorandum for Release of the Information Sharing Environment (ISE) Functional Standard for Suspicious Activity Reporting, Version 1.5 (May 21, 2009) (ISE-SAR Functional Standard V1.5 Cover Letter.pdf)		448
	Exhibit 28: Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) version 1.5 (May 21, 2009) (ISE-FS-200_ ISESAR_ Functional_ Standard_ V1.5_ Issued.pdf)		450
	Exhibit 30: NSI Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations report issued by PMISE on privacy compliance outcomes of the ISE SAR Evaluation Environment and providing recommendations for additional privacy protections during nationwide expansion of the NSI (July 2010) (NSI_PCRCL_ Analysis_July2010_final.pdf)		486

INDEX
(continued)

Docket No.	Description	Date	Page No.
	Exhibit 40: ISE-SAR Functional Standard Version 1.5.5 Executive Summary (February 17, 2015) (FS v1_5_5 Executive Summary PM_ISE 21715 Comprehensive)		493
	Exhibit 41: Final and signed version of the ISE-SAR Functional Standard version 1.5.5 issued by the PM-ISE. (February 23, 2015) (SAR_FS_1.5.5_IssuedFeb2015.pdf)		501
46-1	Defendants' Answer To Complaint	04/24/15	561
40	Joint Case Management Statement & [Proposed] Order	03/05/15	566
38	Order Denying Motion To Dismiss	02/20/15	569
36	Joint Case Management Statement & [Proposed] Order	12/31/14	581
21	Notice Of Motion And Memorandum Of Law In Support Of Defendants' Motion To Dismiss	10/16/14	586
—	District Court Docket	—	632

1 BENJAMIN C. MIZER
 Principal Deputy Assistant Attorney General
 2 ANTHONY J. COPPOLINO
 Deputy Branch Director
 3 KIERAN G. GOSTIN
 DC Bar No. 1019779
 4 Trial Attorney
 5 Civil Division, Federal Programs Branch
 U.S. Department of Justice
 6 P.O. Box 883
 Washington, D.C. 20044
 7 Telephone: (202) 353-4556
 8 Facsimile: (202) 616-8460
 E-mail: kieran.g.gostin@usdoj.gov
 9

10 *Attorneys for Federal Defendants*

11 **UNITED STATES DISTRICT COURT**
 12 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**

13 WILEY GILL; JAMES PRIGOFF; TARIQ
 14 RAZAK; KHALID IBRAHIM; and AARON
 CONKLIN,

15 Plaintiffs,

16 v.

17 DEPARTMENT OF JUSTICE, *et al.*,

18 Defendants.
 19
 20

No. 3:14-cv-03120 RS-KAW

**DEFENDANTS' NOTICE OF FILING OF
 SUPPLEMENTAL ADMINISTRATIVE
 RECORD**

1 In accordance with the Magistrate Judge’s and District Court’s Orders, Dkt Nos. 88, 102,
 2 Defendants have revisited the administrative record to ensure its completeness and are providing
 3 the following documents as attachments to this Notice: (1) Amended Certification of
 4 Administrative Record and Supplemental Administrative Record; (2) Supplemental
 5 Administrative Record – Part 1; and (3) Supplemental Administrative Record – Part 2. As
 6 directed by the Court, the Amended Certification of Administrative Record and Supplemental
 7 Administrative Record describes the search conducted by Defendants and its results.

8
9 May 10, 2016

Respectfully submitted,

10 BENJAMIN C. MIZER
11 Principal Deputy Assistant Attorney General

12 ANTHONY J. COPPOLINO
13 Deputy Branch Director

14 /s/ Kieran G. Gostin
15 KIERAN G. GOSTIN
16 DC Bar No. 1019779
17 Trial Attorney

18 Civil Division, Federal Programs Branch
19 U.S. Department of Justice
20 P.O. Box 883
21 Washington, D.C. 20044
22 Telephone: (202) 353-4556
23 Facsimile: (202) 616-8460
24 E-mail: kieran.g.gostin@usdoj.gov

25 *Attorneys for Federal Defendants*
26
27
28

Pages ER 255-62 intentionally omitted.

SUPPLEMENTAL ADMINISTRATIVE RECORD INDEX

	<u>DOCUMENT INFORMATION</u>	<u>BATES NUMBER</u>	<u>REDACTION</u> ¹
1	ISE Privacy Guidelines (December 4, 2006)	001-009	None
2	May 22, 2007 Review 2: Agenda May 22, 2007 Review 2: Agenda (May, 22, 2007)	010	None
3	National Strategy for Information Sharing (October 2007)	011-058	None
4	December 2007 SAR WG Meeting Agenda (December 13, 2007)	059	01
5	Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project (October 1, 2008)	060-097	01
6	ISE Suspicious Activity Reporting Evaluation Environment Segment Architecture (December 2008)	098-188	None
7	ISE SAR Evaluation Environment Implementation Guide, Version 1.0 (January 9, 2009)	189-218	01 & 03
8	Final Report: Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Evaluation Environment (January 2010)	219-381	01 & 03
9	Review of Advocate Websites for Concerns and Issues on ISE-Related Activities (2012)	382-388	None
10	Meeting Agenda for May 20, 2013 DOJ/FBI Functional Standard Stakeholders Meeting (May 13, 2013)	389	None
11	Sign-in sheet for May 2013 DOJ/FBI Functional Standard Stakeholders Meeting (May 20, 2013)	390	01, 02 & 03
12	Sign-in sheet for May 2013 DHS Functional Standard Stakeholders Meeting (May 24, 2013)	391	01 & 03
13	Attendee list for November 2014 NSI Functional Standard Meeting (November 18, 2014)	392	01, 02 & 03

¹ The nature of each of the redactions is explained in Defendants' Notice of Filing of Administrative Record. Dkt. No. 52.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

14	Email from Mike Sena re: Proposed Final ISE-SAR Functional Standard Version 1.5.5 (November 21, 2014)	393-394	01, 02, & 03
15	Email from Vernon Keenan re: Proposed Final ISE-SAR Functional Standard Version 1.5.5 (November 24, 2014)	395-396	01, 02, & 03

Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment

1. Background and Applicability.

- a. Background.* Section 1016(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) calls for the issuance of guidelines to protect privacy and civil liberties in the development and use of the “information sharing environment” (ISE). Section 1 of Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans, provides that, “[t]o the maximum extent consistent with applicable law, agencies shall ... give the highest priority to ... the interchange of terrorism information among agencies ... [and shall] protect the freedom, information privacy, and other legal rights of Americans in the conduct of [such] activities” These Guidelines implement the requirements under the IRTPA and EO 13388 to protect information privacy rights and provide other legal protections relating to civil liberties and the legal rights of Americans in the development and use of the ISE.
- b. Applicability.* These Guidelines apply to information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States (“protected information”). For the intelligence community, protected information includes information about “United States persons” as defined in Executive Order 12333. Protected information may also include other information that the U.S. Government expressly determines by Executive Order, international agreement, or other similar instrument, should be covered by these Guidelines.

2. Compliance with Laws.

- a. General.* In the development and use of the ISE, all agencies shall, without exception, comply with the Constitution and all applicable laws and Executive Orders relating to protected information.
- b. Rules Assessment.* Each agency shall implement an ongoing process for identifying and assessing the laws, Executive Orders, policies, and procedures that apply to the protected information that it will make available or access through the ISE. Each agency shall identify, document, and comply with any legal restrictions applicable to such information. Each agency shall adopt internal policies and procedures requiring it to:

the other agency's ISE privacy official (the ISE privacy officials are described in section 12 below).

- c. Procedures.* Each agency, consistent with its legal authorities and mission requirements, shall adopt and implement policies and procedures with respect to the ISE requiring the agency to:
- (i) take appropriate steps, when merging protected information about an individual from two or more sources, to ensure that the information is about the same individual;
 - (ii) investigate in a timely manner alleged errors and deficiencies and correct, delete, or refrain from using protected information found to be erroneous or deficient; and
 - (iii) retain protected information only so long as it is relevant and timely for appropriate use by the agency, and update, delete, or refrain from using protected information that is outdated or otherwise irrelevant for such use.

6. Data Security.

Each agency shall use appropriate physical, technical, and administrative measures to safeguard protected information shared through the ISE from unauthorized access, disclosure, modification, use, or destruction.

7. Accountability, Enforcement and Audit.

- a. Procedures.* Each agency shall modify existing policies and procedures or adopt new ones as appropriate, requiring the agency to:
- (i) have and enforce policies for reporting, investigating, and responding to violations of agency policies relating to protected information, including taking appropriate action when violations are found;
 - (ii) provide training to personnel authorized to share protected information through the ISE regarding the agency's requirements and policies for collection, use, and disclosure of protected information, and, as appropriate, for reporting violations of agency privacy-protection policies;
 - (iii) cooperate with audits and reviews by officials with responsibility for providing oversight with respect to the ISE; and

(iv) designate each agency's ISE privacy official to receive reports (or copies thereof if the agency already has a designated recipient of such reports) regarding alleged errors in protected information that originate from that agency.

b. *Audit.* Each agency shall implement adequate review and audit mechanisms to enable the agency's ISE privacy official and other authorized officials to verify that the agency and its personnel are complying with these Guidelines in the development and use of the ISE.

8. Redress.

To the extent consistent with its legal authorities and mission requirements, each agency shall, with respect to its participation in the development and use of the ISE, put in place internal procedures to address complaints from persons regarding protected information about them that is under the agency's control.

9. Execution, Training, and Technology.

- a. *Execution.* The ISE privacy official shall be responsible for ensuring that protections are implemented as appropriate through efforts such as training, business process changes, and system designs.
- b. *Training.* Each agency shall develop an ongoing training program in the implementation of these Guidelines, and shall provide such training to agency personnel participating in the development and use of the ISE.
- c. *Technology.* Where reasonably feasible, and consistent with standards and procedures established for the ISE, each agency shall consider and implement, as appropriate, privacy enhancing technologies including, but not limited to, permissioning systems, hashing, data anonymization, immutable audit logs, and authentication.

10. Awareness.

Each agency shall take steps to facilitate appropriate public awareness of its policies and procedures for implementing these Guidelines.

11. Non-Federal Entities.

Consistent with any standards and procedures that may be issued to govern participation in the ISE by State, tribal, and local governments and private sector entities, the agencies and the PM-ISE will work with non-Federal entities seeking to access protected information through the ISE to ensure that such non-Federal entities

NATIONAL STRATEGY FOR
**INFORMATION
SHARING**

*Successes and Challenges
In Improving
Terrorism-Related
Information Sharing*



OCTOBER 2007

unrelated information from other sources, and therefore we must foster a culture of awareness in which people at all levels of government remain cognizant of the functions and needs of others and use knowledge and information from all sources to support counterterrorism efforts;

- Information sharing must be woven into all aspects of counterterrorism activity, including preventive and protective actions, actionable responses, criminal and counterterrorism investigative activities, event preparedness, and response to and recovery from catastrophic events;
- The procedures, processes, and systems that support information sharing must draw upon and integrate existing technical capabilities and must respect established authorities and responsibilities; and
- State and major urban area fusion centers represent a valuable information sharing resource and should be incorporated into the national information sharing framework, which will require that fusion centers achieve a baseline level of capability to gather, process, share, and utilize information and operate in a manner that respects individuals' privacy rights and other legal rights protected by U.S. laws.

Foundational Elements

This *Strategy* is focused on improving the sharing of homeland security, terrorism, and law enforcement information related to terrorism within and among all levels of governments and the private sector.

- **Information Sharing at the Federal Level.** The instruments of our national power have long depended on the capabilities of the Intelligence Community to collect, process, analyze, and disseminate intelligence regarding our adversaries and enemies. Our efforts to combat terrorism depend on enhancing those intelligence capabilities, while enabling other Federal departments and agencies responsible for protecting the United States and its interests to regularly share information and intelligence with other public and private entities in support of mission critical activities. Information sharing at the Federal level has improved significantly since September 11, but challenges still remain that must be addressed before our strategic vision is realized.
- **Information Sharing with State, Local, and Tribal Entities.** As our Nation's first "pre-venters and responders," State, local, and tribal governments are critical to our efforts to prevent future terrorist attacks and to respond if an attack occurs. They must have access to the information that enables them to protect our local communities. In addition, these State, local, and tribal officials are often best able to identify potential threats that exist within their jurisdictions. They are full and trusted partners with the Federal Government in our Nation's efforts to combat terrorism, and therefore they must be a part of an information sharing framework that supports an effective and efficient two-way flow of information enabling officials at all levels of government to counter and respond to threats.

PROTECTING PRIVACY AND OTHER LEGAL RIGHTS IN THE SHARING OF INFORMATION

Protecting the rights of Americans is a core facet of our information sharing efforts. While we must zealously protect our Nation from the real and continuing threat of terrorist attacks, we must just as zealously protect the information privacy rights and other legal rights of Americans. With proper planning we can have both enhanced privacy protections and increased information sharing – and in fact, we must achieve this balance at all levels of government, in order to maintain the trust of the American people. The President reaffirmed this in his December 16, 2005, Memorandum to the Heads of Executive Departments and Agencies.

At the direction of the President, the Attorney General and the Director of National Intelligence developed a set of Privacy Guidelines to ensure the information privacy and other legal rights of Americans are protected in the development and use of the ISE. The Privacy Guidelines provide a consistent framework for identifying information that is subject to privacy protection, assessing applicable privacy rules, implementing appropriate protections, and ensuring compliance. An array of laws, directives, and policies provide substantive privacy protections for personally identifiable information. The parameters of those protections vary depending on the rules that apply to particular agencies and the information they are proposing to share. As described below, however, the Guidelines demand more than mere compliance with the laws; they require executive departments and agencies to take pro-active and explicit actions to ensure the balance between information privacy and security is maintained, as called for by the *National Commission on Terrorist Attacks Upon the United States*. The full text of the ISE Privacy Guidelines can be found at www.ise.gov.

Core Privacy Principles

The Privacy Guidelines build on a set of core principles that Federal departments and agencies must follow. Those principles require specific, uniform action and reflect basic privacy protections and best practices. Agencies must:

- Share protected information only to the extent it is terrorism information, homeland security information, or law enforcement information related to terrorism;
- Identify and review the protected information to be shared within the ISE;
- Enable ISE participants to determine the nature of the protected information to be shared and its legal restrictions (e.g., “this record contains individually identifiable information about a U.S. citizen”);
- Assess, document, and comply with all applicable laws and policies;
- Establish data accuracy, quality, and retention procedures;
- Deploy adequate security measures to safeguard protected information;

- Implement adequate accountability, enforcement, and audit mechanisms to verify compliance;
- Establish a redress process consistent with legal authorities and mission requirements;
- Implement the guidelines through appropriate changes to business processes and systems, training, and technology;
- Make the public aware of the agency's policies and procedures as appropriate;
- Ensure agencies disclose protected information to non-Federal entities—including State, local, tribal, and foreign governments—only if the non-Federal entities provide comparable protections; and
- State, local, and tribal governments are required to designate a senior official accountable for implementation.

Privacy Governance

Successful implementation of the Privacy Guidelines requires a governance structure to monitor compliance and to revise the Guidelines as we gain more experience. The President, therefore, directed the Program Manager to establish the ISE Privacy Guidelines Committee. The Committee is chaired by representatives of the Attorney General and the Director of National Intelligence, and consists of the Privacy Officials of the departments and agencies of the Information Sharing Council. The Committee seeks to ensure consistency and standardization, as well as serve as a forum to share best practices and resolve agency concerns.



FINDINGS AND RECOMMENDATIONS OF THE

SUSPICIOUS ACTIVITY REPORT (SAR)

SUPPORT AND IMPLEMENTATION PROJECT

OCTOBER 2008

About Global

The U.S. Department of Justice's Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee to the U.S. Attorney General on critical justice information sharing initiatives. Global promotes standards-based electronic information exchange to provide justice and public safety communities with timely, accurate, complete, and accessible information in a secure and trusted environment. Global is administered by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance.



FINDINGS AND RECOMMENDATIONS OF THE

SUSPICIOUS ACTIVITY REPORT (SAR)

SUPPORT AND IMPLEMENTATION PROJECT

OCTOBER 2008

ACKNOWLEDGEMENTS

The *Suspicious Activity Report (SAR) Support and Implementation Project* appreciates the support and guidance of the project sponsors: the Bureau of Justice Assistance (BJA), U.S. Department of Justice (DOJ); the Major Cities Chiefs Association (MCCA); DOJ's Global Justice Information Sharing Initiative (Global); the Criminal Intelligence Coordinating Council (CICC); the U.S. Department of Homeland Security (DHS); and the Federal Bureau of Investigation (FBI). Representatives of these organizations were vital in the development of the findings and recommendations for the reporting of suspicious activity.

The SAR Support and Implementation Project team and participants involved numerous law enforcement experts from local, state, tribal, and federal agencies whose knowledge and dedication to the project are reflected within this document. The project's site visit team and the executive steering committee's insight helped guide the project through to its completion. A complete listing of all project team members and participants is contained in Appendix A.

Special appreciation goes to the Los Angeles, California, Police Department for spearheading the SAR Initiative and bringing it to the national forefront. Without the leadership and commitment of Chief William Bratton, Deputy Chief Michael Downing, and Commander Joan McNamara, this project would not be as advanced as it is today. Particular thanks are extended to Chief R. Gil Kerlikowske, Chief of Police, Seattle Police Department, and President of the MCCA, for his guidance throughout this project. The forward thinking from the senior leadership involved was instrumental in the development of these findings and recommendations.

This report would not have been possible without the effort of the Office of the Program Manager, Information Sharing Environment (PM-ISE) and its commitment to the sharing of criminal and terrorist information among local, state, tribal, and federal law enforcement agencies. A special thank-you is given to Ambassador Thomas E. ("Ted") McNamara, Program Manager; Ms. [REDACTED], Deputy Program Manager; and [REDACTED], Senior Advisor, for their dedication to this important nationwide initiative.

This project was supported by Grant No. 2007-MC-RX-K001 awarded by the Bureau of Justice Assistance, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative and the Program Manager, Information Sharing Environment. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the SMART Office, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the U.S. Department of Justice or the Program Manager, Information Sharing Environment.

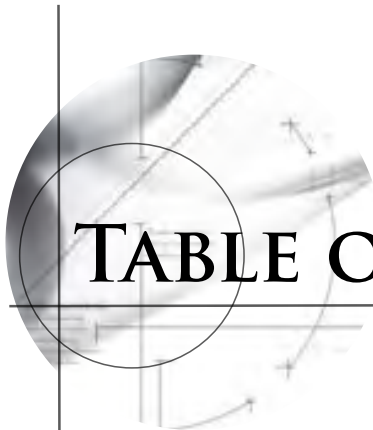


TABLE OF CONTENTS

Acknowledgements..... ii

Table of Contents..... iii

Executive Summary..... 1

Introduction 5

Section One: Executive Leadership..... 7

Section Two: Privacy and Civil Liberties Protections 9

Section Three: Gathering, Processing, Reporting, Analyzing, and Sharing of Suspicious Activity (SAR Process) 11

Section Four: Standard Reporting Format and Data Collection Codes..... 15

Section Five: Training and Community Outreach 17

Section Six: Technology 19

Site Visit Overviews 21

Notional SAR Flowchart..... 23

Appendix A: Project Team Members and Participants 25

Appendix B: Los Angeles Police Department Special Order Regarding SAR..... 27

Appendix C: Sample of Los Angeles Police Department Terrorism-Related CCAD Codes..... 31



EXECUTIVE SUMMARY

The development of the recommendations for the reporting of suspicious activity is the direct result of the hard work and ingenuity of many local, state, tribal, and federal law enforcement representatives who believe national guidelines for suspicious activity reporting will help protect the citizens of the United States and aid in the prevention of another terrorist attack occurring on American soil. First and foremost, it should be noted that local law enforcement entities carry out counterterrorism-related activities within the context of their core mission of protecting local communities from crime and violence. Accordingly, it is essential that local law enforcement officers receive training to recognize those behaviors and incidents indicative of criminal activity associated with the planning and carrying out of a terrorist attack. Furthermore, it is important that local law enforcement entities incorporate the documenting, processing, analyzing, and sharing of information related to such activities into existing processes and systems used to better protect communities from criminal activity.

The Suspicious Activity Report (SAR) process, as defined in this paper, focuses on what law enforcement agencies have been doing for years—gathering information regarding behaviors and incidents associated with crime and establishing a process whereby information can be shared to detect and prevent criminal activity, including that associated with domestic and international terrorism. Implementation of the SAR process can be accomplished within the agency's existing framework to gather, process, analyze, and report behaviors and events that are indicative of criminal activity. Just as the *National Criminal Intelligence Sharing Plan*,¹ the *Fusion Center Guidelines*,² and the *National Strategy for Information Sharing*³ are key tools

¹ www.it.ojp.gov/documents/National_Criminal_Intelligence_Sharing_Plan.pdf.

² www.it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf.

³ www.whitehouse.gov/nsc/infosharing/index.html.

for law enforcement, the *Findings and Recommendations of the SAR Support and Implementation Project* will be another resource that agencies can employ to support their crime-fighting and public safety efforts.

The purpose of the *Findings and Recommendations of the SAR Support and Implementation Project* is to describe the all-crimes approach to gathering, processing, reporting, analyzing, and sharing of suspicious activity (SAR process) by the local police agency. This report and its recommendations are important for establishing national guidelines that will allow for the timely sharing of SAR information; however, it is understood that every jurisdiction will have to develop policies and procedures

The purpose of the *Findings and Recommendations of the SAR Support and Implementation Project* is to describe the all-crimes approach to gathering, processing, reporting, analyzing, and sharing of suspicious activity (SAR process) by the local police agency.

that take into account the unique circumstances and relationships within that community. In accordance with the *National Criminal Intelligence Sharing Plan* and the *National Strategy for Information Sharing* (NSIS), the Bureau of Justice Assistance (BJA), U.S. Department of Justice (DOJ); the Major Cities Chiefs Association (MCCA); DOJ's Global Justice Information Sharing Initiative (Global); the Criminal Intelligence Coordinating Council (CICC); the U.S. Department of Homeland Security (DHS); and

the Federal Bureau of Investigation (FBI) have developed these recommendations to be used by law enforcement agencies to improve the identification and reporting of suspicious activity and the sharing of that information with fusion centers and Joint Terrorism Task Forces (JTTF).

In the spring of 2008, site visits to four major law enforcement agencies were conducted by subject-matter experts. During the site visits (Los Angeles, California; Chicago, Illinois; Boston, Massachusetts; and Miami-Dade, Florida, Police Departments), a number of findings were identified in order to develop a standardized approach to the reporting of suspicious activity in the United States.

MAJOR FINDINGS

1. Executive Leadership

- Leadership must recognize the importance of implementing a SAR process.

2. Privacy and Civil Liberties Protections

- Implement an agency privacy policy.

3. Gathering, Processing, Reporting, Analyzing, and Sharing of Suspicious Activity (SAR Process)

- Identify existing SAR processes and determine what SAR processes need to be developed.
- Incorporate national guidelines into standard operating procedures.

4. Standard Reporting Format and Data Collection Codes

- Institutionalize the SAR process within the agency.

5. Training and Community Outreach

- Train all agency personnel on the SAR process.
- Educate the community on the SAR process.

6. Technology

- Partner with others, and connect to information sharing networks.

MAJOR FINDINGS

EXECUTIVE LEADERSHIP

1. Strong executive leadership is an essential element leading to the success of any SAR program.
2. Agencies should educate and gain the support of policymakers.

PRIVACY AND CIVIL LIBERTIES PROTECTIONS

1. Local law enforcement entities should incorporate the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents into existing processes and systems used to manage other crime-related information and criminal intelligence so as to leverage existing policies and protocols utilized to protect the information privacy, civil liberties, and other legal rights of the general public.
2. Agencies should evaluate and update, if necessary, their privacy and civil liberties policy to ensure that the gathering, documenting, processing, and sharing of information regarding terrorism-related criminal activity are specifically addressed.
3. The policy should be transparent and communicated with the public, community organizations, and other groups as appropriate.

GATHERING, PROCESSING, REPORTING, ANALYZING, AND SHARING OF SUSPICIOUS ACTIVITY (SAR PROCESS)

1. The SAR process is critical to preventing crimes, including those associated with domestic and international terrorism.
2. Local law enforcement entities should incorporate the gathering, documenting, processing, analyzing, and sharing of terrorism-related suspicious activities and incidents into existing processes and systems used to manage other crime-related information and criminal intelligence.
3. Local law enforcement agencies or agencies with original jurisdiction are the initial collection points and investigative leads for all suspicious activity data. Suspicious activity submissions should not bypass the local law enforcement agency and the standard 911 reporting systems.

4. When an agency receives information that impacts another jurisdiction, it is the responsibility of the receiving agency to immediately notify the impacted agency and discuss coordination, deconfliction, investigation, and vetting procedures with the impacted agency. Once vetted, further dissemination of the information will be the responsibility of the impacted agency.
5. A defined process is needed by the originating agency to ensure that suspicious activity reporting is made available to fusion centers and local Joint Terrorism Task Forces (JTTF) in a timely manner.
6. An ongoing emphasis should be placed on defining and communicating trends in terrorism activity, geographically specific threat reporting, dangers to critical infrastructure, and general situational awareness.

STANDARD REPORTING FORMAT AND DATA COLLECTION CODES

1. There is a need for a common national methodology for the sharing of suspicious activity data in order to discern patterns across the country.
2. Utilizing a standard reporting format and common national data collection codes is essential to identifying local, regional, and national crime trends.

TRAINING AND COMMUNITY OUTREACH

1. Training is a key component of the SAR process—all relevant agency personnel must be trained to recognize behavior and incidents indicative of criminal activity associated with international and domestic terrorism.
2. Incorporating outreach to the public, law enforcement, and the private sector in the collection process is important to the success of the program.

TECHNOLOGY

1. Technology and use of common national standards enhance the capability to quickly and accurately analyze suspicious activity data in support of controlling and preventing criminal activity.
2. Agencies should explore the concepts and use of virtual fusion centers that are accessible to all law enforcement personnel via a Web-enabled interface.

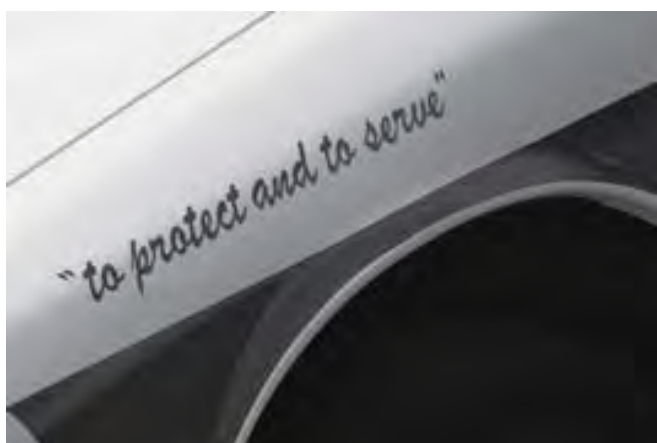
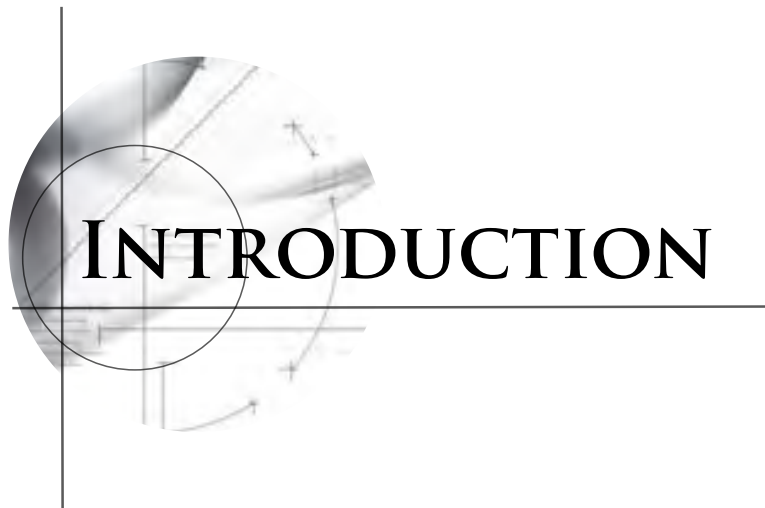
CONSIDERATIONS FOR FURTHER ACTIONS ON THE NATIONAL LEVEL

- ◆ Develop a set of common national data collection codes in order to allow for common analysis of data across jurisdictions.
 - a. Formulate a working group to consolidate and standardize the suspicious activity to be reported and shared. Currently, a number of agencies have identified certain activities to be reported and assigned codes for those activities. In addition, the *Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.0* (ISE-SAR Functional Standard) and the DOJ Information Exchange Package Document (IEPD) identify activities to document and share. In order to have a consistent methodology to share SAR data, these activities and codes need to be standardized.
- ◆ The findings and recommendations developed in this report are supported by the Major Cities Chiefs Association; however, the report is not a template solely for major cities. Smaller agencies and jurisdictions can also utilize this report in establishing a SAR process. For agencies that do not currently have a method to document, process, analyze, and share suspicious activity, training and technical assistance should be provided.
- ◆ Update the common definition for *suspicious activity*. The ISE-SAR Functional Standard defines suspicious activity as “observed behavior that may be indicative of intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit intention.”⁴
 - a. Consideration should be given to update the definition to include “observed incident or behavior.”
 - b. Additionally, while the ISE-SAR Functional Standard provides a comprehensive list of examples of suspicious activity, the definition lists only two categories: intelligence gathering and preoperational planning. Although most SARs may fall into these categories, not all will. For example, the suspicious activity may be an actual attack or other crime. It may be a report of a suspicious association or material that supports activity. Because of these limitations, consideration should be given to expanding the definition: “Reported or observed activity and/or

⁴ *Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.0*, p. 6. For additional information, go to www.ise.gov/pages/ctiss.html.

behavior that, based on an officers training and experience, is believed to be indicative of criminal activity associated with terrorism.”

- ◆ Emphasis should be placed on the analytical component of the SAR process. Analysis is vital to the success of the SAR process to ensure that the information gathered is properly vetted and analyzed to determine its credibility. Information that is shared should document the current status of the SAR to indicate factors such as whether an investigation was opened, whether the SAR was referred to another agency, or whether it was unresolved, before it is shared with other agencies.
- ◆ Develop a common national methodology to share SAR data in a timely manner. This methodology should articulate how SAR information will be shared with other law enforcement agencies, both horizontally and vertically, and how privacy and civil liberties policies of the originating agencies will be protected.
- ◆ Agencies should leverage the ISE Privacy Guidelines, Global privacy products, and tenets of 28 Code of Federal Regulations (CFR) Part 23 to evaluate, update, or develop privacy and civil liberties protection policies. Law enforcement agencies across the nation operate under privacy and information-handling frameworks that are governed by state law, local ordinances, judicial decrees, and federal regulation. Some jurisdictions may have more restrictive privacy procedures than others; however, there is a need for common procedures and standards to facilitate data sharing while protecting privacy and civil liberties. During the site visits, each agency described slightly different decision-making processes that would determine at what point SAR information actually becomes intelligence and subsequently subject to 28 CFR Part 23 requirements. The determination of when a SAR becomes controlled by the tenets of 28 CFR Part 23 needs to be clearly defined by the agency.
- ◆ Develop a standardized training program in order to provide consistent nationwide SAR training. Although there are a number of training programs regarding terrorism awareness, there should be a common understanding of what is needed to appropriately gather, process, report, analyze, and share suspicious activity. A standardized training program would also address the use of the common national data collection codes and methodology, as well as provide an understanding of the importance of protecting privacy and civil liberties.
 - a. It is critical that a national training protocol be developed for the sharing of SAR data, and it is the responsibility of each agency to train on its collection process.



Local law enforcement agencies are critical to efforts to protect our local communities from another terrorist attack. Fundamental to local efforts to detect and mitigate potential terrorist threats is ensuring that frontline personnel are trained to recognize and document behaviors and incidents indicative of criminal activity associated with domestic and international terrorism. Daily, there are more than 17,000 local law enforcement agencies in the United States that document information regarding suspicious criminal activity, including that

The ISE-SAR Functional Standard defines a Suspicious Activity Report (SAR) as “official documentation of observed behavior that may be indicative of intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit intention.”

related to terrorism. In the absence of national guidance, individual jurisdictions have independently developed intradepartmental policies and procedures for gathering and documenting Suspicious Activity Reports (SARs); however, the lack of standardization has restricted the efficient analysis and sharing of this information on a regional and/or national basis.

The SAR process is the gathering, processing, reporting, analyzing, and sharing of suspicious activity.

The purpose of the *Findings and Recommendations of the SAR Support and Implementation Project* is to describe the gathering, processing, reporting, analyzing, and sharing of suspicious activity (SAR process) by the local police agency. This report and its recommendations are important for establishing national guidelines that will facilitate the improved sharing of SAR information. While these recommendations are intended to bring about standardization of the SAR process, every jurisdiction should develop policies and procedures that take into account the unique circumstances and relationships within that community.

The ISE-SAR Functional Standard defines a Suspicious Activity Report as “official documentation of observed behavior that may be indicative of intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit intention.”⁵ The SAR process focuses on what law enforcement agencies have been doing for years—gathering information and establishing a process

⁵ Ibid., p. 3. For additional information, go to www.ise.gov/pages/ctiss.html.

whereby information can be shared to detect and prevent criminal and terrorist activity. Standardizing the SAR process will assist local law enforcement agencies in incorporating efforts involving the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious behaviors and incidents into the processes and systems used to manage other crime-related information and criminal intelligence. As part of this effort, law enforcement agencies should encourage the principles of intelligence-led policing (ILP) to involve and interact with other agencies in the reporting of suspicious activity to identify and prevent criminal and terrorist activity.

The *Findings and Recommendations of the SAR Support and Implementation Project* report was developed to provide recommendations to the Criminal Intelligence Coordinating Council (CICC)⁶ from the Major Cities Chiefs Association (MCCA).⁷ To develop these findings and recommendations, site visits were conducted at police departments in Los Angeles, California; Chicago, Illinois; Boston, Massachusetts; and Miami-Dade, Florida, to observe and document their SAR practices and processes. The site visit teams were selected by the sponsoring agencies—the Bureau of Justice Assistance (BJA), U.S. Department of Justice (DOJ); MCCA; DOJ's Global Justice Information Sharing Initiative (Global); CICC; the U.S. Department of Homeland Security (DHS), and the Federal Bureau of Investigation (FBI). After the site visits, the *Findings and Recommendations of the SAR Support and Implementation Project* report was developed by the

SAR Executive Steering Committee, which was composed of local, state, and federal agencies representing the CICC, the Global Advisory Committee (GAC),⁸ and the MCCA. Promising practices from these site visits were identified and are detailed throughout this report. In June 2008, the *Findings and Recommendations of the SAR Support and Implementation Project* was presented for review to the MCCA, which is composed of the 64 largest police departments in the United States and Canada, and was unanimously approved. It was presented to and unanimously approved by the CICC in September 2008 and the GAC in October 2008.

Through this effort, several key areas regarding the implementation of the SAR process were identified: Executive Leadership; Privacy and Civil Liberties Protections; Gathering, Processing, Reporting, Analyzing, and Sharing of Suspicious Activity; Standard Reporting Format and Data Collection Codes; Training and Community Outreach; and Technology. This report examines each of these issues, provides information on the findings, and presents SAR process implementation recommendations. Following the issue-specific findings and recommendations, the report examines promising practices identified from the site visits.

⁶ For more information on the CICC, visit www.iir.com/global/council.htm.
⁷ For more information on the MCCA, visit www.majorcitieschiefs.org/.

⁸ For more information on the GAC, visit www.iir.com/global/committee.htm.

SECTION TWO: PRIVACY AND CIVIL LIBERTIES PROTECTIONS

ISSUE-SPECIFIC FINDINGS

- ◆ **Local law enforcement entities should incorporate the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents into existing processes and systems used to manage other crime-related information and criminal intelligence so as to leverage existing policies and protocols utilized to protect the information privacy, civil liberties, and other legal rights of the general public.**
- ◆ **Agencies should evaluate and update, if necessary, their privacy and civil liberties policy to ensure that the gathering, documenting, processing, and sharing of information regarding terrorism-related criminal activity are specifically addressed.**
- ◆ **The policy should be transparent and communicated with the public, community organizations, and other groups as appropriate.**

In order to balance law enforcement's ability to share information with the rights of citizens, appropriate privacy and civil liberties policies must be utilized.¹⁰ Agencies should establish their SAR process in a manner that is consistent with existing privacy and civil liberties policies. A strong privacy and civil liberties policy will not only protect the rights of the citizens but also protect the agency.

SAR PROCESS IMPLEMENTATION RECOMMENDATIONS

- ◆ In recognition of their state laws and local ordinances, agencies should promote a policy of openness and transparency when communicating with the public regarding their SAR process.
- ◆ When developing an order to mandate the SAR process, agencies should clearly articulate when 28 CFR Part 23 should be applied.
- ◆ Consistent with federal, state, and local statutory and regulatory requirements, agencies should ensure that key privacy-related issues—such as accuracy, redress, and purging—are addressed in their existing privacy and civil liberties policy.
- ◆ When developing the SAR process, agencies should review and consider their jurisdictional and state laws and local ordinances regarding the retention, disposition, and release of information.

¹⁰ *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*, p. 41. For more information regarding the Fusion Center Guidelines, visit www.fbi.gov/documents/fusion_center_guidelines_law_enforcement.pdf.

- ◆ Random audits of the quality and substance of reports should be conducted in order to ensure that the integrity of the program is maintained and that appropriate respect and attention are given to reasonable suspicion and other civil rights issues.
- ◆ Utilizing interagency privacy agreements and standardized vetting mechanisms.
- ◆ Mandating supervisory review of SARs to ensure that all of the information has been properly reviewed and evaluated.
- ◆ Utilizing legal/privacy advisors in the development of the SAR process.

PROMISING PRACTICES IDENTIFIED DURING THE SITE VISITS

The site visits provided several promising practices related to privacy protection. These include:

SECTION FIVE: TRAINING AND COMMUNITY OUTREACH

ISSUE-SPECIFIC FINDINGS

- ◆ **Training is a key component of the SAR process—all relevant agency personnel must be trained to recognize behavior and incidents indicative of criminal activity associated with international and domestic terrorism.**
- ◆ **Incorporating outreach to the public, law enforcement, and the private sector in the collection process is important to the success of the program.**

Training is a vital component of the implementation of a SAR process within an agency. SAR training must be provided throughout the department to ensure that the SAR process is institutionalized within the agency. In addition to in-service and roll-call training, distance learning or e-training capabilities are becoming a readily available option to law enforcement agencies. E-training can facilitate SAR training to personnel with schedules that do not permit them to attend traditional classroom training and will help ensure that everyone within the law enforcement agency is trained. External stakeholders should be trained and alerted regarding the concept of suspicious activity and where/when to report it. Educating the entire spectrum of stakeholders regarding the SAR process will help ensure that suspicious activity is properly reported and addressed accordingly.

SAR PROCESS IMPLEMENTATION RECOMMENDATIONS

- ◆ Agencies must implement a training program that reaches all levels of law enforcement personnel so that they can recognize the behaviors and incidents that represent terrorism-related suspicious activity.
 - ◇ Training for both law enforcement and the public should be conducted in a phased approach. It should be updated regularly and provided on an ongoing basis. Training should include:
 - The SAR program and basic reporting.
 - Detailed training on the recognition of reportable behaviors.
 - ◇ Training must be provided to in-service law enforcement personnel and basic recruits on the SAR process. Training should include but not be limited to the following:
 - Recruits or cadets
 - Dispatch center personnel
 - Analysts
 - Records clerks or records management system (RMS) personnel
 - Patrol officers/deputies
 - Line supervisors
 - Executive and command-level personnel
 - Governance board members
 - Other stakeholders as appropriate
 - ◇ Training should:
 - Emphasize that all personnel, regardless of position, have an important role in the

collection, processing, analysis, and reporting of SAR data.

- Emphasize that SAR reporting is based on observable/articulable behaviors and not individual characteristics such as race, culture, religion, or political associations.
 - Include the protection of privacy and civil liberties.
 - Instruct personnel on how to use new reports and/or technology.
- ◇ Agencies should use cases and other examples to illustrate the usefulness of suspicious activity reporting as a tool to mitigate criminal activity associated with terrorism.
 - ◇ Agencies should consider the use of one-page training bulletins to help identify the current and emerging trends of the SAR process.
 - ◇ When resources are available, agencies should consider the use of e-training to reach out to individuals and ensure that agency personnel are trained in the SAR process.
- ◆ Law enforcement agencies should develop a liaison officer program to help ensure that terrorism-related suspicious activity is being gathered and reported to the proper personnel, local JTTFs, and fusion center.
 - ◇ Liaison officers may be utilized as “train the trainer” assets and assist in standardizing and reinforcing the SAR policy throughout an agency. They frequently provide a more local or immediate resource to many frontline officers and units (especially in larger agencies).
 - ◇ The liaison officer program will help expand and augment the SAR process and ensure that feedback is being provided to the original submitter.
 - ◇ The liaison officer program will help foster trust between law enforcement agencies and the public and private sector.
 - ◆ Agencies should provide feedback for training programs and updates through the auditing of completed reports to identify common errors, omissions, and training/knowledge gaps.
 - ◆ Agencies should develop outreach material for other first responders, the public, and the private sector to educate them on the recognition and reporting of behaviors and incidents indicative of criminal activity associated with international and domestic terrorism. Outreach material could include but is not limited to the following:

- ◇ Internet-based newsletters
- ◇ E-mail notification to targeted stakeholders
- ◇ Officer-to-citizen interaction programs
- ◇ Media commercials outlining the program goals and how stakeholders can help
- ◇ Community awareness/training classes
- ◇ Informational fliers
- ◇ Distribution of CDs and DVDs related to the reporting of suspicious activity
- ◇ Distribution of a redacted daily report to appropriate stakeholders
- ◇ BJA’s Communities Against Terrorism (CAT) CD

PROMISING PRACTICES IDENTIFIED DURING THE SITE VISITS

The site visits provided several promising practices related to the importance of training. These include:

- ◆ Employing terrorism awareness training to inform officers and other stakeholders on what to look for regarding suspicious activity and how to report this activity.
- ◆ Utilizing Internet-based newsletters to communicate with other stakeholders, such as the business community and private security contacts.
- ◆ Utilizing liaison officer programs to provide direct liaison with other community partners, such as fire departments, university police, and area probation/parole partners.
- ◆ Utilizing community outreach and awareness programs to provide agencies with feedback and information from the community.
- ◆ Utilizing a daily report with redacted sensitive information to communicate information to the private sector.
- ◆ Utilizing the Communities Against Terrorism (CAT) Program developed by BJA, Office of Justice Programs, DOJ. This program provides agencies with ready-made materials to assist public and private sector organizations with the identification and reporting of suspicious activity.



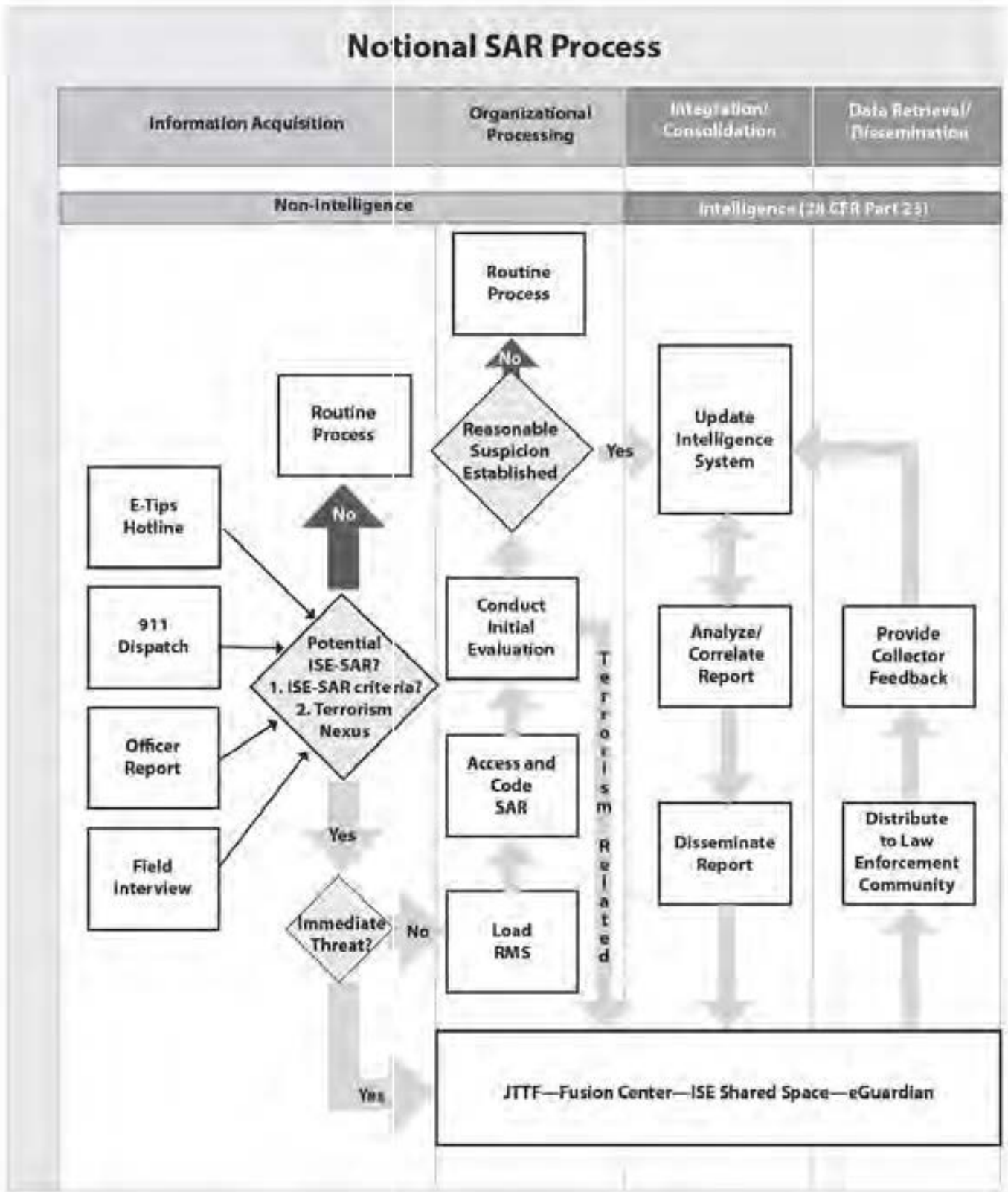
NOTIONAL SAR FLOWCHART

On the following page is a diagram, the Notional SAR Process, which represents a composite view of the processes used today by the four police departments identified in the study or discussed as a future direction for SAR reporting. As shown, SARs potentially pass through four general stages as defined in the ISE-SAR Functional Standard:

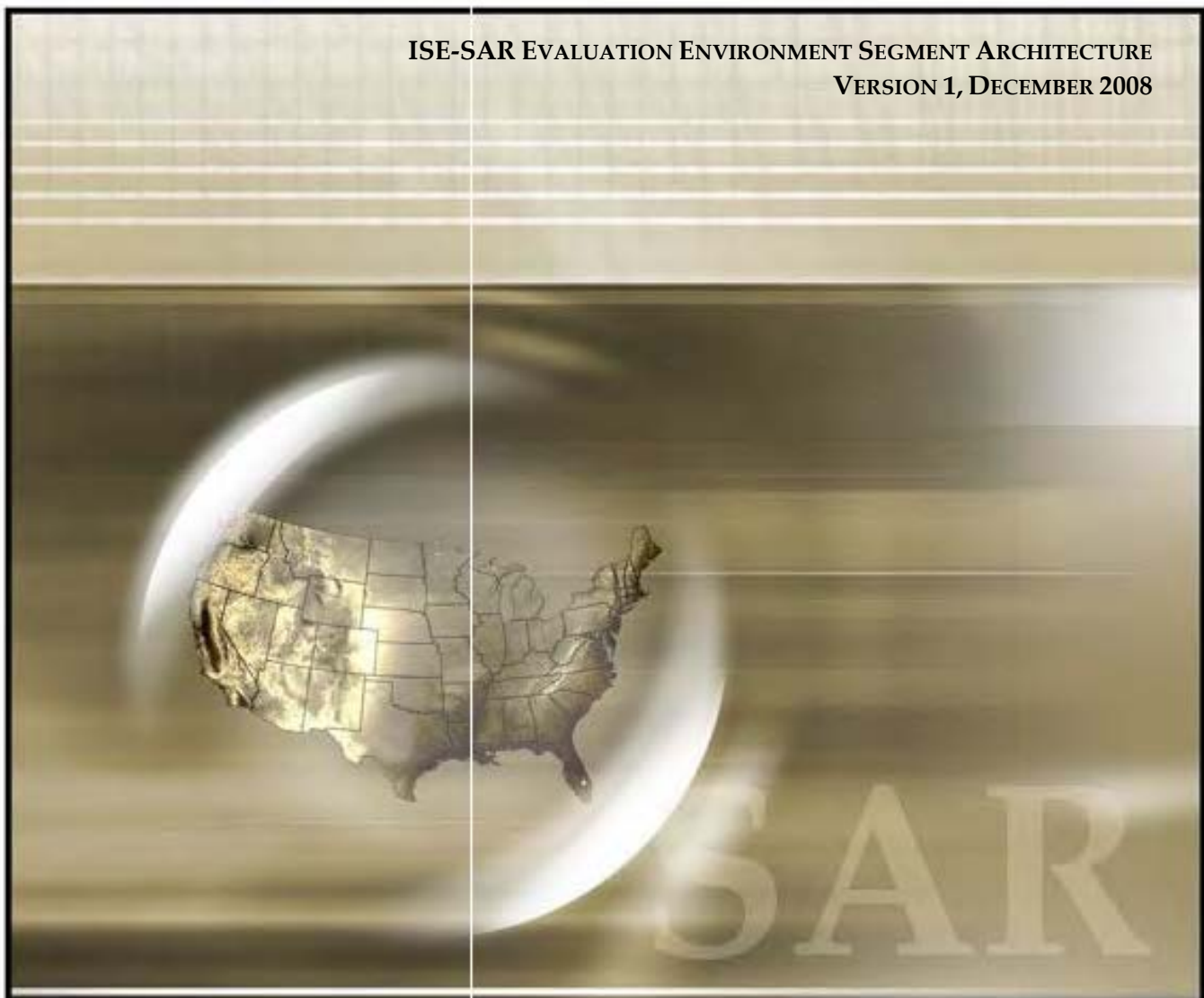
- ◆ **Information Acquisition** (how the information is originally collected, observed, or submitted)
- ◆ **Organizational Processing** (the series of manual and automated steps and decision points followed by the agency to evaluate the SAR information)
- ◆ **Integration and Consolidation** (the point at which SAR information transitions to intelligence and is then subject to 28 CFR Part 23 regulations)
- ◆ **Data Retrieval and Dissemination** (the process of making the intelligence available to other agencies and obtaining feedback on investigative outcomes)

Each agency employed different intake and preliminary review procedures to determine whether a report actually had a “potential” connection with terrorist activity subject to special treatment. In addition, as illustrated on the large horizontal box at the bottom of the diagram, each agency varied in the determination of when or if SARs are passed or made available to an external agency or system such as a JTTF or fusion center. More important, each agency described slightly different decision processes that would determine when SAR information actually became intelligence and subsequently subject to 28 CFR Part 23 requirements.

While the diagram illustrates some basic stages of a SAR processing cycle, the purpose of creating the activities or decision points shown was not to describe any particular agency’s process but to highlight the primary steps that, as a group, all of the agencies followed to one degree or another.



**ISE-SAR EVALUATION ENVIRONMENT SEGMENT ARCHITECTURE
VERSION 1, DECEMBER 2008**



**INFORMATION SHARING ENVIRONMENT (ISE)
SUSPICIOUS ACTIVITY REPORTING (SAR)
EVALUATION ENVIRONMENT (EE)
SEGMENT ARCHITECTURE**

Prepared by the
Program Manager, Information Sharing Environment

Version 1, December 2008

- A. SLT threat/risk assessment and integration of the identified SLT information needs with Federal information needs to produce a consolidated set of national priority information needs;
- B. Issuance of criteria for recognizing potential terrorism-related activity, to be utilized across all levels of government;
- C. Information gathering and reporting from Federal field units and SLTs to JTTFs and Fusion Centers; and
- D. Allocation of responsibilities for national-level, regional, and jurisdictional analysis of ISE-SAR information.

Protection of privacy and civil liberties is a major consideration for this ISE-SAR EE and, as such, warrants special attention. Additional information on privacy and civil liberties protections is located in Section 5.1 of this document.

2.2 ISE-SAR EE Participating Organizations and Proposed EE Sites

The ISE-SAR EE is sponsored and funded by the PM-ISE who is responsible for overall direction and oversight. The Department of Justice's Bureau of Justice Assistance (DoJ/BJA) provides planning, project management, and implementation services. The Office of the Assistant Secretary of Defense for Homeland Defense and America's Security Affairs (ASD HD&ASA) participates in support of the DoD force protection mission. DHS fusion center representatives will support ISE-SAR activities at participating sites. In addition, at least one DHS component organization will implement an ISE Shared Space that will be accessible by other ISE-SAR EE participants. The FBI will participate in the ISE-SAR EE primarily through its JTTFs, some of which are collocated with fusion centers. In addition to these Federal organizations, the Criminal Intelligence Coordinating Council (CICC), the International Association of Chiefs of Police (IACP), the Major City Chiefs' Association (MCCA), and the Major County Sheriffs' Association (MCSA) will provide a consolidated State and local perspective.

The following States and cities are being considered as proposed ISE-SAR EE sites. The venues listed are being considered because of a number of factors, including involvement in the MCCA SAR Support and Implementation Project (which developed several recommendations regarding implementation of the SAR process), level of technology, maturity of the Fusion Centers, and existing data efforts in the area of SARs. This list does not preclude the consideration of other States or cities as possible ISE-SAR EE participants.

- Boston (UASI)
- Houston (UASI)
- Las Vegas (UASI)
- Chicago/Illinois (UASI/State)
- Los Angeles/JRIC (UASI/State)
- Miami-Dade (UASI)
- Phoenix/Arizona (UASI/State)
- Seattle/Washington (UASI/State)

Encryption—The process of obscuring information to make it unreadable without special knowledge.

Enterprise Architecture (EA)—A strategic information asset base that defines the mission, the information necessary to perform the mission and the technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to changing mission needs.

Enterprise Search—The act of searching content to discover data, information, and knowledge wherever it exists.

Extensible Markup Language (XML)—XML is a simple, flexible text format derived from Standard Generalized Markup Language (SGML). Originally designed to meet the challenges of large-scale electronic publishing, XML also plays an increasingly important role in the exchange of a wide variety of data on the Web and elsewhere. [<http://www.w3.org/XML/>]

Federal Enterprise Architecture—A business-driven framework that defines and aligns Federal business functions and supporting technology and includes a set of five common models (performance, business, service component, data, and technical).

Fusion Center—A center established by State and major urban area governments designed to coordinate the gathering, analysis, and dissemination of terrorist-related, law enforcement, and public-safety information.

Global Justice Information Sharing Initiative (Global)—Serves as a Federal Advisory Committee (FAC) and advises the U.S. Attorney General on justice information sharing and integration initiatives. Global was created to support the broad scale exchange of pertinent justice and public safety information. It promotes standards-based electronic information exchange to provide the justice community with timely, accurate, complete, and accessible information in a secure and trusted environment.

Homeland Security Information—Any information possessed by a Federal, State, or local agency that (A) relates to the threat of terrorist activity; (B) relates to the ability to prevent, interdict, or disrupt terrorist activity; (C) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (D) would improve the response to a terrorist act. [Section 892(f)(1) of the Homeland Security Act (6 U.S.C. 482(f)(1))]

Identity and Access Management (IdAM)—An overarching term often used to refer to the processes of authentication, authorization, assignment of attributes and privileges, access management, credential issuance, and the identification of a digital identity and the binding of that digital identity to an individual.

**INFORMATION SHARING ENVIRONMENT
(ISE)-SUSPICIOUS ACTIVITY REPORTING
(SAR) EVALUATION ENVIRONMENT
IMPLEMENTATION GUIDE***

Version 1.0

January 9, 2009

** This document was previously known as the *Concept of Operations and Implementation Overview for the State and Local Law Enforcement Information Sharing Environment (ISE)-Suspicious Activity Reporting (SAR) Shared Space, Version 1.4.**

ISE-SAR Evaluation Environment Implementation Guide

into existing processes and systems used to manage other crime-related information and criminal intelligence so as to leverage existing policies and protocols utilized to protect the information, privacy, civil liberties, and other legal rights of the general public. See Section 3.2, Privacy and Civil Liberties Protection, for ISE-SARs privacy policy guidance.

Business rules for collecting, documenting, processing, and sharing terrorism-related suspicious activity information (the activity that takes place at the first, second, and third steps of the Information Flow Description contained in the ISE-SAR Functional Standard) are currently being developed and reviewed in several major cities and jurisdictions across the country. This effort is part of a PM-ISE-funded effort in collaboration with the Major Cities Chiefs Association (MCCA), the International Association of Chiefs of Police (IACP), the U.S. Department of Homeland Security, the Global Justice Information Sharing Initiative (Global), the Criminal Intelligence Coordinating Council (CICC), the U.S. Department of Defense, and the Bureau of Justice Assistance (BJA). These project partners reviewed the SAR business rules of four major police departments and a host of other major police agencies. They developed recommended guidelines for implementing a SAR process and identified best practices/business rules that can be leveraged across the law enforcement community.

Systems for Sharing SARs Among Participants

Section 1016(b)(2) of the Intelligence Reform and Terrorism Prevention Act of 2004, as amended, directs that the sharing of protected information through the ISE be done in a manner that leverages existing systems. At the present time, there is no single system or database that is used by or is available to all ISE participant agencies for sharing ISE-SARs.

The ISE-SAR Shared Spaces concept and environment described in the ISE Enterprise Architecture Framework (EAF) ultimately envisions the establishment of an ISE-wide system of attribute-based controls that would manage access authorization based on the mission and function of the ISE participant requesting access. Under such a federated system, it would be possible, for example, to grant full access to one set of users and partial access to another set of users based on credentialing levels. As more ISE-SAR Shared Spaces become operational and the standardized access rules and requirements for the shared spaces are issued, information sharing within the ISE will become more efficient. For example, once access, system certification, and accreditation rules are standardized and applied to ISE-SAR Shared Spaces that support connectivity between ISE members, members will have direct access to ISE information within those spaces, including ISE-SARs, rather than having to negotiate multiple systems with multiple access rules.

Project Sponsors and Partners

- U.S. Department of Justice (DOJ), Bureau of Justice Assistance (BJA), <http://www.ojp.usdoj.gov/BJA>
- Federal Bureau of Investigation (FBI), <http://www.fbi.gov>
- U.S. Department of Homeland Security (DHS), <http://www.dhs.gov>
- Program Manager, Information Sharing Environment (PM-ISE), <http://www.ise.gov>
- Major Cities Chiefs Association (MCCA), <http://www.majorcitieschiefs.org>

ISE-SAR Evaluation Environment Implementation Guide

- DOJ's Global Justice Information Sharing Initiative (Global), Criminal Intelligence Coordinating Council (CICC), <http://www.it.ojp.gov/global>
- U.S. Department of Defense (DoD), http://www.defenselink.mil/policy/sections/policy_offices/hd/index.html
- International Association of Chiefs of Police (IACP), <http://www.theiacp.org>
- Major County Sheriffs' Association (MCSA), <http://www.mcsheriffs.com>

ISE-SAR Evaluation Environment

The PM-ISE is sponsoring an "evaluation environment," which includes an ISE-SAR Shared Spaces evaluation initiative, to test the assumptions of sharing ISE-SAR information (based on the ISE-SAR Functional Standard and business rules) across multiple domains: state and local law enforcement agencies, state and major urban area fusion centers, federal law enforcement (DOJ), DoD, and DHS. The ISE-SAR tests will examine the usefulness of the ISE-SAR Criteria Guidance (Part B of the ISE-SAR Functional Standard) and the sharing of ISE-SAR information among major city and other law enforcement agencies, JTTFs, and fusion centers and among the fusion centers, JTTFs, and the federal government. Specifically, the evaluation environment will provide the capability to establish, test, and assess end-to-end SAR processes. These include priority information needs (PINs)/guidance, information gathering and reporting, report vetting and standards application, shared SARs, analysis and other utilization, and enabling activities. The SAR Project Management Team will evaluate the evaluation project processes and leverage best/promising practices to develop a model to be expanded to additional agencies.

The agencies participating in the Evaluation Environment (EE) initiative will assess the process of designating information as ISE-SARs, the value of the ISE-SAR information (including the value of including personal information fields), the rules for providing access to the ISE-SAR information, and the types of feedback mechanisms (e.g., for notifying source and submitting organizations of inaccurate information) that are most effective. The ISE-SAR EE will also provide access to a library of free-text SAR summaries without personal information on criminal suspects.

The ISE-SAR Evaluation Environment initiative will use multiple secure Controlled Unclassified Information (CUI) (formerly Sensitive But Unclassified [SBU]) networks as the connection and transport mechanism for sharing SARs. This will give law enforcement agencies access to the SAR Evaluation Environment through the CUI network(s) they currently utilize. Those networks could include RISSNET™; Law Enforcement Online (LEO); the Homeland Security Information Network (HSIN), the DHS network for law enforcement access; Director of National Intelligence—Unclassified (DNI-U); and other CUI networks. The ISE-SAR Evaluation Environment uses a separate server for each agency, controlled by that agency. The server resides outside the agency's firewall and is accessible as the agency's "ISE-SAR Shared Space" to other evaluation environment participants as conceptualized in the PM-ISE EAF.

Lessons learned from the evaluation environment will be used to make recommendations for modifications and expansion of the ISE-SAR Functional Standard. Such modifications are not expected to significantly affect federal, state, and local activities currently under way to implement the ISE-SAR Functional Standard. In addition, the lessons learned will be used to



FINAL REPORT:
INFORMATION SHARING ENVIRONMENT
(ISE)-SUSPICIOUS ACTIVITY REPORTING (SAR)
EVALUATION
ENVIRONMENT

This project created new and enhanced existing partnerships among the state and local ISE-SAR EE participant sites. Working with their federal partners, these agencies articulated a common need for a unified SAR process. Throughout the implementation, the users provided constructive feedback and recommendations to improve the initiative. Partnerships within the larger law enforcement community have also proved to be critically important to the achievement of the project goals. An important factor in the development of the project was the leadership of the MCCA and its Major Cities Chiefs Intelligence Commanders Working Group. Using the tenets of the successful Los Angeles Police Department SAR initiative, the MCCA and its working group provided leadership and guidance in the development of standard processes and policies to guide the sharing of SAR information. Further, in June 2008, to illustrate their support of the project, both the MCCA and the Major County Sheriffs' Association unanimously passed resolutions supporting the implementation of the SAR process within their member agencies. Additionally, the National Sheriffs' Association, the IACP, the FBI, the Criminal Intelligence Coordinating Council (CICC), and Global² have endorsed this project.

KEY RECOMMENDATIONS

A number of recommendations were made by the participating agencies based upon the lessons learned from the Evaluation Environment.³ The key recommendations were:

Leadership: Prior to initiating the next phase of this project, the project team must ensure that each agency has the support of its executive leadership. This can be accomplished through regular briefings to law enforcement associations and through the MCCA's Chief Executive Officer Briefing. Face-to-face briefings are important to allow agency executives to understand the full scope of the project and the requirements and resources necessary from their agency.

Policy and Common Processes: If the ISE-SAR EE is expanded, future participating agencies should develop policies and processes that govern the processing of SARs within all areas of their agency. This will ensure compliance with the ISE-SAR Functional Standard and related project resources. It is understood that each agency will have unique requirements, but a common set of processes across the initiative is needed.

Privacy: Future participating agencies should continue to be required to have a privacy framework that is consistent with the ISE Privacy Guidelines. Agencies should ensure transparency and openness in their privacy policy development

²In June 2008, the *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project* (SAR report) was developed to provide recommendations to the CICC from the MCCA. The SAR report was unanimously approved by the CICC in September 2008 and by Global in October 2008.

³Additional information and background regarding each of the recommendations and lessons learned can be found within the full report.

efforts by engaging privacy advocates and community leaders as the policies are developed or refined.

Technology: The proposed program management office should evaluate the best method of deploying operating systems and examine the pros and cons of other programming languages. Specific training courses or targeted technical assistance should be identified to help site staff improve their technical system administration capabilities.

Training: The executive, analytic, and line officer training programs should be delivered to all agencies that are developing a SAR process and will participate in the Nationwide SAR Initiative (NSI). Varied methods of delivery—including CD-based training, Web-based training, and video streaming—should be considered as delivery mechanisms for these courses.

Outreach: Agencies engaged in a SAR program should train their Liaison Officers to assist in public, private sector, and law enforcement outreach and awareness opportunities. Providing additional training to officers utilizing the *Safeguarding America* DVD and providing additional outreach material to the officers to interact with the public and private sectors will provide greater awareness of behaviors indicative of potential terrorism activity.

NEXT STEPS

Moving forward, the technology, training design, types of technical assistance support offered, and business processes developed during this project can be replicated for the sharing of other types of criminal activity information. Based on feedback received from the 12 participating state and local agencies, the ISE-SAR EE has proved successful in providing law enforcement agencies with a reliable and consistent method of sharing terrorism-related SARs, and this type of project can be expanded to other law enforcement activities. The following sections are contained in the full report:

- Project Overview and Background
- Leveraging Promising Practices
- Lessons Learned
- Appendices:
 - Appendix One: Project Participants
 - Appendix Two: Project Timeline
 - Appendix Three: Acronyms and Abbreviations
 - Appendix Four: Participating Agency Assessments
- Contacts for Questions

PROJECT OVERVIEW AND BACKGROUND

Chief Cathy Lanier, DC Metro: "The hope is that everyone across the country will start doing this. The value of this program lies in the number of people that buy in and participate."

The exchange of information is a critical component of law enforcement investigative efforts. Exchanging information becomes even more important when crime prevention becomes multijurisdictional. The ability to share information in a consistent and timely manner across jurisdictional boundaries is a key element to the law enforcement process. Historically, gaps in information sharing among federal, state, and local law enforcement agencies have hindered law enforcement's ability to effectively and efficiently detect, deter, prevent, and respond

to criminal and terrorist events. Information sharing gaps often stem from the fact that although law enforcement agencies individually may have pieces of information concerning criminals or terrorists and their activities, these agencies often lack a standardized mechanism by which information can be exchanged with other agencies and/or collected to support crime detection and prevention. Consequently, the law enforcement community's efforts to prevent crime or respond to a criminal or terrorist incident may be fragmented, duplicative, and/or limited.

Addressing these issues, the *National Strategy for Information Sharing* (NSIS) was released in October 2007 to prioritize and unify our nation's efforts to advance the sharing of terrorism-related information among federal, state, and local government entities; the private sector; and foreign partners while continuing to protect privacy, civil rights, and civil liberties. The NSIS calls for the federal government to support a nationwide capability for the gathering, analysis, and sharing of information, including suspicious activity and incident reports related to terrorism, with state and local governments and across the federal government. The development of the NSIS was based on several foundational documents, including the report of the National Commission on Terrorist Attacks Upon the United States,⁴ also known as the 9/11 Commission, which identified a breakdown in information sharing as a key factor contributing to the failure to prevent the September 11, 2001, attacks. In response to the 9/11 Commission's recommendations, Congress passed—and the President signed—the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). Per Section 1016, the Information Sharing Environment (ISE) was created and is defined as "an approach that facilitates the sharing of terrorism and homeland security information." Further, the IRTPA required the President to designate a Program Manager for the ISE and establish the Office of the Program Manager for the Information Sharing Environment (PM-ISE). The PM-ISE has government-wide authority to manage the ISE, assist in the development of ISE standards and practices, and monitor and assess its implementation by federal agencies as well as state and major urban area fusion centers.

⁴See <http://www.9-11commission.gov>.

Consistent with the IRTPA, the ISE sought an information sharing solution that would allow data to be shared through a distributed mechanism by which law enforcement agencies could retain data ownership and control. The solution would need to be economically developed and deployed, ideally with the ability to be easily replicated nationwide.

Consistent with the NSIS and as a priority for the establishment of the ISE, the PM-ISE—in conjunction with the U.S. Department of Justice (DOJ), Bureau of Justice Assistance (BJA); the Federal Bureau of Investigation (FBI); the Office of the Assistant Secretary of Defense for Homeland Defense and America’s Security Affairs, U.S. Department of Defense; and the U.S. Department of Homeland Security (DHS)—supported a comprehensive effort to develop a nationwide network of state and major urban area fusion centers. One of the goals of this integrated network is to facilitate the sharing of terrorism-related information across federal, state, and local communities. The information to be shared in this national network includes information based on an everyday activity of most law enforcement agencies: documenting suspicious activities observed or reported. This practice is well-institutionalized in the law enforcement community and occurs with varying degrees of standardization and formality in other communities, such as in the public health and private sectors. Throughout most communities, the reporting of SARs is not represented by a formalized, institutional process, and there is typically no established mechanism for the reporting of preoperational terrorism behaviors. Leveraging the existing SAR collection functions, the ISE-SAR Evaluation Environment (EE) recognized a broader mission need. Accordingly and consistent with the direction in the NSIS, it was deemed necessary to establish a standardized process that includes flexibility to meet the unique individual requirements of the jurisdiction in the area of privacy protection and associated data models for identifying, documenting, and sharing terrorism-related suspicious activity reports (SARs) to the maximum extent possible (initially referred to as the SAR initiative).

Former Chief William Bratton, LAPD: “We have learned from the past that there are early warning signs. Terrorism and behaviors are linked. How do I maximize our efforts and multiply our force? Analysis is critical to differentiate criminal from terrorist activity.... We all need to assess our vulnerability. Similarly with SAR—we need a united front and leadership support so that every agency in the area is contributing. If we don’t have a seamless Web and some agencies are not cooperating, we are in trouble. The effort today is not only to educate but to enlist your support and make sure you understand the importance to this effort. We want to move in a big and aggressive way to move this issue forward. We hope those of you here ‘get it.’ This is not a departure from what we normally do—there are some enhancements—we want you to take it to your people. Embrace the concept and appreciate the enhancements.”

In October 2006, a foundational meeting was held in Denver, Colorado, to bring together state and local subject-matter experts, as well as the federal project partners, to discuss the

initial plans for the development of what would eventually become the ISE-SAR EE. In response to the need of the state and local law enforcement community to develop a standardized SAR reporting process, this meeting highlighted the need to build the project using a common set of behavior-specific categories that can be related back to the precursors of terrorism.

From the beginning of this initiative, it was evident that there was a need to leverage existing technology standards, such as the National Information Exchange Model (NIEM).⁵ NIEM is based on the work of the Global Justice Information Sharing Initiative's XML Data Model and is designed to develop, disseminate, and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations, as well as support the day-to-day operations of agencies throughout the nation. NIEM enables information sharing, focusing on information exchanged among organizations as part of their current or intended business practices. The NIEM exchange development methodology results in a common semantic understanding among participating organizations and data formatted in a semantically consistent manner. NIEM standardizes content (actual data exchange standards) and provides tools and managed processes.

In early 2007, the project discussions continued with a series of conference calls and WebEx meetings to further develop the project's behavior codes, business processes, and implementation strategies. These efforts continued with the development of a reference Information Exchange Package Documentation (IEPD) intended to support SAR exchanges between and among fusion centers and their federal, state, local, and tribal law enforcement partners. Developed by state and local stakeholders, the IEPD was ultimately enhanced to be consistent with the ISE Privacy Guidelines and the *Privacy and Civil Liberties Policy Development Guide and Implementation Templates*. The development of the IEPD ultimately resulted in the development of the ISE-SAR Functional Standard.

In January 2008, the first ISE-SAR Functional Standard was released by the PM-ISE to build upon, consolidate, and standardize nationwide aspects of those ISE-relevant activities already occurring at the federal, state, and local levels with respect to the

Commissioner Gerald Bailey, Florida Department of Law Enforcement: "Law enforcement has excellent information gathering techniques and skills in place. However, in order for that information to be useful, it must be shared. Simply put, the heart of this initiative is to glean information from routine police work for the fusion centers so that they may provide the analysis and intelligence that is critical to our efforts against crime and terrorism. We can no longer operate as 50 independent states, but as one country with one goal—to keep our citizens safe."

⁵See www.it.ojp.gov/iepd.

processing, sharing, and use of suspicious activity information. The ISE-SAR Functional Standard provides guidance on a limited end-to-end information sharing process and continues to be enhanced to meet the needs of the agencies. It was developed for the analysis of SARs and includes the business rules for gathering, documenting, processing, and sharing terrorism-related suspicious activity information. These efforts ultimately resulted in the development of the ISE-SAR EE, which was used to outline the scope, objectives, and goals of the project, including the implementation of the SAR Summary Reports Library Pilot Project and SAR Operational Study Evaluation Project (now known as the ISE-SAR Evaluation Environment [ISE-SAR EE]).

The Evaluation Environment officially began on September 1, 2008, and concluded on September 30, 2009. The purpose of the Evaluation Environment (EE) at state and major urban area fusion centers and local law enforcement organizations was to test and evaluate the policies, procedures, and technology needed to implement a

Sheriff Gillespie, Las Vegas Metro Police Department: "The strength [of the NSI] is in partnering and the common mission. Today, we face unique challenges in law enforcement not only from the traditional aspect. We cannot allow the human trust aspects to interfere with the actions we must take. This is a VERY worthwhile approach to information sharing, and I look forward to utilizing it in southern Nevada."

unified process that fosters a broader sharing of SARs that are reasonably indicative of potential intelligence gathering or preoperational planning related to terrorism or other criminal activity. The project was developed in a phased approach beginning with the development of privacy frameworks and the implementation of the technology. The first data was not shared until May of 2009. The participating agencies continue to implement the processes and procedures needed to successfully share SAR information.

The SAR Summary Reports Library was a conceptual pilot project that provided a collection point for existing SAR summary or free-text narrative information reports. The Library pilot was designed to provide a method for fusion centers and other authorized individuals (e.g., sworn law enforcement and analysts) to enter, store, and access SAR documents (e.g., Summary SARs, Daily Briefs, and Weekly Analytic Reports), regularly created and published by fusion centers and other contributing agencies. Because of the need to concentrate on the larger ISE-SAR EE rollout, the full implementation of the Library project was suspended in order to focus on the primary purpose of the project. However, the development of the Library project and its initial testing demonstrated the potential success of the technology design and provided a viable tool for further applications.

The ISE-SAR EE operated on the concept of "Shared Spaces," which is an idea consistent with the guidance provided in the IRTPA. The Shared Spaces concept uses a networked and distributed information exchange process to make standardized terrorism-related information available through Common Terrorism Information Sharing

SYSTEM SECURITY

The ISE-SAR EE is not a national security system and does not contain classified information. The ISE-SAR EE project uses multiple secure Sensitive But Unclassified (SBU) networks, including the DOJ-supported Regional Information Sharing Systems® Secure Intranet (RISSNET™), the FBI-supported Law Enforcement Online, and DHS-supported Homeland Security Information Network,²⁷ as the connection and transport mechanisms for sharing SARs. This gives law enforcement agencies access to the ISE-SAR EE through the SBU network(s) they currently utilize. The ISE-SAR EE uses a separate server for each agency controlled by that agency. Additionally, the eGuardian system provides the connection between the JTTF and the ISE-SAR Shared Spaces, whereas the DHS Shared Space provides a connection to all DHS entities.

The ISE-SARs are stored, processed, and disseminated in a protected information environment that provides adequate security controls. These controls include:

- Controlled access to the information that allows only authorized users—limited to certain individuals assigned by participating fusion centers—to access, retrieve, and display ISE-SAR information.
- Use of DOJ’s Trusted Broker solution to allow access to the Shared Spaces from multiple SBU networks. The Trusted Broker is an identity management process that allows users to avoid having to use multiple usernames and passwords to sign on to different systems.
- Encrypted transmission of information sent between Shared Spaces sites and the NCIRC portal.
- Use of VPN and additional firewall technology installed at the fusion center sites to limit access by ISE-SAR EE users to only those servers that are supporting the Shared Spaces environment.
- Force a ISE-SAR EE participating agency to explicitly “mark” SARs that should be pushed to the agency’s Shared Spaces repository and thereby ensure that only information it is allowed to share by its constitution or statutes, local ordinances, or agency policy is made available to the broader ISE-SAR EE community.
- The Implementation Guide is used to ensure that all participants use the same standards, rules, process, and guidelines.

²⁷Homeland Security State and Local Intelligence Community (HSLIC).

APPENDIX ONE: PROJECT PARTICIPANTS

PROJECT SPONSORS AND PARTNERS:

- U.S. Department of Justice (DOJ), Bureau of Justice Assistance (BJA), <http://www.ojp.usdoj.gov/BJA>
- Federal Bureau of Investigation (FBI), <http://www.fbi.gov>
- U.S. Department of Homeland Security (DHS), <http://www.dhs.gov>
- Program Manager, Information Sharing Environment (PM-ISE), <http://www.ise.gov>
- Major Cities Chiefs Association (MCCA), <http://www.majorcitieschiefs.org>
- DOJ's Global Justice Information Sharing Initiative (Global), Criminal Intelligence Coordinating Council (CICC), <http://www.it.ojp.gov/global>
- U.S. Department of Defense (DoD), http://www.defenselink.mil/policy/sections/policy_offices/hd/index.html
- International Association of Chiefs of Police (IACP), <http://www.theiacp.org>
- Major County Sheriffs' Association (MCSA), <http://www.mcsheriffs.com>

PROJECT PARTICIPANTS:

- Arizona Counter Terrorism Information Center (AcTIC)/Arizona Department of Public Safety
- Boston Regional Intelligence Center/Boston Police Department
- Chicago Police Department
- Florida Fusion Center/Florida Department of Law Enforcement
- Houston Regional Intelligence Service Center/Houston Police Department
- Los Angeles Police Department
- Miami-Dade Police Department
- New York State Intelligence Center (NYSIC)/New York State Police
- Washington State Fusion Center/Seattle Police Department
- Southern Nevada Counter-Terrorism Center/Las Vegas Metropolitan Police Department
- Virginia Fusion Center/Virginia State Police
- Washington Regional Threat and Analysis Center/Washington, DC, Metropolitan Police Department

PROJECT RECOMMENDATIONS FROM THE BOSTON POLICE DEPARTMENT

- There is a need for some form of governing body, such as a national program office, to monitor the Nationwide SAR Initiative (NSI) and take the lead in the coordination efforts between agencies at all levels of government.
- There should be a national training program to assist agencies in the development and/or delivery of SAR-related training.
- If it can be made affordable, there is tremendous value in the creation of a national users group for the NSI. A national users group would bring agencies together so they can form relationships and discuss issues, best practices, and lessons learned regarding the NSI.
- There is a need for ongoing technical support in order for the technology to evolve with the project.
- A national legal office should not be created. Multiple legal resources already exist for law enforcement agencies at all levels of the government.
- A “daily digest” should be created for the ISE-SAR Shared Spaces. This capability would allow agencies to monitor the SARs that are being submitted to the ISE-SAR Shared Spaces on a daily basis and could save the time and effort it takes to conduct multiple searches.
- An appropriate threshold should be clearly defined for entering a SAR into the ISE-SAR Shared Spaces. During the ISE-SAR EE, there seemed to be a disparate amount of SARs being entered between the agencies. BPD wants to avoid the entry of information into the ISE-SAR Shared Spaces that is not of value and avoid large volumes of information being “dumped” into the system.

Note: This is a non-exhaustive list for Background Purposes

Review of Advocate Websites for Concerns and Issues on ISE-related Activities

1. Review of websites of proposed P/CL and open government advocate groups to identify concerns and positions on ISE-related activities for discussion during engagement meetings.
 - a. American Civil Liberties Union (ACLU) – Mike German
 - **ACLU Lawsuit Seeks Information from FBI on Nationwide System for Collecting “Suspicious System May be Used to Track and Store Information about Innocent Americans with No Evidence of Wrongdoing** (“The American Civil Liberties Union [in August 2011] filed a Freedom of Information Act (FOIA) lawsuit challenging the government’s failure to release documents about the FBI’s nationwide system of collecting and sharing so-called “Suspicious Activity Reports” from local, state and federal law enforcement agencies....The public needs to know if the government is collecting information for eGuardian through the illegal profiling of innocent Americans on the basis of their race, religion or constitutionally protected beliefs and activities.”) <http://www.aclu.org/free-speech-technology-and-liberty/aclu-v-united-states-department-justice-complaint-injunctive>
 - We encourage greater oversight and transparency in the ISE SAR program to ensure these [ISE-SAR FS version 1.5]are being met and maintained. <http://www.aclu.org/spy-files/more-about-suspicious-activity-reporting>
 - Rather than tightening SAR collection standards, however, many federal, state and local law enforcement agencies are expanding them by encouraging not just police but the general public to report suspicious activity.... And none of these new SAR programs have the same limiting language that was added to the ISE functional standard, making it far more likely that both the police and the public will continue over-reporting the commonplace behavior of their neighbors. <http://www.aclu.org/spy-files/more-about-suspicious-activity-reporting>
 - Photographers appear to be the most frequent targets of SAR and SAR-like information collection efforts. Whether lawfully photographing scenic railroad [stations](#), government-commissioned art displays outside federal [buildings](#) or national [landmarks](#), citizens, [artists](#) and [journalists](#) have been systematically [harassed](#) or detained by federal, state, and local law enforcement. In some instances, the ensuing confrontation with police escalates to the point where the photographer is arrested and their photos erased or cameras confiscated with no reasonable indication that criminal activity is involved. A Los Angeles Sheriff’s Deputy even [threatened](#) to put a

DRAFT/DELIBERATIVE

1

Note: This is a non-exhaustive list for Background Purposes

NSI's Program Management Office, in consultation with the PM-ISE, decides to reshape the concept of operations to better address non-terrorist threats. Such a move would likely prove useful for state and local law enforcement agencies forced to deal with crime tied to drugs, gangs, and other non-terrorist activities.

The numerous programs tied to the Nationwide SAR Initiative and the broader Information Sharing Environment signal an important step toward alleviating what the 9/11 Commission recognized as a major flaw in the country's national security apparatus. And with the recent uptick in "homegrown" extremism, programs like the NSI, which explicitly reaches out to state and local law enforcement officials, will prove especially important. How these initiatives are implemented—and how they evolve—will ultimately determine their success.

○ See at http://csis.org/files/publication/100831_nelson_sar.pdf for more information.

c. Congressional Research Service (CRS):

- i. "Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress" (June 10, 2011) at <http://fpc.state.gov/documents/organization/166837.pdf>
- ii. **Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress**" (December 28, 2011) at <http://www.fas.org/sgp/crs/intel/R40901.pdf> raises the question of whether a national system may become overwhelmed by the sheer number of inputs.

The CRS report, in fact, identifies four primary issues that Congress, as the final overseer of the NSI, will face in plotting a course for DHS' suspicious activity reporting (SAR) programs:

- ***Too Many Dots.*** The NSI is designed to increase the amount of information flowing from state and local law enforcement agencies to the federal government, but the goal of "connecting the dots" will become more difficult as the number of dots increase. An avalanche of irrelevant or redundant data will divert law enforcement personnel and other resources from meaningful work. During a 40-month period prior to a 2007 SAR pilot program, for example, the FBI documented about 108,000 potential terror threats, suspicious incidents, and terrorist watchlist hits. The report

DRAFT/DELIBERATIVE

5

Note: This is a non-exhaustive list for Background Purposes

points to a need for Congress to consider which agency or agencies should handle quality control of SARs to prevent system overload.

- **Data Privacy and Access.** To achieve the objectives of the program, the report states, agency partners must establish protocols for protecting the privacy and civil liberties of individual citizens. An authorized use standard, including identification/authentication and privilege management, should be developed for users of a system that contains sensitive information, and Congress should examine NSI policies governing data privacy and access.
- **Information Technology (IT) Infrastructure.** The success of the NSI will depend on the infrastructure that supports it, and funding may fall short at fusion centers in some jurisdictions. As the minder of the nation's purse strings, Congress will need to consider ways to provide funding to fusion centers for this purpose.
- **Metrics.** Critics of SAR programs, who claim that a focus on suspicious activity will lead to racial and ethnic profiling and an avalanche of spurious tips, are – much like the DHS in formulating the program – relying on anecdotal or even hypothetical information. The only way to validate the program's effectiveness is through concrete measurements – of how many of the SARs collected by the program are meaningful intelligence “dots,” or whether the right “dots” are being connected as a result of the program, for example. The report recommends that Congress request the DHS' Program Management Office for the NSI to develop these metrics.

Metrics are an important first step in determining the NSI's value – but once those metrics are established, of course, DHS will be faced with the task of achieving these new standards of success. History has shown that SAR reporting has stopped several terrorist attacks. But will a nationwide SAR program increase the likelihood that additional attacks will be stopped? The Department of Homeland Security thinks so – it just can't prove it yet.

- d. Berkeley City Council backs police reforms with civil liberties in mind. The council decided Tuesday night to approve recommendations that would make it more difficult for police to report suspected terrorists and criminals to regional and federal authorities; stop holding some people in its jails the federal government wants for immigration violations; and restrict police from gathering intelligence on people engaged in nonviolent, non-felonious civil disobedience.

DRAFT/DELIBERATIVE

6

Note: This is a non-exhaustive list for Background Purposes

http://www.mercurynews.com/breaking-news/ci_20901524/berkeley-passes-tentative-police-reforms-civil-liberties-mind

- e. Center for Investigative Reporting – GW Schultz (in partnership with NPR) -- Civil liberties and privacy advocates, including members of Congress, have criticized some homeland security initiatives as intrusive and prone to abusive profiling. Advocates say such reporting can fuel anxiety and create a chilling atmosphere in which people who seem different are targeted for extra attention. Suspicious activity reports, they add, are part of a broader trend of surveillance of the innocent and suspect alike since 9/11. <http://americaswarwithin.org/articles/2011/09/07/finding-meaning-suspicious-activity-reports-more-art-science>
- f. Geoffrey Stone, a constitutional law professor at the University of Chicago, said that government officials should consider how a program affects the exercise of political and religious beliefs, regardless of whether they insist the information is being used appropriately.
 - i. Publications include: *Speaking Out! Reflections on Law, Liberty and Justice* (2010); *Top Secret: When Our Government Keeps Us in the Dark* (2007) and *War and Liberty: An American Dilemma* (2007); and *Perilous Times: Free Speech in Wartime from the Sedition Act of 1798 to the War on Terrorism* (2004)
- g. [Juliette Kayyem](#), a former homeland security assistant secretary in the Obama administration and a onetime adviser to Massachusetts Gov. Deval Patrick, said that “You have just a tremendous amount of information going into the intelligence-sharing apparatus in the hopes that it will either come up with terrorism or suspicious activity or criminal activity,” “That’s a lot of input ... to ensure that you’re going to connect the dots better, right? One clear way is to make sure the dots are better. There (are) too many dots right now.”

DRAFT/DELIBERATIVE

7

1 BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General

2 MELINDA L. HAAG
3 United States Attorney

4 ANTHONY J. COPPOLINO
5 Deputy Branch Director

6 PAUL G. FREEBORNE
7 Senior Trial Counsel
8 Va. Bar No. 33024

9 KIERAN G. GOSTIN
10 Trial Attorney
D.C. Bar. No. 1019779

11 Civil Division, Federal Programs Branch
12 U.S. Department of Justice
13 P.O. Box 883
14 Washington, D.C. 20044
15 Telephone: (202) 353-0543
16 Facsimile: (202) 616-8460
17 E-mail: paul.freeborne@usdoj.gov

Attorneys for the Defendants

18 **UNITED STATES DISTRICT COURT**
19 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**

20 WILEY GILL; JAMES PRIGOFF; TARIQ
21 RAZAK; KHALID IBRAHIM; and AARON
22 CONKLIN,

Plaintiffs,

v.

25 DEPARTMENT OF JUSTICE, *et al.*,

26 Defendants.
27

No. 3:14-cv-03120 (RS)

**NOTICE OF MOTION AND
MEMORANDUM OF LAW IN SUPPORT
OF DEFENDANTS' MOTION FOR
RELIEF FROM NONDISPOSITIVE
PRETRIAL ORDER OF MAGISTRATE
JUDGE**

28
Gill v. Dep't of Justice, No. 14-3120 (RS)
Notice of Motion and Memorandum of Law in Support of Defendants' Motion for Relief from Nondispositive Pretrial
Order of Magistrate Judge

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

NOTICE OF MOTION FOR RELIEF

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE THAT Defendants hereby move for relief from portions of Magistrate Judge Kandis A. Westmore’s Order Granting in Part and Denying in Part Plaintiffs’ Motion to Complete Administrative Record, Dkt. No. 88. A proposed order granting the motion is attached hereto.

Pages ER 312-21 intentionally omitted.

1 BENJAMIN C. MIZER
 Principal Deputy Assistant Attorney General
 2 ANTHONY J. COPPOLINO
 Deputy Branch Director
 3 PAUL G. FREEBORNE
 Virginia Bar No. 33024
 4 Senior Trial Counsel
 5 KIERAN G. GOSTIN
 Trial Attorney
 6 D.C. Bar No. 1019779

7 Civil Division, Federal Programs Branch
 U.S. Department of Justice
 8 P.O. Box 883
 Washington, D.C. 20044
 9 Telephone: (202) 353-0543
 10 Facsimile: (202) 616-8460
 E-mail: paul.freeborne@usdoj.gov

11 *Attorneys for Federal Defendants*

12
 13 **UNITED STATES DISTRICT COURT**
FOR THE NORTHERN DISTRICT OF CALIFORNIA

15 WILEY GILL; JAMES PRIGOFF; TARIQ
 16 RAZAK; KHALID IBRAHIM; and AARON
 CONKLIN,

17 Plaintiffs,

18 v.

19 DEPARTMENT OF JUSTICE, *et al.*,

20 Defendants.
21
22

No. 3:14-cv-03120 (RS)(KAW)

**DEFENDANTS' OPPOSITION TO
 PLAINTIFFS' MOTION TO COMPLETE
 THE ADMINISTRATIVE RECORD**

Hearing Date: December 3, 2015

Time: 11:00 a.m.

Judge: Hon. Kandis A. Westmore

Gill v. Dep't of Justice, No. 14-3120, Defendants' Opposition to Plaintiffs' Motion to Complete the Administrative Record

TABLE OF CONTENTS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

INTRODUCTION 1

BACKGROUND 3

 I. PLAINTIFFS CHALLENGE ONLY THE “REASONABLY INDICATIVE”
 STANDARD IN THE FUNCTIONAL STANDARD 3

 II. THE ADMINISTRATIVE RECORD IS APPROPRIATELY TAILORED TO
 THE PENDING CHALLENGE 5

 III. THE PARTIES’ MEET AND CONFER 7

ARGUMENT 7

 I. STANDARD OF REVIEW 7

 II. PLAINTIFFS HAVE FAILED TO CARRY THEIR BURDEN OF SHOWING
 THAT THE CERTIFIED ADMINSTRATIVE RECORD IS INCOMPLETE 8

 A. The Record Is Properly Limited To Plaintiffs’ Challenge to the “Reasonably
 Indicative” Standard 9

 B. Granting Plaintiffs’ Motion Would Be Tantamount to Granting
 Discovery 13

 C. Deliberative Material Is Properly Excluded from the
 Administrative Record 14

 III. NO GROUNDS EXIST TO PERMIT CONSIDERATION OF
 EXTRA-RECORD EVIDENCE 16

CONCLUSION 18

Pages ER 324-73 intentionally omitted.

1 BENJAMIN C. MIZER
 Principal Deputy Assistant Attorney General
 2 ANTHONY J. COPPOLINO
 Deputy Branch Director
 3 PAUL G. FREEBORNE
 Virginia Bar No. 33024
 4 Senior Trial Counsel
 KIERAN G. GOSTIN
 5 D.C. Bar No. 1019779
 Trial Attorney
 6

7 Civil Division, Federal Programs Branch
 U.S. Department of Justice
 8 P.O. Box 883
 Washington, D.C. 20044
 9 Telephone: (202) 353-0543
 Facsimile: (202) 616-8460
 10 E-mail: paul.freeborne@usdoj.gov

11 *Attorneys for Federal Defendants*

12 **UNITED STATES DISTRICT COURT**
 13 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**

14 WILEY GILL; JAMES PRIGOFF; TARIQ
 15 RAZAK; KHALID IBRAHIM; and AARON
 CONKLIN,

16 Plaintiffs,

17 v.

18 DEPARTMENT OF JUSTICE, *et al.*,

19 Defendants.
 20
 21
 22
 23
 24
 25
 26
 27
 28

No. 3:14-cv-03120 (RS)

**DEFENDANTS' OPPOSITION TO
 PLAINTIFFS' SPECIAL MOTION TO
 ESTABLISH RIGHT TO DISCOVERY ON
 THE DEPARTMENT OF JUSTICE'S
 STANDARD FOR SUSPICIOUS
 ACTIVITY REPORTING**

Hearing Date: August 20, 2015
 Time: 1:30 p.m.
 Judge: Hon. Richard Seeborg
 Ctrm: 3, 17th Floor

Table of Contents

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

INTRODUCTION 1

BACKGROUND 4

 I. Procedural Background..... 4

 II. The FBI’s Privacy Impact Assessment for the eGuardian System 5

 A. The E-Government Act of 2002..... 5

 B. The FBI’s eGuardian Privacy Impact Assessment 6

ARGUMENT..... 9

 I. Discovery Standard in an APA Action 10

 II. Plaintiffs Have Failed To Plead a Cognizable Claim that Unlocks the Doors of
Discovery 11

 A. Plaintiffs Have Not Identified a DOJ Standard that Is Distinct from the
Functional Standard..... 11

 B. The Privacy Impact Assessment Does Not Impose Legal Obligations..... 14

 C. Plaintiffs’ Other Allegations Likewise Fail to Set Forth a Cognizable
Claim 17

 D. Plaintiffs’ Citation of Documents Not Referenced in the Complaint Does
Not Entitle Plaintiffs to Discovery 18

 III. Even If Plaintiffs’ “DOJ Standard” Claim Could Proceed, Discovery Should Not
Be Permitted in this APA Action..... 19

CONCLUSION..... 21

No. 17-16107

**In the United States Court of Appeals
for the Ninth Circuit**

WILEY GILL; JAMES PRIGOFF; TARIQ RAZAK; KHALED IBRAHIM;
AARON CONKLIN,

Plaintiffs-Appellants,

v.

DEPARTMENT OF JUSTICE; JEFF SESSIONS, Attorney General; PROGRAM
MANAGER – INFORMATION SHARING ENVIRONMENT; KSHEMENDRA
PAUL, in his official capacity as Program Manager of the Information Sharing
Environment,

Defendants-Appellees.

EXCERPTS OF RECORD
Volume 4 of 4 – Pages 376 to 656

On Appeal from the United States District Court
for the Northern District of California
No. 3:14-cv-03120-RS
The Honorable Richard Seeborg, District Judge

Stephen Scotch-Marmo
stephen.scotch-
marmo@morganlewis.com
Michael James Ableson
michael.ableson@morganlewis.com
MORGAN, LEWIS & BOCKIUS LLP
101 Park Avenue
New York, NY 10178
T. 212.309.6000
F. 212.309.6001

Linda Lye
llye@aclunc.org
Julia Harumi Mass
jmass@aclunc.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN
CALIFORNIA, INC.
39 Drumm Street
San Francisco, CA 94111
T. 415.921.2493
F. 415.255.8437

Attorneys for Appellants
Wiley Gill, James Prigoff, Tariq Razak, Khaled Ibrahim, and Aaron Conklin

(Additional Counsel on Inside Cover)

Mitra Ebadolahi
mebadolahi@aclusandiego.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF SAN DIEGO AND
IMPERIAL COUNTIES
P.O. Box 87131
San Diego, CA 92138
T. 619.232.2121
F. 619.232.0036

Peter Bibring
pbibring@aclusocal.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF SOUTHERN
CALIFORNIA
1313 West 8th Street
Los Angeles, CA 90017
T. 213.977.9500
F. 213.977.5299

Hugh Handeyside
hhandeyside@aclu.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
T. 212.549.2500
F. 212.549.2654

Jeffrey S. Raskin
jeffrey.raskin@morganlewis.com
Phillip J. Wiese
phillip.wiese@morganlewis.com
MORGAN LEWIS & BOCKIUS LLP
One Market, Spear Street Tower
San Francisco, CA 94105
T. 415.442.1000
F. 415.442.1001

Christina Sinha
christinas@advancingjustice-alc.org
ASIAN AMERICANS ADVANCING
JUSTICE – ASIAN LAW CAUCUS
55 Columbus Avenue
San Francisco, CA 94111
T. 415.848.7711
F. 415.896.1703

Attorneys for Appellants
Wiley Gill, James Prigoff, Tariq Razak, Khaled Ibrahim, and Aaron Conklin

INDEX

Docket No.	Description	Date	Page No.
Volume 1 of 4 – Pages 1 to 10			
134	Order On Cross Motions For Summary Judgment	03/27/17	1
Volume 2 of 4 – Pages 11 to 252			
136	Notice Of Appeal To The United States Court Of Appeals For The Ninth Circuit	05/28/17	11
135	Judgment	03/29/17	16
127	Declaration Of Wiley Gill In Support Of Plaintiffs' Motion For Summary Judgment	11/03/16	17
	Exhibit 1: Letter, Dated January 3, 2014		25
	Exhibit 2: Letter, Dated June 23, 2014		28
	Exhibit 3: Letter, Dated February 29, 2016		48
124	Defendants' Reply In Support Of Motion For Summary Judgment, Opposition To Plaintiffs' Motion For Summary Judgment, And Opposition To Plaintiffs' Motion To Strike Defendants' Declarations And To Supplement The Record With Plaintiffs' Declarations	10/20/16	68
121	Plaintiffs' Motion To Strike Defendants' Declarations And To Supplement The Record With Plaintiffs' Declarations; Memorandum Of Points And Authorities In Support	09/22/16	73
120	Declaration Of Aaron Conklin In Support Of Plaintiffs' Motion For Summary Judgment And Plaintiffs' Opposition To Defendants' Motion For Summary Judgment	09/22/16	88

INDEX
(continued)

Docket No.	Description	Date	Page No.
119	Declaration Of Khaled Ibrahim In Support Of Plaintiffs' Motion For Summary Judgment	09/22/16	94
	Exhibit 1: Suspicious Activity Report		100
118	Declaration Of Tariq Razak In Support Of Plaintiffs' Motion For Summary Judgment	09/22/16	104
	Exhibit 1: Suspicious Activity Report		111
	Exhibit 2: Letter, Dated February 13, 2015		115
	Exhibit 3: Letter, Dated April 9, 2015		132
	Exhibit 4: Letter, Dated May 21, 2015		136
	Exhibit 5: Letter, Dated June 25, 2014		139
117	Declaration Of James Prigoff In Support Of Plaintiffs' Motion For Summary Judgment And Plaintiffs' Opposition To Defendants' Motion For Summary Judgment	09/22/16	143
	Exhibit 1: Business Card With Note, Dated August 19, 2004		153
	Exhibit 2: Suspicious Activity Report On James Burt Prigoff, Dated June 21, 2004		156
	Exhibit 3: Suspicious Activity Report On James Burt Prigoff, Dated October 18, 2004		160
	Exhibit 4: Suspicious Activity Report On James Burt Prigoff, Dated November 8, 2004		165

INDEX
(continued)

Docket No.	Description	Date	Page No.
	Exhibit 5: Letter, Dated March 24, 2015		168
	Exhibit 6: Letter, Dated May 19, 2015		172
	Exhibit 7: Letter, Dated January 27, 2016		176
	Exhibit 8: Letter, Dated January 8, 2015		179
	Exhibit 9: Letter, Dated September 15, 2015		181
	Exhibit 10: ISE-SAR Criteria Guidance		186
	Exhibit 11: Potential Indicators of Terrorist Activities Related to the General Public		201
116	Declaration Of Linda Lye In Support Of Plaintiffs' Opposition To Defendants' Motion For Summary Judgment And Cross-Motion For Summary Judgment	09/22/16	204
	Exhibit 1: Letter, Dated July 12, 2013		209
	Exhibit 2: Emails, Dated July 22, 2013, July 23, 2013 and August 2, 2013		212
	Exhibit 3: Letter, Dated March 7, 2016		217
	Exhibit 4: Letter, Dated March 21, 2016		220
	Exhibit 5: Regional Information Sharing Systems (RISS)		238
	Exhibit 6: 28 CFR Part 23 Frequently Asked Questions		241

INDEX
(continued)

Docket No.	Description	Date	Page No.
113	Defendants' Notice Of Motion For Summary Judgment And Memorandum In Support	08/18/16	243
Volume 3 of 4 – Pages 253 to 375			
107	Defendants' Notice Of Filing Of Supplemental Administrative Record	05/10/16	253
	Amended Certification Of Administrative Record And Supplemental Administrative Record		255
	Document 1: ISE Privacy Guidelines (December 4, 2006)		265
	Document 3: National Strategy for Information Sharing (October 2007)		268
	Document 5: Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project (October 1, 2008)		272
	Document 6: ISE Suspicious Activity Reporting Evaluation Environment Segment Architecture (December 2008)		290
	Document 7: ISE SAR Evaluation Environment Implementation Guide, Version 1.0 (January 9, 2009)		293
	Document 8: Final Report: Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Evaluation Environment (January 2010)		296

INDEX
(continued)

Docket No.	Description	Date	Page No.
	Document 9: Review of Advocate Websites for Concerns and Issues on ISE-Related Activities (2012)		306
94	Notice Of Motion And Memorandum Of Law In Support Of Defendants' Motion For Relief From Nondispositive Pretrial Order Of Magistrate Judge	01/15/16	310
79	Defendants' Opposition To Plaintiffs' Motion To Complete The Administrative Record	10/22/15	322
56	Defendants' Opposition To Plaintiffs' Special Motion To Establish Right To Discovery On The Department Of Justice's Standard For Suspicious Activity Reporting	07/10/15	374
Volume 4 of 4 – Pages 376 to 656			
52	Defendants' Notice Of Filing Of Administrative Record	06/16/15	376
	Certification of Administrative Record		380
53	Administrative Record	06/16/15	—
	Exhibit 1: White House Memorandum on Guidelines and Requirements in Support of the Information Sharing Environment (December 16, 2005) (wh121605- memo .pdf)		390

INDEX
(continued)

Docket No.	Description	Date	Page No.
	Exhibit 3: The Information Sharing Environment Suspicious Activity Reporting (SAR) Working Group's Business Process Analysis (February 13, 2007) (SAR_BusinessAnalysis_final20070215.doc)		395
	Exhibit 6: PM-ISE Memorandum, Release of the Information Sharing Environment (ISE) Functional Standard for Suspicious Activity Reporting (SAR) Version 1.0 (ISE-FS-200) (January 25, 2008) (Transmittal_Memorandum_ISE-FS-200.pdf)		397
	Exhibit 7: Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.0 ISE-FS-200 (January 25, 2008) (Functional Standard_Issuance_Version_1.0_Final_Signed).pdf)		401
	Exhibit 15: Information Sharing Environment – Suspicious Activity Reporting Functional Standard And Evaluation Environment Initial Privacy and Civil Liberties Analysis September 2008— Version 1 (September 2008) (ISE-SAR FS and EE Initial Privacy and Civil Liberties Analysis_090508.pdf)		433

INDEX
(continued)

Docket No.	Description	Date	Page No.
	Exhibit 20: Feedback Session with Privacy and Civil Liberties Advocates: Suspicious Activity Reporting (SAR) Line-Officer Training and the ISE-SAR Functional Standard—Agenda (February 13, 2009) (Agenda February 18, 2009 - SAR Feedback Session.doc)		447
	Exhibit 26: Memorandum for Release of the Information Sharing Environment (ISE) Functional Standard for Suspicious Activity Reporting, Version 1.5 (May 21, 2009) (ISE-SAR Functional Standard V1.5 Cover Letter.pdf)		448
	Exhibit 28: Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) version 1.5 (May 21, 2009) (ISE-FS-200_ ISESAR_ Functional_ Standard_ V1.5_ Issued.pdf)		450
	Exhibit 30: NSI Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations report issued by PMISE on privacy compliance outcomes of the ISE SAR Evaluation Environment and providing recommendations for additional privacy protections during nationwide expansion of the NSI (July 2010) (NSI_PCRCL_ Analysis_July2010_final.pdf)		486

INDEX
(continued)

Docket No.	Description	Date	Page No.
	Exhibit 40: ISE-SAR Functional Standard Version 1.5.5 Executive Summary (February 17, 2015) (FS v1_5_5 Executive Summary PM_ISE 21715 Comprehensive)		493
	Exhibit 41: Final and signed version of the ISE-SAR Functional Standard version 1.5.5 issued by the PM-ISE. (February 23, 2015) (SAR_FS_1.5.5_IssuedFeb2015.pdf)		501
46-1	Defendants' Answer To Complaint	04/24/15	561
40	Joint Case Management Statement & [Proposed] Order	03/05/15	566
38	Order Denying Motion To Dismiss	02/20/15	569
36	Joint Case Management Statement & [Proposed] Order	12/31/14	581
21	Notice Of Motion And Memorandum Of Law In Support Of Defendants' Motion To Dismiss	10/16/14	586
—	District Court Docket	—	632

1 BENJAMIN C. MIZER
 Principal Deputy Assistant Attorney General
 2 ANTHONY J. COPPOLINO
 Deputy Branch Director
 3 PAUL G. FREEBORNE
 Virginia Bar No. 33024
 4 Senior Trial Counsel
 5 KIERAN G. GOSTIN
 Trial Attorney
 6
 Civil Division, Federal Programs Branch
 7 U.S. Department of Justice
 P.O. Box 883
 8 Washington, D.C. 20044
 Telephone: (202) 353-0543
 9 Facsimile: (202) 616-8460
 10 E-mail: paul.freeborne@usdoj.gov

11 *Attorneys for Federal Defendants*

12 **UNITED STATES DISTRICT COURT**
 13 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**

14 WILEY GILL; JAMES PRIGOFF; TARIQ
 15 RAZAK; KHALID IBRAHIM; and AARON
 CONKLIN,

16 Plaintiffs,

17 v.

18 DEPARTMENT OF JUSTICE, *et al.*,

19 Defendants.
20
21

No. 3:14-cv-03120 (RS)

DEFENDANTS' NOTICE OF FILING OF ADMINISTRATIVE RECORD

1 Pursuant to L.R. 16-5 and the Court's Orders, Dkt. Nos. 41 and 49, Defendants have filed
2 a certified administrative record containing non-privileged information considered in the
3 development of the standard for the reporting of suspicious activity, including the behavioral
4 standards pertaining to such reporting, as that standard was developed and revised. Given the
5 size of the record, hard copy binders of the administrative record are being delivered to the
6 Clerk, the Court and opposing counsel (as explained in the certificate of service below), and are
7 not filed on the CM/ECF system.

8 As noted in Defendants' motion to dismiss, *see* Dkt. Nos. 21, 28, Defendants do not
9 believe that the standard challenged is a legislative rule subject to notice and comment
10 rulemaking. Notwithstanding that position, Defendants have compiled a record consistent with
11 the requirements of the Administrative Procedure Act in an effort to facilitate a final resolution
12 of this matter upon summary judgment.

13 The names and personal information of Office of Director of National Intelligence
14 employees and other Federal employees in the intelligence community, names and personal
15 information of law enforcement agency personnel, and the personal information (*e.g.*, e-mail
16 addresses and phone numbers) of third-parties and government employees who are otherwise not
17 included in the two preceding categories are redacted from the administrative record and
18 indicated with the codes 01, 02, and 03, respectively. The redactions are indicated in the index
19 accompanying the certification of the administrative record, attached hereto. Pre-decisional and
20 deliberative information has been excluded or otherwise redacted from the administrative record.
21 *See e.g., San Luis Obispo for Peace v. NRC*, 789 F.2d 26, 44-45 (D.C. Cir. 1986) (*en banc*)
22 (refusing to supplement the administrative record to consider transcripts of deliberative agency
23 proceedings); *Norris & Hirshberg v. SEC*, 163 F.2d 689, 693 (D.C. Cir. 1947) ("internal
24 memoranda made during the decisional process . . . are never included in the record").
25 Deliberative material is redacted from the administrative record with the code 04, and where
26 such redactions are made to the record, those redactions are also indicated in the administrative
27 record index.
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

June 16, 2015

Respectfully submitted,

BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

/s/ Paul G. Freeborne
PAUL G. FREEBORNE
Senior Trial Counsel

KIERAN G. GOSTIN
Trial Attorney

Civil Division, Federal Programs Branch
U.S. Department of Justice
P.O. Box 883
Washington, D.C. 20044
Telephone: (202) 353-0543
Facsimile: (202) 616-8460
E-mail: paul.freeborne@usdoj.gov

Attorneys for Federal Defendants

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

CERTIFICATE OF SERVICE

I hereby certify that on June 16, 2015, I filed the above pleading and its attachments with the Court’s CM/ECF system, which will send notice of such filing to all parties. In addition, I separately caused to be sent by overnight delivery the hard copy of the administrative record to the following:

Stephen Scotch-Marmo
MORGAN, LEWIS & BROCKIUS LLP
101 Park Avenue
New York, NY 100178
Tel: (212) 309-6167

Julia Harumi Mass
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
Tel: (415).621-2493

Date: June 16, 2015

/s/ Paul G. Freeborne
PAUL G. FREEBORNE

Pages ER 380-82 intentionally omitted.

1 BENJAMIN C. MIZER
 Principal Deputy Attorney General
 2 ANTHONY J. COPPOLINO
 Deputy Branch Director
 3 PAUL G. FREEBORNE
 Virginia Bar No. 33024
 4 Senior Trial Counsel
 KIERAN G. GOSTIN
 5 Trial Attorney
 6
 Civil Division, Federal Programs Branch
 7 U.S. Department of Justice
 P.O. Box 883
 8 Washington, D.C. 20044
 Telephone: (202) 353-0543
 9 Facsimile: (202) 616-8460
 10 E-mail: paul.freeborne@usdoj.gov

11 *Attorneys for Federal Defendants*

12 **UNITED STATES DISTRICT COURT**
 13 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**

14 WILEY GILL; JAMES PRIGOFF; TARIQ
 15 RAZAK; KHALID IBRAHIM; and AARON
 CONKLIN,

16 Plaintiffs,

17 v.

18 DEPARTMENT OF JUSTICE, *et al.*,

19 Defendants.
20
21

No. 3:14-cv-03120 (RS)

EXHIBIT A TO CERTIFICATION OF ADMINISTRATIVE RECORD

22
23
24
25
26
27
28

ADMINISTRATIVE RECORD INDEX

	<u>DOCUMENT INFORMATION</u>	<u>BATES NUMBER</u>	<u>REDACTION¹</u>
1			
2			
3	1	White House Memorandum on Guidelines and Requirements in Support of the Information Sharing Environment (December 16, 2005) (wh121605-memo.pdf)	1-5 None
4			
5			
6	2	Guideline 2 – Develop a Common Framework for the Sharing of Information Between and Among Executive Departments and Agencies and State, Local, and Tribal Governments, Law Enforcement Agencies, and the Private Sector (November 24, 2006) (Guideline 2 - common sharing framework.pdf)	6-27 None
7			
8			
9			
10	3	The Information Sharing Environment Suspicious Activity Reporting (SAR) Working Group's Business Process Analysis (February 13, 2007) (SAR_BusinessAnalysis_final20070215.doc)	28-36 None
11			
12			
13	4	Common Terrorism Information Sharing Standards (CTISS) Program Manual, Version 1.0 (October 2007) (CTISS Program Manual 20071031.pdf)	37-66 None
14			
15	5	Information Sharing Environment Administrative Memoranda (ISE-AM) Common Terrorism Information Sharing Standards (CTISS) Program (October 31, 2007) (ise-asm300-ctiss-issuance.pdf)	67-70 None
16			
17			
18	6	PM-ISE Memorandum, Release of the Information Sharing Environment (ISE) Functional Standard for Suspicious Activity Reporting (SAR) Version 1.0 (ISE-FS-200) (January 25, 2008) (Transmittal_Memorandum_ISE-FS-200.pdf)	71-74 None
19			
20			
21	7	Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.0 ISE-FS-200 (January 25, 2008) (Functional Standard_Issuance_Version_1.0_Final_Signed).pdf)	75-106 None
22			
23			
24			
25	8	ISE-SAR Governance Panel June Meeting Agenda	107 01

¹ The nature of each of the redactions is explained in Defendants' Notice of Filing of Administrative Record.

1		(June 17, 2008) (ISE-SAR SC Agenda (06-17-2008).doc)		
2	9	ISE-SAR Steering Committee email, with attachment ISE-SAR Steering Group - Contact List.doc (June 26, 2008) (FW ISE-SAR Steering Committee.msg)	108-110	01, 02 & 03
3				
4	10	ISE-SAR Governance Panel July Meeting Agenda (July 17, 2008) (ISE-SAR SC Agenda (07-17-2008).doc)	111	01
5				
6	11	ISE- SAR Steering Committee September email (August 26, 2008) (FW Next Meeting - Monday September 8.msg), with attachment containing the agenda for the September 2008 meeting (ISE-SAR SC Agenda_2008-09-08.doc)	112-113	01 & 02
7				
8	12	Agenda for a September 2008 Dialogue on Privacy and Civil Liberties outreach meeting agenda hosted by the PM-ISE (August 27, 2008) (PCL Dialogue Agenda 090308.pdf)	114-115	01
9				
10	13	September 2008 PM-ISE hosted Dialogue on Privacy and Civil Liberties outreach meeting attendee list (August 27, 2008) (AttendeeList Sept2008.doc)	116-119	01, 02 & 03
11				
12	14	September 2008 PM-ISE hosted Dialogue on Privacy and Civil Liberties outreach meeting description of meeting purpose and ground rules (August 28, 2008) (Purpose of 9-3_SAR.pdf)	120	None
13				
14	15	Information Sharing Environment – Suspicious Activity Reporting Functional Standard And Evaluation Environment Initial Privacy and Civil Liberties Analysis September 2008—Version 1 (September 2008) (ISE-SAR FS and EE Initial Privacy and Civil Liberties Analysis_090508.pdf)	121-152	None
15				
16	16	Agenda for the ISE-SAR Steering Committee on October 7, 2008 (ISE-SAR SC Agenda_2008-10-07.doc)	153	01
17				
18	17	Email from Michael German (ACLU) providing suspicious activity examples (January 16, 2009), with attachment Suspicious Activity Examples.docx (SAR	154-157	01 & 03
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				

1		meeting.msg)		
2	18	Email from Michael German regarding possible amendments to the ISE-SAR Functional Standard ver. 1.0 (January 23, 2009) (Comments on Functional Standard.msg)	158-160	01 & 03
3				
4	19	Tips and Leads Issue Paper email, with attachment Tips and Leads Issue Paper 10 07.pdf (February 10, 2009) (Tips and Leads Issue Paper.msg)	161-174	01 & 03
5				
6	20	Feedback Session with Privacy and Civil Liberties Advocates: Suspicious Activity Reporting (SAR) Line-Officer Training and the ISE-SAR Functional Standard --Agenda (February 13, 2009) (Agenda February 18, 2009 - SAR Feedback Session.doc)	175	01
7				
8	21	Feedback Session with Privacy and Civil Liberties Advocates: Suspicious Activity Reporting (SAR) Line-Officer Training and the ISE-SAR Functional Standard --Attendee List (February 18, 2009) (Attendee List v3 Feb2009 roundtable.xls)	176-177	01 & 03
9				
10	22	ISE- SAR Steering Committee March meeting email, with attachment ISE-SAR SC Agenda_2009-03-05_v2.doc (February 25, 2009) (FW ISE-SAR Steering Committee Meeting March 5 2009.msg)	178-179	01 & 02
11				
12	23	Email from Mohamed Elibiary regarding feedback (February 26, 2009) (Re follow-up and some heart-felt feedback.msg)	180-182	01 & 03
13				
14	24	Suggestions from Michael German for revision to functional standard email (March 30, 2009) (Re Thanks.msg)	183-184	01, 03 & 04
15				
16	25	ISE- SAR Steering Committee April meeting email, with attachment ISE-SAR SC_Agenda_2009-04-07.doc (April 1, 2009) (FW ISE-SAR Steering Committee Meeting April 7 2009.msg)	185-186	01 & 02
17				
18	26	Memorandum for Release of the Information Sharing Environment (ISE) Functional Standard for Suspicious Activity Reporting, Version 1.5 (May 21, 2009) (ISE-SAR Functional Standard V1.5 Cover	187-188	None
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				

1		Letter.pdf)		
2	27	Fact Sheet: Update to Suspicious Activity Reporting Functional Standard Provides Greater Privacy and Civil Liberties Protections (May 21, 2009) (ISE-SAR_Functional_Standard_V1_5_Fact_Sheet.pdf)	189-191	None
3				
4	28	Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) version 1.5 (May 21, 2009) (ISE-FS-200_ISE-SAR_Functional_Standard_V1.5_Issued.pdf)	192-227	None
5				
6				
7	29	Proposed redlines and feedback provided by Michael German (ACLU) to the PM-ISE on the draft NSI Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations report issued by PM-ISE (May 17, 2010) (NSI_PCRCL_Analysis_05132010_(ver_188)_ACLU R.doc)	228-264	None
8				
9				
10				
11				
12	30	NSI Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations report issued by PM-ISE on privacy compliance outcomes of the ISE SAR Evaluation Environment and providing recommendations for additional privacy protections during nationwide expansion of the NSI (July 2010) (NSI_PCRCL_Analysis_July2010_final.pdf)	265-301	None
13				
14				
15				
16				
17	31	Email regarding meeting between Mike German and the Program Manager on July 18, 2012 (July 9, 2012) (MGerman Scheduling meeting with Kshemendra Paul July2012.msg) and meeting invitation (MGerman PM meeting 7182012.pdf)	302-305	01 & 03
18				
19				
20	32	Email regarding meeting between Lillie Coney (EPIC) and the Program Manager on July 31, 2012 (Meeting between Kshemendra Paul PM-ISE and Lillie Coney (EPIC).msg) and meeting invitation (LConey PM meeting 7312012.pdf)	306-307	01 & 03
21				
22				
23	33	Email regarding meeting between Sharon Bradford Franklin (The Constitution Project) and Program Manager on September 24, 2012 (SBFranklin meet with Kshemendra Paul September 2012.msg) and meeting invitation (SBFranklin PM 09242012)	308-313	01 & 03
24				
25				
26				

1	34	Email regarding meeting between Greg Nojeim (Center for Democracy and Technology) and the Program Manager on October 22, 2012 (GNojeim confirm meeting Kshemendra Paul Oct2012.msg) and meeting invitation (GNojeim PM meeting 10222012.pdf)	314-319	01 & 03
2				
3				
4				
5	35	Email from PM-ISE Executive Secretariat issuing formal invitation to May 30, 2013 ISE Privacy, Civil Rights, and Civil Liberties Roundtable outreach event (May 15, 2013) (PMISE Invitation to Privacy Civil Rights and Civil Liberties Roundtable-Copy.msg)	320	01, 02 & 03
6				
7				
8	36	May 30, 2013 ISE Privacy, Civil Rights, and Civil Liberties Roundtable outreach event final attendee list (May 16, 2013) (May 30th invitees by category 051613.xlsx)	321-325	01 & 02
9				
10				
11	37	Email from PM-ISE Executive Secretariat providing final meeting agenda and read-ahead materials to confirmed attendees for the May 30, 2013 ISE Privacy, Civil Rights, and Civil Liberties Roundtable outreach event (Read aheads May 30 ISE PCRCL Roundtable.msg), including attachments (Agenda ISE PCRCL Roundtable May 30 2013 final.pdf) and (ISE Privacy Roundtable Background and Resources.pdf)	326-329	01, 02 & 03
12				
13				
14				
15				
16	38	Letter addressed to Attorney General Eric Holder, and four other senior government officials, including the Program Manager, ISE, Kshemendra Paul, from the ACLU and 27 signatory advocacy groups requesting reform of the ISE and eGuardian standards (September 9, 2013) (SAR Sign On Letter Final.pdf)	330-335	01
17				
18				
19				
20	39	Email from Program Manager to Vernon Keenan, Chair of the Criminal Intelligence Coordinating Council, and Mike Sena, Chair of the National Fusion Center Association, sharing proposed changes to the ISE-SAR Functional Standard for version 1.5.5 (November 21, 2014) (KP to SLTTs Proposed final ISE-SAR Functional Standard version 1.5.5.msg), including attachments (FS v1_5_5 Executive Summary PM_ISE_QC_112114 Comprehensive Update.docx; and ISE SAR FS 1 5 5 PM_ISE QC	336-405	01, 02 & 03
21				
22				
23				
24				
25				
26				

1		Final DRAFT Clean 112114.doc)		
2	40	ISE-SAR Functional Standard Version 1.5.5 Executive Summary (February 17, 2015) (FS v1_5_5 Executive Summary PM_ISE 21715 Comprehensive)	406-413	None
3				
4	41	Final and signed version of the ISE-SAR Functional Standard version 1.5.5 issued by the PM-ISE. (February 23, 2015) (SAR_FS_1.5.5_IssuedFeb2015.pdf)	414-473	None
5				
6				
7	42	Screenshot of ISE.gov blog post of the Program Manager announcing the issuance of ISE-SAR Functional Standard version 1.5.5. This blog post serves as the transmittal memorandum for the ISE- SAR Functional Standard v. 1.5.5. (March 2, 2015) (ISE_gov FS v1_5_5 blog 2March2015.jpg)	474	None
8				
9				
10				

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



the
White House
President George W. Bush

For Immediate Release
Office of the Press Secretary
December 16, 2005

Memorandum for the Heads of Executive Departments and Agencies

SUBJECT: Guidelines and Requirements in Support of the Information Sharing Environment

Ensuring the appropriate access to, and the sharing, integration, and use of, information by Federal, State, local, and tribal agencies with counterterrorism responsibilities, and, as appropriate, private sector entities, while protecting the information privacy and other legal rights of Americans, remains a high priority for the United States and a necessity for winning the war on terror. Consistent with section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108 458) (IRTPA), my Administration is working to create an Information Sharing Environment (ISE) to facilitate the sharing of terrorism information (as defined in Executive Order 13388 of October 25, 2005).

Section 1016 of IRTPA supplements section 892 of the Homeland Security Act of 2002 (Public Law 107 296), Executive Order 13311 of July 29, 2003, and other Presidential guidance, which address various aspects of information access. On April 15, 2005, consistent with section 1016(f) of IRTPA, I designated the program manager (PM) responsible for information sharing across the Federal Government. On June 2, 2005, my memorandum entitled "Strengthening Information Sharing, Access, and Integration - Organizational, Management, and Policy Development Structures for Creating the Terrorism Information Sharing Environment" directed that the PM and his office be part of the Office of the Director of National Intelligence (DNI), and that the DNI exercise authority, direction, and control over the PM and ensure that the PM carries out his responsibilities under IRTPA. On October 25, 2005, I issued Executive Order 13388 to facilitate the work of the PM and the expeditious establishment of the ISE and restructure the Information Sharing Council (ISC), which provides advice concerning and assists in the establishment, implementation, and maintenance of the ISE.

On June 2, 2005, I also established the Information Sharing Policy Coordination Committee (ISPCC), which is chaired jointly by the Homeland Security Council (HSC) and the National Security Council (NSC), and which has the responsibilities set forth in section D of Homeland Security Presidential Directive 1 and other relevant presidential guidance with respect to information sharing. The ISPCC is the main day-to-day forum for interagency coordination of information sharing policy, including the resolution of issues raised by the PM, and provides policy analysis and recommendations for consideration by the more senior committees of the HSC and NSC systems and ensures timely responses.

Section 1016(d) of IRTPA calls for leveraging all ongoing efforts consistent with establishing the ISE, the issuance of guidelines for acquiring, accessing, sharing, and using information in support of the ISE and for protecting privacy and civil liberties in the development of the ISE, and the promotion of a culture of information sharing. Consistent with the Constitution and the laws of the United States, including section 103 of the National Security Act of 1947, as amended, and sections 1016 and 1018 of IRTPA, I hereby direct as follows:

1. Leveraging Ongoing Information Sharing Efforts in the Development of the ISE. The ISE shall build upon existing Federal Government policies, standards, procedures, programs, systems, and architectures (collectively "resources") used for the sharing and integration of and access to terrorism information, and shall leverage those resources to the maximum extent practicable, with the objective of establishing a decentralized, comprehensive, and coordinated environment for the sharing and integration of such information.

- a. The DNI shall direct the PM to conduct and complete, within 90 days after the date of this memorandum, in consultation with the ISC, a comprehensive evaluation of existing resources pertaining to terrorism information sharing employed by individual or multiple executive departments and agencies. Such evaluation shall assess such resources for their utility and integrative potential in furtherance of the establishment of the ISE and shall identify any unnecessary redundancies.

b. To ensure that the ISE supports the needs of executive departments and agencies with counterterrorism responsibilities, and consistent with section 1021 of IRTPA, the DNI shall direct the PM, jointly with the Director of the National Counterterrorism Center (NCTC), and in coordination with the heads of relevant executive departments and agencies, to review and identify the respective missions, roles, and responsibilities of such executive departments and agencies, both as producers and users of terrorism information, relating to the acquisition, access, retention, production, use, management, and sharing of terrorism information. The findings shall be reviewed through the interagency policy coordination process, and any recommendations for the further definition, reconciliation, or alteration of such missions, roles, and responsibilities shall be submitted, within 180 days after the date of this memorandum, by the DNI to the President for approval through the Assistant to the President for Homeland Security and Counterterrorism (APHS-CT) and the Assistant to the President for National Security Affairs (APNSA). This effort shall be coordinated as appropriate with the tasks assigned under the Guidelines set forth in section 2 of this memorandum.

c. Upon the submission of findings as directed in the preceding paragraph (1(b)), the DNI shall direct the PM, in consultation with the ISC, to develop, in a manner consistent with applicable law, the policies, procedures, and architectures needed to create the ISE, which shall support the counterterrorism missions, roles, and responsibilities of executive departments and agencies. These policies, procedures, and architectures shall be reviewed through the interagency policy coordination process, and shall be submitted, within 180 days after the submission of findings as directed in the preceding paragraph (1(b)), by the DNI to the President for approval through the APHS-CT and the APNSA.

2. Information Sharing Guidelines. Consistent with section 1016(d) of IRTPA, I hereby issue the following guidelines and related requirements, the implementation of which shall be conducted in consultation with, and with support from, the PM as directed by the DNI:

a. Guideline 1 - Define Common Standards for How Information is Acquired, Accessed, Shared, and Used Within the ISE

The ISE must, to the extent possible, be supported by common standards that maximize the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE consistent with the protection of intelligence, law enforcement, protective, and military sources, methods, and activities.

Consistent with Executive Order 13388 and IRTPA, the DNI, in coordination with the Secretaries of State, Defense, and Homeland Security, and the Attorney General, shall develop and issue, within 90 days after the date of this memorandum, common standards (i) for preparing terrorism information for maximum distribution and access, (ii) to enable the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE while safeguarding such information and protecting sources and methods from unauthorized use or disclosure, (iii) for implementing legal requirements relating to the handling of specific types of information, and (iv) that include the appropriate method for the Government-wide adoption and implementation of such standards. Such standards shall accommodate and reflect the sharing of terrorism information, as appropriate, with State, local, and tribal governments, law enforcement agencies, and the private sector. Within 90 days after the issuance of such standards, the Secretary of Homeland Security and the Attorney General shall jointly disseminate such standards for use by State, local, and tribal governments, law enforcement agencies, and the private sector, on a mandatory basis where possible and a voluntary basis where not. The DNI may amend the common standards from time to time as appropriate through the same process by which the DNI issued them.

b. Guideline 2 - Develop a Common Framework for the Sharing of Information Between and Among Executive Departments and Agencies and State, Local, and Tribal Governments, Law Enforcement Agencies, and the Private Sector

Recognizing that the war on terror must be a national effort, State, local, and tribal governments, law enforcement agencies, and the private sector must have the opportunity to participate as full partners in the ISE, to the extent consistent with applicable laws and executive orders and directives, the protection of national security, and the protection of the information privacy rights and other legal rights of Americans.

Within 180 days after the date of this memorandum, the Secretary of Homeland Security and the Attorney

General, in consultation with the Secretaries of State, Defense, and Health and Human Services, and the DNI, and consistent with the findings of the counterterrorism missions, roles, and responsibilities review under section 1 of this memorandum, shall:

(i) perform a comprehensive review of the authorities and responsibilities of executive departments and agencies regarding information sharing with State, local, and tribal governments, law enforcement agencies, and the private sector; and

(ii) submit to the President for approval, through the APHS-CT and the APNSA, a recommended framework to govern the roles and responsibilities of executive departments and agencies pertaining to the acquisition, access, retention, production, use, management, and sharing of homeland security information, law enforcement information, and terrorism information between and among such departments and agencies and State, local, and tribal governments, law enforcement agencies, and private sector entities.

c. Guideline 3 - Standardize Procedures for Sensitive But Unclassified Information

To promote and enhance the effective and efficient acquisition, access, retention, production, use, management, and sharing of Sensitive But Unclassified (SBU) information, including homeland security information, law enforcement information, and terrorism information, procedures and standards for designating, marking, and handling SBU information (collectively "SBU procedures") must be standardized across the Federal Government. SBU procedures must promote appropriate and consistent safeguarding of the information and must be appropriately shared with, and accommodate and reflect the imperative for timely and accurate dissemination of terrorism information to, State, local, and tribal governments, law enforcement agencies, and private sector entities. This effort must be consistent with Executive Orders [13311](#) and [13388](#), section 892 of the Homeland Security Act of 2002, section 1016 of IRTPA, section 102A of the National Security Act of 1947, the Freedom of Information Act, the Privacy Act of 1974, and other applicable laws and executive orders and directives.

(i) Within 90 days after the date of this memorandum, each executive department and agency will conduct an inventory of its SBU procedures, determine the underlying authority for each entry in the inventory, and provide an assessment of the effectiveness of its existing SBU procedures. The results of each inventory shall be reported to the DNI, who shall provide the compiled results to the Secretary of Homeland Security and the Attorney General.

(ii) Within 90 days after receiving the compiled results of the inventories required under the preceding paragraph (i), the Secretary of Homeland Security and the Attorney General, in coordination with the Secretaries of State, Defense, and Energy, and the DNI, shall submit to the President for approval recommendations for the standardization of SBU procedures for homeland security information, law enforcement information, and terrorism information in the manner described in paragraph (iv) below.

(iii) Within 1 year after the date of this memorandum, the DNI, in coordination with the Secretaries of State, the Treasury, Defense, Commerce, Energy, Homeland Security, Health and Human Services, and the Attorney General, and in consultation with all other heads of relevant executive departments and agencies, shall submit to the President for approval recommendations for the standardization of SBU procedures for all types of information not addressed by the preceding paragraph (ii) in the manner described in paragraph (iv) below.

(iv) All recommendations required to be submitted to the President under this Guideline shall be submitted through the Director of the Office of Management and Budget (OMB), the APHS-CT, and the APNSA, as a report that contains the following:

(A) recommendations for government-wide policies and procedures to standardize SBU procedures;

(B) recommendations, as appropriate, for legislative, policy, regulatory, and administrative changes; and

(C) an assessment by each department and agency participating in the SBU procedures

Case 3:14-cv-03120-RS Document 53 Filed 06/17/15 Page 5 of 75

review process of the costs and budgetary considerations for all proposed changes to marking conventions, handling caveats, and other procedures pertaining to SBU information.

(v) Upon the approval by the President of the recommendations submitted under this Guideline, heads of executive departments and agencies shall ensure on an ongoing basis that such recommendations are fully implemented in such department or agency, as applicable. The DNI shall direct the PM to support executive departments and agencies in such implementation, as well as in the development of relevant guidance and training programs for the standardized SBU procedures.

d. Guideline 4 - Facilitate Information Sharing Between Executive Departments and Agencies and Foreign Partners

The ISE must support and facilitate appropriate terrorism information sharing between executive departments and agencies and foreign partners and allies. To that end, policies and procedures to facilitate such informational access and exchange, including those relating to the handling of information received from foreign governments, must be established consistent with applicable laws and executive orders and directives.

Within 180 days after the date of this memorandum, the Secretary of State, in coordination with the Secretaries of Defense, the Treasury, Commerce, and Homeland Security, the Attorney General, and the DNI, shall review existing authorities and submit to the President for approval, through the APHS-CT and the APNSA, recommendations for appropriate legislative, administrative, and policy changes to facilitate the sharing of terrorism information with foreign partners and allies, except for those activities conducted pursuant to sections 102A(k), 104A(f), and 119(f)(1)(E) of the National Security Act of 1947.

e. Guideline 5 - Protect the Information Privacy Rights and Other Legal Rights of Americans

As recognized in Executive Order 13353 of August 27, 2004, the Federal Government has a solemn obligation, and must continue fully, to protect the legal rights of all Americans in the effective performance of national security and homeland security functions. Accordingly, in the development and use of the ISE, the information privacy rights and other legal rights of Americans must be protected.

(i) Within 180 days after the date of this memorandum, the Attorney General and the DNI, in coordination with the heads of executive departments and agencies that possess or use intelligence or terrorism information, shall (A) conduct a review of current executive department and agency information sharing policies and procedures regarding the protection of information privacy and other legal rights of Americans, (B) develop guidelines designed to be implemented by executive departments and agencies to ensure that the information privacy and other legal rights of Americans are protected in the development and use of the ISE, including in the acquisition, access, use, and storage of personally identifiable information, and (C) submit such guidelines to the President for approval through the Director of OMB, the APHS-CT, and the APNSA. Such guidelines shall not be inconsistent with Executive Order 12333 and guidance issued pursuant to that order.

(ii) Each head of an executive department or agency that possesses or uses intelligence or terrorism information shall ensure on an ongoing basis that (A) appropriate personnel, structures, training, and technologies are in place to ensure that terrorism information is shared in a manner that protects the information privacy and other legal rights of Americans, and (B) upon approval by the President of the guidelines developed under the preceding subsection (i), such guidelines are fully implemented in such department or agency.

3. Promoting a Culture of Information Sharing. Heads of executive departments and agencies must actively work to create a culture of information sharing within their respective departments or agencies by assigning personnel and dedicating resources to terrorism information sharing, by reducing disincentives to such sharing, and by holding their senior managers and officials accountable for improved and increased sharing of such information.

Accordingly, each head of an executive department or agency that possesses or uses intelligence or terrorism information shall:

- a. within 90 days after the date of this memorandum, designate a senior official who possesses knowledge of the operational and policy aspects of information sharing to (i) provide accountability and oversight for terrorism information sharing within such department and agency, (ii) work with the PM, in consultation with the ISC, to develop high level information sharing performance measures for the department or agency to be assessed no less than semiannually, and (iii) provide, through the department or agency head, an annual report to the DNI on best practices of and remaining barriers to optimal terrorism information sharing;
 - b. within 180 days after the date of this memorandum, develop and issue guidelines, provide training and incentives, and hold relevant personnel accountable for the improved and increased sharing of terrorism information. Such guidelines and training shall seek to reduce obstructions to sharing, consistent with applicable laws and regulations. Accountability efforts shall include the requirement to add a performance evaluation element on information sharing to employees' annual Performance Appraisal Review, as appropriate, and shall focus on the sharing of information that supports the mission of the recipient of the information; and
 - c. bring to the attention of the Attorney General and the DNI, on an ongoing basis, any restriction contained in a rule, regulation, executive order or directive that significantly impedes the sharing of terrorism information and that such department or agency head believes is not required by applicable laws or to protect the information privacy rights and other legal rights of Americans. The Attorney General and the DNI shall review such restriction and jointly submit any recommendations for changes to such restriction to the APHS-CT and the APNSA for further review.
4. Heads of executive departments and agencies shall, to the extent permitted by law and subject to the availability of appropriations, provide assistance and information to the DNI and the PM in the implementation of this memorandum.
5. This memorandum:
- a. shall be implemented in a manner consistent with applicable laws, including Federal laws protecting the information privacy rights and other legal rights of Americans, and subject to the availability of appropriations;
 - b. shall be implemented in a manner consistent with the statutory authority of the principal officers of executive departments and agencies as heads of their respective departments or agencies;
 - c. shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budget, administrative, and legislative proposals; and
 - d. is intended only to improve the internal management of the Federal Government and is not intended to, and does not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its departments, agencies, or entities, its officers, employees, or agencies, or any other person.

GEORGE W. BUSH

###

Source: [The White House](#)

The Information Sharing Environment
Suspicious Activity Reporting (SAR) Working Group's
Business Process Analysis

February 13, 2007

Background & Scope:

In November 2006, the Program Manager for the Information Sharing Environment (ISE), in consultation with the Information Sharing Council, established a Suspicious Activity Reporting (SAR) Working Group to review current SAR processes, identify issues and impediments, and develop a common framework for improving the development, distribution, and access of terrorism suspicious activity reports across the ISE. Leveraging previous efforts by an NCTC-led interagency group, the ISE SAR Working Group (SAR WG), which includes over 40 subject matter experts from more than 14 Federal and State organizations, met regularly through November and December to gain a baseline understanding of current SAR processes across ISE organizations, and to develop a path forward toward establishing a common ISE SAR Framework. A complete listing of the organizations represented on the SAR WG is provided in Attachment 1.

Bounding the Issue

Suspicious activity was previously defined by the NCTC-led interagency group as “behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, espionage, or other illicit intention.” Such activities could include, but are not limited to, surveillance, photography of facilities, site breach or physical intrusion, cyber attacks, possible testing of security or security response, indications of unusual public health sector activity, unauthorized attempts to obtain precursor chemicals/agents or toxic materials, or other unusual behavior or sector-specific incidents. Suspicious activity reporting document the observation of such activities, and are currently collected at all levels of Federal, State, Local, Tribal and Foreign Governments, as well as within the Private Sector.

The challenge for the SAR WG was to define the ISE-specific “framework” by which Suspicious Activity Reports that contain potential terrorism-related information can be made available to the diverse pool of relevant customers – ranging from the Intelligence, Law Enforcement, Diplomatic, Homeland Security and Defense Communities to State, Local, Tribal, Foreign Government and Private Sector entities – that require the information to assess, deter, protect, prevent or prosecute those planning terrorist activities. For the purpose of this effort, the SAR WG came to an agreement that the SAR process would be bounded at the front end with observation of a suspicious activity, and the process would be considered complete when data associated with potential terrorist precursor activity is available for retrieval by the ISE participants with requisite need. Process analysis also would be limited to the content and movement of data from the agency in which it was created to point where it is available to the consumer of the information. (Subsequent processes which utilize the shared data are viewed as separate processes and were not reviewed as part of this exercise.) Of note, the SAR WG also

reflective of purely criminal activity, malicious or juvenile delinquency, or random actions, in addition to terrorism-related information).

For the SAR Information Acquisition business process, the SAR WG concluded that the focus for the ISE should not be to attempt to standardize all aspects of the various agency-specific processes. Instead, the ISE focus should be centered on ensuring that specific information or “data elements” that are needed collectively by the ISE are obtained, reflected through an organization’s process whenever possible, and shared appropriately. To this end, the SAR WG developed and defined an initial common list of desired data elements (provided in Attachment 2).

II. Organizational Processing: Each contributing organization has its own process or processes to review and validate SAR information. For example, in some cases, information is reviewed by a supervisor and/or other subject matter expert before being advanced; in other agencies, a quality assurance review is also required. As in the Information Acquisition process noted above, the SAR WG concluded that the majority of the processes in the Organizational Processing category are, again, agency specific – constructed to support agency missions to include, but not limited to, terrorism. While certain of these processes will need to conform to address overall ISE standards, the SAR WG determined that the primary focus of the ISE in this business process category is to establish common criteria to ensure potential terrorism-related SAR information is placed into the ISE.

The SAR WG wrestled with the challenge of encouraging maximum reporting of potential terrorism-related SAR information while minimizing unrelated reports, but in the end developed an initial set of criteria – including screening categories and activity descriptions – that identify an event as potentially terrorism-related. (The initial set of criteria is provided in Attachment 3.) It is also expected that this process will include cross-organizational coordination.

III. Integration/Consolidation: The SAR WG agreed that once SAR information has been identified as potentially terrorism-related, using the criteria in Attachment 3, the organization would then make that information, specifically the “data elements,” available to the broader ISE membership.

Of note, the SAR WG began an initial examination of potential constraints, considerations, policies and issues related to the release, control, handling and management of SAR information. This included consideration of the legal (i.e., U.S. persons, retention, Privacy Act and Freedom of Information Act), regulatory, and agreement-based considerations and constraints affecting the Law Enforcement (National, State, local, etc) and Intelligence Communities. The SAR WG identified a number of challenges and issues that will need to be further addressed, including:

- Potential caveats, constraints and/or expiration dates on the sharing and handling of specific types of information;
- Potential agency specific dissemination and handling requirements;
- Potential end-use constraints and deconfliction mechanisms;
- Ensuring conformity regarding all agency inputs/data availability.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
PROGRAM MANAGER, INFORMATION SHARING ENVIRONMENT
WASHINGTON, DC 20511

January 25, 2008

MEMORANDUM FOR HEADS OF DEPARTMENTS AND AGENCIES

SUBJECT: Release of the Information Sharing Environment (ISE) Functional Standard for Suspicious Activity Reporting (SAR) Version 1.0 (ISE-FS-200)

REFERENCE: 1) Presidential Memorandum of December 16, 2005, subject: Guidelines and Requirement in Support of the Information Sharing Environment
2) National Strategy for Information Sharing, October 2007

In fall 2005, the White House Counterterrorism (CT) Security Group (CSG) tasked the National Counterterrorism Center (NCTC) to coordinate with the CT community to examine options for improving the value of suspicious activity reporting (SAR) to the counterterrorism mission. In September 2006, the CSG requested the Program Manager for the Information Sharing Environment (PM-ISE) to build on this work and incorporate it into ISE implementation planning activities. In response, one of the first priority activities with the interagency was to establish a terrorism-related SAR standard for government-wide use to ensure compliance with the ISE. The attached ISE-SAR Functional Standard Version 1.0 (ISE-FS-200) serves as the initial functional standard for the ISE.

This initial functional standard is the first Common Terrorism Information Sharing Standard (CTISS) issued by the PM-ISE, in accordance with the President's Guidelines^{*} directing the development and issuance of common standards governing how terrorism information is acquired, accessed, shared, and used within the ISE. All CTISS, to include the ISE-SAR Functional Standard, will be implemented by ISE participants into supporting infrastructures in accordance with the ISE Enterprise Architecture Framework. This ISE-SAR Functional Standard is also in alignment with the President's October 2007 National Strategy for Information Sharing (NSIS), which outlines Federal, State, local, and tribal responsibilities for sharing ISE-SAR data.

The ISE-SAR Functional Standard is based on documented information sharing exchanges and business requirements, and describes the structure, content, and products associated with processing, integrating, and retrieving ISE-SAR by ISE participants. Each Information Sharing Council (ISC) member and other affected agencies responsible for the collection and processing of SARs with a nexus to terrorism must apply this functional standard when processing, integrating, and retrieving ISE-SAR, and incorporate this functional standard

President's Memorandum dated December 16, 2005 <http://www.whitehouse.gov/news/releases/2005/12/20051216-1Q.html>

into their business processes development and information resource planning. In particular, ISC agencies should, as appropriate, incorporate this ISE-SAR Functional Standard and any subsequent implementation guidance into budgetary planning activities associated with current (operational) and future development efforts associated with relevant mission-specific programs, systems, or initiatives. As appropriate, Departments and Agencies may consider utilizing this standard as part of the grant application process.

This initial version of the functional standard will continue to be tested and evaluated by the user community. Any resulting refinements, including changes to SAR business processes and data elements, will be incorporated in future versions. Privacy assessments will also be performed as appropriate to identify privacy issues that may arise in implementing the proposed ISE-SAR Functional Standard and information flow.

The ISE-SAR Functional Standard is not intended to address all the implementation issues associated with the reporting, tracking, processing, accessing, storage, and retrieval of SAR information within the ISE. These additional details and business rules will be informed by further testing and evaluation, and addressed in future implementation guidance, as necessary. The purpose of this functional standard is to describe the structure, content, and products associated with processing, integrating, and retrieving ISE-SAR by ISE participants.

The PM-ISE SAR initiative includes several ISE-SAR-related efforts to ensure alignment with department and agency business processes, policy, programming and performance, as well as technology development and deployment activities. This ISE-SAR Functional Standard is one component of the overall ISE-SAR initiative. Other ISE-SAR initiatives are described in Attachment C.

Please address any questions associated with the ISE-SAR Functional Standard to your designated ISC Representative (Attachment B) or the office of the Program Manager.



Thomas E. McNamara

Attachments:

- A. Information Sharing Environment (ISE) Functional Standard (FS) for Suspicious Activity Reporting (SAR) Version 1.0 (ISE-FS-200)
- B. Information Sharing Council Members
- C. ISE-SAR Initiatives

cc: Information Sharing Council

Attachment B - ISC Council Members

Department of State	Mr. Lee Lohman
Department of the Treasury	Mr. Michael Duffy
Department of Defense	Ms. Debra Filippi
The Attorney General	Mr. Vance Hitch
Department of the Interior	Ms. Kim Thorsen
Department of Commerce	Ms. Suzanne Hilding
Department of Health And Human Services	RADM Arthur Lawrence
Department of Transportation	Mr. Lawrence Hopkins
Department of Energy	Mr. Jay Tilden
Department of Homeland Security	Mr. Carter Morris
Director of National Intelligence	Mr. Michael Johnson

Attachment C - ISE SAR Initiatives

FY 2009 OMB Passback language tasks ISC departments and agencies to develop and make available an inventory of programs and systems to create or maintain suspicious activity reports. The definitions in this functional standard will assist Departments and Agencies to identify the information required by OMB.

The ISE Implementation Plan introduced the concept of information sharing evaluation environments as a cost effective approach for identifying requirements for ISE policies, business processes, capabilities, and standards, and as platforms to demonstrate and evaluate solutions to operational needs in a relatively controlled environment. PM-ISE is facilitating the operation of one or more Federal/State/local ISE-SAR evaluation environments through a collaborative effort between DoD, DHS, and DOJ/FBI. The evaluation period is expected to be completed by October 2008. An important purpose of the evaluation environment is to test the ISE-SAR Functional Standard in an operational environment and to identify any refinements or changes to the SAR business process and data elements that may be necessary. In addition, a privacy assessment will be performed in the operational environment to identify privacy issues that may arise in implementing the initial ISE-SAR Functional Standard and information flow.

PM-ISE, in consultation with the Information Sharing Council, is executing an ISE Performance Management Program with related SAR performance measures. The SAR performance measures and results to date will be incorporated into the June 2008 Annual Report to the Congress on the Information Sharing Environment. The PM-ISE, in consultation with the ISC, is working to refine these measures over the coming months.

PM-ISE is developing FY2010-2014 ISE programmatic guidance for Departments and Agencies that will include SAR.

ISE SAR implementation issues associated with the reporting, tracking, processing, access, storage, retrieval of information, and governance of these activities within the ISE will be documented further, as necessary.

INFORMATION SHARING ENVIRONMENT (ISE)**FUNCTIONAL STANDARD (FS)****SUSPICIOUS ACTIVITY REPORTING (SAR)****VERSION 1.0**

1. Authority. The National Security Act of 1947, as amended; The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended; Presidential Memorandum dated April 10, 2007 (Assignment of Functions Relating to the Information Sharing Environment); Presidential Memorandum dated December 16, 2005 (Guidelines and Requirements in Support of the Information Sharing Environment); DNI memorandum dated May 2, 2007 (Program Manager's Responsibilities); Executive Order 13388; and other applicable provisions of law.
2. Purpose. This issuance serves as the initial functional standard for ISE-SARs, and constitutes the first of the *Common Terrorism Information Sharing Standards (CTISS)* issued by the PM-ISE.
3. Applicability. This ISE-FS applies to all departments or agencies that possess or use terrorism or homeland security information, operate systems that support or interface with the ISE, or otherwise participate (or expect to participate) in the ISE, consistent with Section 1016(i) of the IRTPA.
4. References. *ISE Implementation Plan*, November 2006; *ISE Enterprise Architecture Framework (EAF)*, August 2007; *Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment*, Version 1.0; *ISE-AM-300: Common Terrorism Information Standards Program*, 31 October 2007; *Common Terrorism Information Sharing Standards Program Manual*, Version 1.0, October 2007; National Information Exchange Model, *Concept of Operations*, Version 0.5, January 9, 2007; 28 Code of Federal Regulations (CFR) Part 23.
5. Definitions.
 - a. *Artifact*: Detailed mission product documentation addressing information exchanges and data elements for SAR (data models, schemas, structures, etc.).
 - b. *Common Terrorism Information Sharing Standards (CTISS)*: Business process-driven, performance-based "common standards" for preparing terrorism information for maximum distribution and access, to enable the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE. Two categories of common standards are formally identified under CTISS: functional standards and technical standards. Functional standards set forth rules, conditions, guidelines, and characteristics of data and mission products supporting ISE business process areas.

Technical standards document specific technical methodologies and practices to design and implement information sharing capability into ISE systems. CTISS, such as ISE-SAR, are implemented in ISE participant infrastructures that include ISE Shared Spaces as described in the ISE EAF.

- c. *Information Exchange*: The transfer of information from one organization to another organization, in accordance with CTISS processes.
- d. *ISE-Suspicious Activity Report (ISE-SAR)*: An ISE-SAR is a SAR (as defined below in 5g) that has been determined, pursuant to a two-part process, to have a potential terrorism nexus. ISE-SAR business rules will serve as a unified process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.
- e. *National Information Exchange Model (NIEM)*: A joint technical and functional standards program initiated by the Department of Homeland Security (DHS) and the Department of Justice (DOJ) that supports national-level interoperable information sharing.
- f. *Privacy Field*: A data element that may be used to identify an individual and, therefore, may be subject to privacy protection.
- g. *Suspicious Activity Report*: Official documentation of observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention.
- h. *Universal Core (UCore)*: A joint technical standard that defines a small set of context-free data elements for loosely-coupled information sharing at the national level.

6. Guidance. This functional standard is hereby established as the initial functional standard for ISE-SARs. It is based on documented information exchanges and business requirements, and describes the structure, content, and products associated with processing, integrating, and retrieving ISE-SARs by ISE participants.

7. Responsibilities.

- a. The PM-ISE, in consultation with the Information Sharing Council (ISC), will:
 - (1) Maintain and administer this ISE-SAR Functional Standard, to include:
 - (a) Updating the business process and information flows for ISE-SAR.
 - (b) Updating data elements and product definitions for ISE-SAR.
 - (2) Publish and maintain configuration management of this ISE-SAR Functional Standard.

- (3) Assist with the development of ISE-SAR implementation guidance and governance structure, as appropriate, to address privacy, policy, architecture, and legal issues.
 - (4) Work with ISE participants, through the CTISS Committee, to develop a new or modified ISE-SAR Functional Standard, as needed.
 - (5) Coordinate, publish, and monitor implementation and use of this functional standard, and coordinate with the White House Office of Science and Technology Policy and with the National Institute of Standards and Technology (in the Department of Commerce) for broader publication, as appropriate.
- b. Each ISC member and other affected department or agency shall:
- (1) Propose updates to the PM-ISE for this functional standard, as appropriate.
 - (2) As appropriate, incorporate this ISE-SAR Functional Standard, and any subsequent implementation guidance, into budget activities associated with relevant current (operational) mission specific programs, systems, or initiatives (e.g. operations and maintenance {O&M} or enhancements).
 - (3) As appropriate, incorporate this ISE-SAR Functional Standard, and any subsequent implementation guidance, into budget activities associated with future or new development efforts for relevant mission specific programs, systems, or initiatives (e.g. development, modernization, or enhancement {DME}).
 - (4) Ensure incorporation of this ISE-SAR Functional Standard, as set forth in 7b(2) or 7b(3) above, is done in compliance with ISE Privacy Guidelines and any additional guidance provided by the ISE Privacy Guidelines Committee.
8. Effective Date and Expiration. This ISE-FS is effective immediately and will remain in effect as the initial functional standard for ISE-SAR until updated, superseded, or cancelled.



Program Manager for the
Information Sharing Environment

Date: *January 25, 2008*

This page intentionally blank.

PART A – ISE-SAR FUNCTIONAL STANDARD ELEMENTS

SECTION I – DOCUMENT OVERVIEW

A. List of ISE-SAR Information Exchange Artifacts

The full ISE-SAR information exchange contains four types of supporting artifacts. This documentation provides details of implementation processes and other relevant reference materials. A synopsis of the functional standard artifacts is contained in Table 1 below.

Table 1 – Functional Standard Artifacts¹

Artifact Type	Artifact	Artifact Description
Development and Implementation Tools	1. Component Mapping Template (CMT) (SAR-to-NIEM/UCore)	This spreadsheet captures the ISE-SAR information exchange class and data element (source) definitions and relates each data element to corresponding National Information Exchange Model (NIEM) Extensible Mark-Up Language (XML) elements and UCore elements, as appropriate.
	2. NIEM Wantlist	The Wantlist is an XML file that lists the elements selected from the NIEM data model for inclusion in the Schema Subset. The Schema Subset is a compliant version to both programs that has been reduced to only those elements actually used in the ISE-SAR document schema.
	3. XML Schemas	The XML schema provides a technical representation of the business data requirements. They are a machine readable definition of the structure of an ISE-SAR-based XML Message.
	4. XML Sample Instance	The XML Sample Instance is a sample document that has been formatted to comply with the structures defined in the XML Schema. It provides the developer with an example of how the ISE-SAR schema is intended to be used.

¹ Development and implementation tools may be accessible through www.ise.gov. Additionally, updated versions of this functional standard will incorporate the CTISS Universal Core which harmonizes the NIEM Universal Core with the DoD/IC UCore.

SECTION II – SUSPICIOUS ACTIVITY REPORTING EXCHANGES

A. ISE-SAR Purpose

This ISE-SAR Functional Standard is designed to support the sharing of suspicious activity, incident, or behavior (hereafter referred to as activity) information that has a potential terrorism nexus throughout the Information Sharing Environment (ISE) and between State and major urban area fusion centers and their law enforcement,² homeland security,³ or other information sharing partners at the Federal, State, local, and tribal levels to the full extent permitted by law. ISE-SARs will provide for the discovery of patterns, trends, or nationally suspicious activities beyond what would be recognized within a single jurisdiction, state, or territory. Standardized and consistent sharing of suspicious activity information with the State and major urban area fusion centers is deemed vital to assessing, deterring, preventing, or prosecuting those planning terrorist activities. This ISE-SAR Functional Standard has been designed to incorporate key elements for terrorist related activities and may be potentially leveraged by other communities for other crimes.

B. ISE-SAR Scope

Suspicious activity is defined as “*observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention.*” An ISE-SAR requires a two-part process to determine that a SAR has a potential terrorism nexus. Some examples of the criteria for identifying SAR as having a potential terrorism nexus are listed below, but a more comprehensive list can be found in Part B (ISE-SAR Criteria Guidance).

- Surveillance
- Photography of facilities
- Site breach or physical intrusion
- Cyber attacks
- Probing of security

It is also important to acknowledge that many terrorist activities are now being funded via local or regional crimes organizations. This places law enforcement and homeland security professionals in the unique, yet demanding, position of identifying suspicious activities, behavior, or materials as a byproduct or secondary element to a criminal enforcement or investigation activity. This means that, while some ISE-SARs may document activities or incidents to which local agencies have already responded, they are being shared to facilitate aggregate trending or analysis.

² All references to Federal, State, local and tribal law enforcement are intended to encompass civilian law enforcement, military police, and other security professionals.

³ All references to homeland security are intended to encompass public safety, emergency management, and other officials who routinely participate in the State or major urban area's homeland security preparedness activities.

The Suspicious Activity Reports are not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities. The ISE-SAR effort offers a standardized means for feeding information repositories and data analysis tools. Any patterns identified during ISE-SAR data analysis may be investigated in cooperation with the reporting agency or the State or major urban area fusion center.

C. ISE-SAR Top-level Business Processes & Activities

Beginning with the observation and documentation of a suspicious activity, there are five necessary top-level processes—some of which are primarily organizational specific and others with broader implications for the ISE—that together comprise the ISE Suspicious Activity Reporting Process. These processes have been categorized as listed below and are graphically depicted in Figure 1.

1. Information acquisition
2. Organizational processing
3. Integration/consolidation
4. Data retrieval/distribution
5. Feedback

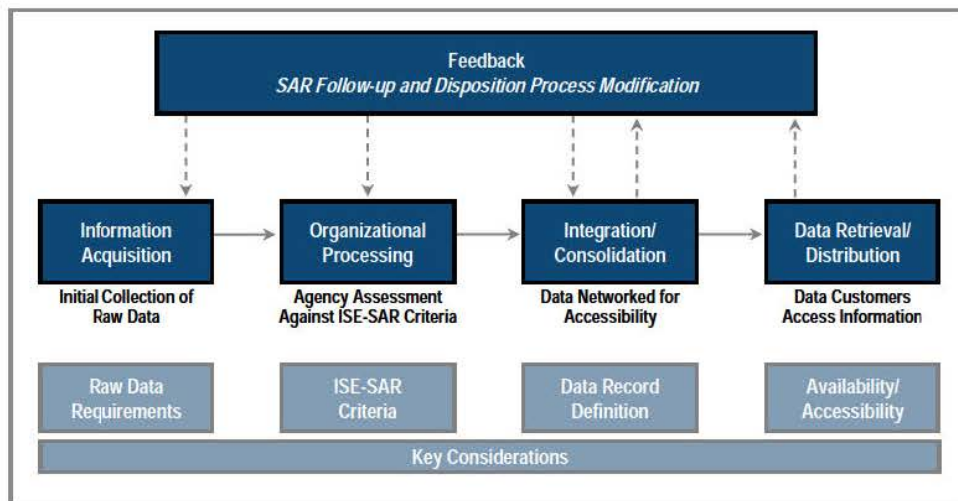


Figure 1 – ISE-SAR Top-level Process

1. Information Acquisition

Information Acquisition includes the activities that transpire between observation of a suspicious activity and the point at which the suspicious activity has been entered into an organizational or agency ISE-SAR reporting process.

There are numerous approaches to collecting and documenting these observations which vary by discipline and agency. For instance, one local law enforcement organization may initially capture all suspicious activity observations via its standard Field Interview Card or Report which, upon identification or validation as a SAR, would later be flagged for ISE-SAR processing. Another local law enforcement officer may instead directly input suspicious activity observation into a SAR interface, tips and leads, or other reporting system where it could be identified and validated as an ISE-SAR.

For the ISE-SAR *Information Acquisition* business phase, the focus for the ISE should not be to standardize all aspects of the various organization-specific analytical processes or systems, but to instead focus on ensuring specific information deemed necessary by ISE-SAR consumers can be acquired, reflected through an organization's process whenever possible, and shared appropriately. This information is codified into data elements which are atomic units of data with associated attributes. These attributes include a data element name which uniquely identifies this piece of information such as "Person First Name" and a definition to describe the type of information that should be stored using this data element.

2. Organizational Processing

The *Organization Processing* category of processes involves assessing whether an event should be deemed a suspicious activity.

Each contributing organization has its own processes to review and validate SAR information. For example, in some cases, information is reviewed by a supervisor and/or other subject matter expert before being advanced; while in other organizations, a quality assurance review is also required. The majority of the processes in the *Organizational Processing* category are specific to each ISE participant constructed to support participant missions to include, but not limited, to terrorism. While modification of some of the processes may be necessary to conform to overall ISE functional standards, the primary focus of the ISE in this business process category is to establish common criteria to ensure potential terrorism-related SAR information is placed into the ISE.

3. Integration/Consolidation

The *Integration/Consolidation* category of processes involves making the individual agency or department's SAR information available for integration in the ISE through ISE Shared Spaces as described in the ISE EAF. The determination of an ISE-SAR is a two-part process. First, at the State or major urban area fusion center or Federal agency, an analyst or law enforcement officer reviews the newly reported information against ISE-SAR criteria. Second, based on available knowledge and information, the analyst or law enforcement

officer determines whether the information meeting the criteria may have a nexus to terrorism. Once SAR information has been identified as potentially terrorism-related, an ISE participant would share that information, specifically the “data elements,” with the State or major urban area fusion center and the broader ISE community.

4. Data Retrieval/Distribution

This process category involves those activities that will allow departments, agencies, and ISE participants to receive or retrieve ISE-SARs from across the ISE population.

5. Feedback

This final ISE-SAR process category captures three types of feedback designed to improve the overall quality and effectiveness of the ISE-SAR process.

1. **Utilization:** This entails the requirement for a mechanism to inform the originating organization if SAR information is utilized or requires modifications to clarify, update, or correct information.
2. **Cross-flow/Back-flow:** This entails a mechanism to link SARs, and to reflect this information in the ISE to give end-users the ability to follow-up on the report.
3. **Process Modification:** This entails adding to, clarifying, or modifying the SAR data elements being collected; the criteria being utilized to nominate SARs to the ISE; and other ISE-SAR process issues.

D. Broader ISE-SAR Applicability

Consistent with ISE Privacy Guidelines and Presidential Guideline 2, and to the full extent permitted by law, this ISE-SAR Functional Standard is designed to support the sharing of unclassified information or controlled unclassified information (CUI) within the ISE.⁴ There is also a provision for using a data element indicator for designating classified national security information as necessary. The State or major urban area fusion centers shall act as the key conduit between the State, local, and tribal (SLT) agencies and other ISE participants. It is also important to note the ISE Shared Space⁵ implementation concept is focused exclusively on terrorism related information, however many SAR originators and consumers have responsibilities beyond terrorist activities and beyond the scope of the ISE. Of special note, there is no intention to modify through this ISE-SAR Functional Standard or otherwise affect the currently supported and/or mandated direct interactions between State, local, and tribal law enforcement and investigatory personnel and the Joint Terrorism Task Force (JTTF) or Field Intelligence Groups (FIGs).

⁴ The Presidential Guideline 3 Report: Standardize Procedures for Sensitive But Unclassified (SBU) information is currently in the final interagency review process. For purposes of this ISE-SAR Functional Standard, the term Controlled Unclassified Information is intended to cover unclassified information that carries a control marking.

⁵ Program Manager-ISE, *ISE Enterprise Architecture Framework, Version 1.0*, (Washington, DC: PM-ISE, 2007), xviii.

This ISE-SAR Functional Standard should be used as the ISE-SAR information exchange standard for all ISE participants. Although the extensibility of this functional standard does support customization for unique communities, jurisdictions wishing to modify this functional standard must carefully consider the consequences of customization. The PM-ISE requests that modification follow a formal change request process through the SAR governance process (to be adopted) and CTISS Committee under the Information Sharing Council, for both community coordination and consideration. Furthermore, messages that do not conform to this functional standard may not be consumable by the receiving organization and may require modifications by the nonconforming organizations.

There exist a variety of internal processes conducted at the State and major urban area fusion centers and their external interfaces to the Federal Government. Figure 2 represents a number of the various information management and exchange processes that take place in the reporting and sharing of suspicious activities. As shown, SAR vetting and standards is one part of a number of processes that support the functional flow of information in the ISE.

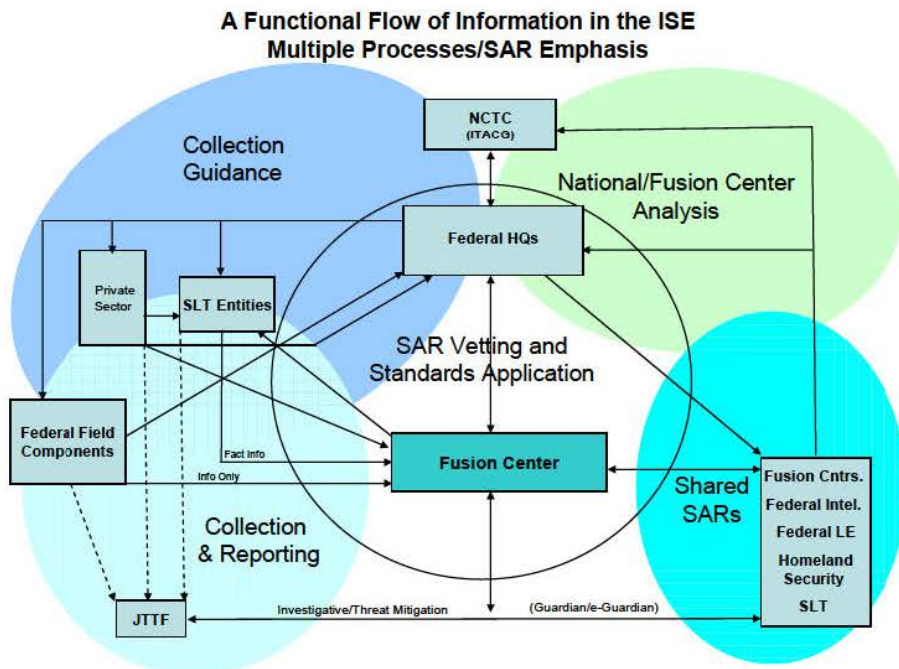


Figure 2 – ISE-SAR Exchanges

E. Protecting Privacy

Laws that prohibit or otherwise limit the sharing of personal information vary considerably between the Federal, State, and local levels. The Privacy Act of 1974 (5 USC §552a) as amended, other statutes such as the E-Government Act, and many government-wide or departmental regulations establish a framework and criteria for protecting information privacy in the Federal Government. The ISE must facilitate the sharing of information in a lawful manner, which by its nature must recognize, in addition to Federal statutes and regulations, different state and local or tribal laws and statutes that affect privacy. One method for protecting privacy while enabling the broadest possible sharing, would be to anonymize ISE-SAR reports by removing data elements that contain personal information. Accordingly two ISE-SAR information exchange packages have been created; a “Detailed” and a “Summary” ISE-SAR package. ISE-SAR exchanges can employ either the “Detailed” or “Summary” SAR information exchange depending on the sending or receiving agencies’ laws, regulations, and other data sharing requirements. The difference between these two exchanges lies in the inclusion or exclusion of certain data elements that may be used to identify an individual, i.e., “privacy fields.”

The “Detailed” ISE-SAR information exchange includes all law enforcement defined data elements *including* privacy fields such as name, address, and vehicle registration information. The “Summary” ISE-SAR information exchange includes the aforementioned law enforcement defined data elements *excluding* privacy fields such as name, address, and vehicle registration information. Each ISE participant can exclude additional data elements from the summary ISE-SAR information exchange in accordance with its own legal and policy requirements. It is believed the data contained within a “Summary” ISE-SAR will support sufficient trending and pattern recognition to trigger further analysis and/or investigation where additional information can be requested from the sending agency. Because of variances of data expected within ISE-SAR exchanges, only the minimum elements are considered mandatory. These are enumerated in the READ ME document in the technical artifacts folder that is part of this ISE-SAR Functional Standard.

It is important to note that implementers can employ either information exchange and still populate only those data elements that are compatible with local statute and policy. As the ISE evolves, it may be possible to specifically identify those privacy fields common to all jurisdictions, enabling development of a standardized summary ISE-SAR. Currently, the privacy fields identified in the ISE-SAR exchange data model (Section IV, below) are the minimum fields that should be removed from a ‘Detailed’ ISE-SAR.

SECTION III – INFORMATION EXCHANGE DEVELOPMENT

This ISE-SAR Functional Standard is a collection of artifacts that support an implementer’s creation of ISE-SAR information exchanges, whether “Detailed” or “Summary.” The basic ISE-SAR information exchange is documented using four unique artifacts giving implementers tangible products which can be leveraged for local implementation. A domain model provides a graphical depiction of those data elements required for implementing an exchange and the cardinality between those data elements. Second, a Component Mapping Template is a spreadsheet that associates each required data element with its corresponding XML data element.

Third, information exchanges include the schemas which consist of a document, extension, and constraint schema. Fourth, at least one sample XML Instance and associated style-sheet is included to help practitioners validate the model, mapping, and schemas in a more intuitive way.

SECTION IV – ISE-SAR EXCHANGE DATA MODEL

A. Summary of Elements

This section contains a full inventory of all ISE-SAR information exchange data classes, elements, and definitions. Items and definitions contained in cells with a light purple background are data classes, while items and definition contained in cells with a white background are data elements. A wider representation of data class and element mappings to source (ISE-SAR information exchange) and target is contained in the Component Mapping Template located in the technical artifacts folder.

Cardinality between objects in the model is indicated on the line in the domain model (see Section 5A). Cardinality indicates how many times an entity can occur in the model. For example, Vehicle, Vessel, and Aircraft all have cardinality of 0..n. This means that they are optional, but may occur multiple times if multiple suspect vehicles are identified.

Clarification of Organizations used in the exchange:

- The **Source Organization** is the agency or entity that originates the SAR report (examples include a local police department, a private security firm handling security for a power plant, and a security force at a military installation). The Source Organization will not change throughout the life of the SAR.
- The **Submitting Organization** is the organization providing the ISE-SAR to the ISE. The Submitting Organization and the Source Organization may be the same.
- The **Owning Organization** is the organization that owns the target associated with the suspicious activity.

Table 2 – ISE-SAR Information Exchange Data Classes, Elements, and Definitions

Privacy Field	Source Class/Element	Source Definition
	Aircraft	
	Aircraft Engine Quantity	The number of engines on an observed aircraft.
	Aircraft Fuselage Color	A code identifying a color of a fuselage of an aircraft.
	Aircraft ID	A unique identifier assigned to the aircraft by the observing organization—used for referencing. [free text field]
	Aircraft Make Code	A code identifying a manufacturer of an aircraft.
	Aircraft Model Code	A code identifying a specific design or type of aircraft made by a manufacturer.
	Aircraft Style Code	A code identifying a style of an aircraft.
	Aircraft Tail Number	An identifier of an aircraft. Sometimes referred to as a tail number. [free text field]

Privacy Field	Source Class/Element	Source Definition
	Aircraft Wing Color	A code identifying a color of the wings of an aircraft.
	Attachment	
	Attachment Type Text	Describes the type of attachment (e.g., surveillance video, mug shot, evidence). [free text field]
	Binary Image	Binary encoding of the attachment.
	Capture Date	The date that the attachment was created.
	Description Text	Text description of the attachment. [free text field]
	Format Type Text	Format of attachment (e.g., mpeg, jpg, avi). [free text field]
	Attachment URI	Uniform Resource Identifier (URI) for the attachment. Used to match the attachment link to the attachment itself. Standard representation type that can be used for Uniform Resource Locators (URLs) and Uniform Resource Names (URNs).
	Attachment Privacy Field Indicator	Identifies whether the binary attachment contains information that may be used to identify an individual.
	Contact Information	
	Person First Name	Person to contact at the organization.
	Person Last Name	Person to contact at the organization.
	E-Mail Address	An email address of a person or organization. [free text field]
	Full Telephone Number	A full length telephone identifier representing the digits to be dialed to reach a specific telephone instrument. [free text field]
	Driver License	
	Expiration Date	The date the document expires.
	Issuing Authority Text	Code identifying the organization that issued the driver license assigned to the person. Examples include Department of Motor Vehicles, Department of Public Safety and Department of Highway Safety and Motor Vehicles. [free text field]
X	Driver License Number	A driver license identifier or driver license permit identifier of the observer or observed person of interest involved with the suspicious activity. [free text field]
	Follow-Up Action	
	Activity Date	Date that the follow-up activity started.
	Activity Time	Time that the follow up activity started.
	Assigned By Text	Organizational identifier that describes the organization performing a follow-up activity. This is designed to keep all parties interested in a particular ISE-SAR informed of concurrent investigations. [free text field]
	Assigned To Text	Text describing the person or sub-organization that will be performing the designated action. [free text field]
	Disposition Text	Description of disposition of suspicious activity investigation. [free text field]
	Status Text	Description of the state of follow-up activity. [free text field]
	Location	
	Location Description	A description of a location where the suspicious activity occurred. If the location is an address that is not broken into its component parts (e.g., 1234 Main Street), this field may be used to store the compound address. [free text field]

Privacy Field	Source Class/Element	Source Definition
	Location Address	
	Building Description	A complete reference that identifies a building. [free text field]
	County Name	A name of a county, parish, or vicinage. [free text field]
	Country Name	A country name or other identifier. [free text field]
	Cross Street Description	A description of an intersecting street. [free text field]
	Floor Identifier	A reference that identifies an actual level within a building. [free text field]
	Mile Marker Text	Identifies the sequentially numbered marker on a roadside that is closest to the intended location. Also known as milepost, or mile post. [free text field]
	Municipality Name	The name of the city or town. [free text field]
	Postal Code	The zip code or postal code. [free text field]
	State Name	Code identifying the state.
	Street Name	A name that identifies a particular street. [free text field]
	Street Number	A number that identifies a particular unit or location within a street. [free text field]
	Street Post Directional	A direction that appears after a street name. [free text field]
	Street Pre Directional	A direction that appears before a street name. [free text field]
	Street Type	A type of street, e.g., Street, Boulevard, Avenue, Highway. [free text field]
	Unit ID	A particular unit within the location. [free text field]
	Location Coordinates	
	Altitude	Height above or below sea-level of a location.
	Coordinate Datum	Coordinate system used for plotting location.
	Latitude Degree	A value that specifies the degree of a latitude. The value comes from a restricted range between -90 (inclusive) and +90 (inclusive).
	Latitude Minute	A value that specifies a minute of a degree. The value comes from a restricted range of 0 (inclusive) to 60 (exclusive).
	Latitude Second	A value that specifies a second of a minute. The value comes from a restricted range of 0 (inclusive) to 60 (exclusive).
	Longitude Degree	A value that specifies the degree of a longitude. The value comes from a restricted range between -180 (inclusive) and +180 (exclusive).
	Longitude Minute	A value that specifies a minute of a degree. The value comes from a restricted range of 0 (inclusive) to 60 (exclusive).
	Longitude Second	A value that specifies a second of a minute. The value comes from a restricted range of 0 (inclusive) to 60 (exclusive).
	Observer	
	Observer Type Text	Indicates the relative expertise of an observer to the suspicious activity (e.g., professional observer versus layman). Example: a security guard at a utility plant recording the activity, or a citizen driving by viewing suspicious activity. [free text field]
X	Person Employer ID	Number assigned by an employer for a person such as badge number. [free text field]
	Owning Organization	

Privacy Field	Source Class/Element	Source Definition
	Organization Item	A name of an organization that owns the target. [free text field]
	Organization Description	A text description of organization that owns the target. The description may indicate the type of organization such as State Bureau of Investigation, Highway Patrol, etc. [free text field]
X	Organization ID	A federal tax identifier assigned to an organization. Sometimes referred to as a Federal Employer Identification Number (FEIN), or an Employer Identification Number (EIN). [free text field]
	Organization Local ID	An identifier assigned on a local level to an organization. [free text field]
	Other Identifier	
X	Person Identification Number (PID)	An identifying number assigned to the person, e.g., military serial numbers. [free text field]
	PID Effective Date	The date that the PID number became active or accurate.
	PID Expiration Date	The date that the PID number expires.
	PID Issuing Authority Text	The issuing authority of the identifier. This may be a state, military organization, etc.
	PID Type Code	Code identifying the type of identifier assigned to the person. [free text field]
	Passport	
X	Passport ID	Document Unique Identifier. [free text field]
	Expiration Date	The date the document expires.
	Issuing Country Code	Code identifying the issuing country. [free text field]
	Person	
X	AFIS FBI Number	A number issued by the FBI's Automated Fingerprint Identification System (AFIS) based on submitted fingerprints. [free text field]
	Age	A precise measurement of the age of a person.
	Age Unit Code	Code that identifies the unit of measure of an age of a person (e.g., years, months). [free text field]
	Date of Birth	A date a person was born.
	Ethnicity Code	Code that identifies the person's cultural lineage.
	Maximum Age	The maximum age measurement in an estimated range.
	Minimum Age	The minimum age measurement in an estimated range.
X	State Identifier	Number assigned by the state based on biometric identifiers or other matching algorithms. [free text field]
X	Tax Identifier Number	A 9-digit numeric identifier assigned to a living person by the U.S. Social Security Administration. A social security number of the person. [free text field]
	Person Name	
X	First Name	A first name or given name of the person. [free text field]
X	Last Name	A last name or family name of the person. [free text field]
X	Middle Name	A middle name of a person. [free text field]
X	Full Name	Used to designate the compound name of a person that includes all name parts. This field should only be used when the name cannot be broken down into its component parts or if the information is not available in its component parts. [free text field]

Privacy Field	Source Class/Element	Source Definition
X	Moniker	Alternative, or gang name for a person. [free text field]
	Name Suffix	A component that is appended after the family name that distinguishes members of a family with the same given, middle, and last name, or otherwise qualifies the name. [free text field]
	Name Type	Text identifying the type of name for the person. For example, maiden name, professional name, nick name.
	Physical Descriptors	
	Build Description	Text describing the physique or shape of a person. [free text field]
	Eye Color Code	Code identifying the color of the person's eyes.
	Eye Color Text	Text describing the color of a person's eyes. [free text field]
	Hair Color Code	Code identifying the color of the person's hair.
	Hair Color Text	Text describing the color of a person's hair. [free text field]
	Person Eyewear Text	A description of glasses or other eyewear a person wears. [free text field]
	Person Facial Hair Text	A kind of facial hair of a person. [free text field]
	Person Height	A measurement of the height of a person.
	Person Height Unit Code	Code that identifies the unit of measure of a height of a person. [free text field]
	Person Maximum Height	The maximum measure value on an estimated range of the height of the person.
	Person Minimum Height	The minimum measure value on an estimated range of the height of the person.
	Person Maximum Weight	The maximum measure value on an estimated range of the weight of the person.
	Person Minimum Weight	The minimum measure value on an estimated range of the weight of the person.
	Person Sex Code	A code identifying the gender or sex of a person (e.g., Male or Female).
	Person Weight	A measurement of the weight of a person.
	Person Weight Unit Code	Code that identifies the unit of measure of a weight of a person. [free text field]
	Race Code	Code that identifies the race of the person.
	Skin Tone Code	Code identifying the color or tone of a person's skin.
	Clothing Description Text	A description of an article of clothing. [free text field]
	Physical Feature	
	Feature Description	A text description of a physical feature of the person. [free text field]
	Feature Type Code	A special kind of physical feature or any distinguishing feature. Examples include scars, marks, tattoo's, or a missing ear. [free text field]
	Location Description	A description of a location. If the location is an address that is not broken into its component parts (e.g., 1234 Main Street), this field may be used to store the compound address. [free text field]
	Registration	

Privacy Field	Source Class/Element	Source Definition
	Registration Authority Code	Text describing the organization or entity authorizing the issuance of a registration for the vehicle involved with the suspicious activity. [free text field]
X	Registration Number	The number on a metal plate fixed to/assigned to a vehicle. The purpose of the license plate number is to uniquely identify each vehicle within a state. [free text field]
	Registration Type	Code that identifies the type of registration plate or license plate of a vehicle. [free text field]
	Registration Year	A 4-digit year as shown on the registration decal issued for the vehicle.
ISE-SAR Submission		
	Additional Details Indicator	Identifies whether more ISE-SAR details are available at the authoring/originating agency than what has been provided in the information exchange.
	Data Entry Date	Date the data was entered into the reporting system (e.g., the Records Management System).
	Dissemination Description Code	Generally established locally, this code describes the authorized recipients of the data. Examples include Law Enforcement Use, Do Not Disseminate, etc.
	Fusion Center Contact First Name	Identifies the first name of the person to contact at the fusion center. [free text field]
	Fusion Center Contact Last Name	Identifies the last name of the person to contact at the fusion center. [free text field]
	Fusion Center Contact E-Mail Address	Identifies the email address of the person to contact at the fusion center. [free text field]
	Fusion Center Contact Telephone Number	The full phone number of the person at the fusion center that is familiar with the record (e.g., law enforcement officer).
	Message Type Indicator	e.g., Add, Update, Purge.
	Privacy Purge Date	The date by which the privacy information will be purged from the record system; general observation data is retained.
	Privacy Purge Review Date	Date of review to determine the disposition of the privacy fields in a Detailed ISE-SAR record.
	Submitting ISE-SAR Record ID	Identifies the Fusion Center ISE-SAR Record identifier for reports that are possibly related to the current report. [free text field]
	ISE-SAR Title	Plain language title (e.g., Bomb threat at the "X" Hotel). [free text field]
	ISE-SAR Version	Indicates the specific version of the ISE-SAR that the XML Instance corresponds. [free text field]
	Source Agency Case ID	The case identifier for the agency that originated the SAR. Often, this will be a local law enforcement agency. [free text field]
	Source Agency Record Reference Name	The case identifier that is commonly used by the source agency—may be the same as the System ID. [free text field]
	Source Agency Record Status	The current status of the record within the source agency system.

Privacy Field	Source Class/Element	Source Definition
	Privacy Information Exists Indicator	Indicates whether privacy information is available from the source fusion center. This indicator may be used to guide people who only have access to the summary information exchange as to whether or not they can follow-up with the originating fusion center to obtain more information.
	Sensitive Information Details	
	Classification Label	A classification of information. Includes Confidential, Secret, Top Secret, no markings. [free text field]
	Classification Reason Text	A reason why the classification was made as such. [free text field]
	Sensitivity Level	Local information security categorization level (Controlled Unclassified Information-CUI, including Sensitive But Unclassified or Law Enforcement Sensitive). [free text field]
	Tearlined Indicator	Identifies whether a report is free of classified information.
	Source Organization	
	Organization Name	The name used to refer to the agency originating the SAR. [free text field]
	Organization ORI	Originating Agency Identification (ORI) used to refer to the agency.
	System ID	The system that the case identifier (e.g., Records Management System, Computer Aided Dispatch) relates to within or the organization that originated the Suspicious Activity Report. [free text field]
	Source Agency Contact First Name	The first name of the person at the agency that is familiar with the record (e.g., law enforcement officer). [free text field]
	Source Agency Contact Last Name	The last name of the person at the agency that is familiar with the record (e.g., law enforcement officer). [free text field]
	Source Agency Contact Email Address	The email address of the person at the agency that is familiar with the record (e.g., law enforcement officer). [free text field]
	Source Agency Contact Phone Number	The full phone number of the person at the agency that is familiar with the record (e.g., law enforcement officer).
	Suspicious Activity Report	
	Community Description	Describes the intended audience of the document. [free text field]
	Community URI	The URL to resolve the ISE-SAR information exchange payload namespace.
	LEXS Version	Identifies the version of Department of Justice LEISP Exchange Specification (LEXS) used to publish this document. ISE-FS-200 has been built using LEXS version 3.1. The schema was developed by starting with the basic LEXS schema and extending that definition by adding those elements not included in LEXS. [free text field]
	Message Date/Time	A timestamp identifying when this message was received.
	Sequence Number	A number that uniquely identifies this message.
	Submitting Organization	
	Organization Name	Common Name of the fusion center or ISE participant that submitted the ISE-SAR record to the ISE. [free text field]
	Organization ID	Fusion center or ISE participant's alpha-numeric identifier. [free text field]

Privacy Field	Source Class/Element	Source Definition
	Organization ORI	ORI for the submitting fusion center or ISE participant. [free text field]
	System ID	Identifies the system within the fusion center or ISE participant that is submitting the ISE-SAR. [free text field]
	Suspicious Activity	
	Activity End Date	The end or completion date in Greenwich Mean Time (GMT) of an incident that occurs over a duration of time.
	Activity End Time	The end or completion time in GMT of day of an incident that occurs over a duration of time.
	Activity Start Date	The date in GMT when the incident occurred or the start date if the incident occurs over a period of time.
	Activity Start Time	The time of day in GMT that the incident occurred or started.
	Observation Description Text	Description of the activity including rationale for potential terrorism nexus. [free text field]
	Observation End Date	The end or completion date in GMT of the observation of an activity that occurs over a duration of time.
	Observation End Time	The end or completion time of day in GMT of the observation of an activity that occurred over a period of time.
	Observation Start Date	The date in GMT when the observation of an activity occurred or the start date if the observation of the activity occurred over a period of time.
	Observation Start Time	The time of day in GMT that the observation of an activity occurred or started.
	Tip Class Code	Broad category of threat to which the tip or lead pertains. Includes Financial Incident, Suspicious Activity, and Cyber Crime.
	Tip Subtype Text	Breakdown of the Tip Type, it indicates the type of threat to which the tip or lead pertains. The subtype is often dependent on the Tip Type. For example, the subtypes for a nuclear/radiological tip class might be Nuclear Explosive or a Radiological Dispersal Device. [free text field]
	Tip Type Code	Indicates the type of threat to which the tip or lead pertains. Examples include a biological or chemical threat.
	Weather Condition Details	The weather at the time of the suspicious activity. The weather may be described using codified lists or text.
	Target	
	Critical Infrastructure Indicator	Critical infrastructure, as defined by 42 USC Sec. 5195c, means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
	Infrastructure Sector Code	The broad categorization of the infrastructure type. These include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government.

Privacy Field	Source Class/Element	Source Definition
	Infrastructure Tier Text	Provides additional detail that enhances the Target Sector Code. For example, if the target sector is Utilities, this field would indicate the type of utility that has been targeted such as power station or power transmission. [free text field]
	Structure Type Code	National Data Exchange (N-DEx) Code that identifies the type of Structure that was involved in the incident.
	Target Type Text	Describes the target type if an appropriate sector code is not available. [free text field]
	Structure Type Text	Text for use when the Structure Type Code does not afford necessary code. [free text field]
	Target Description Text	Text describing the target (e.g., Lincoln Bridge). [free text field]
	Vehicle	
	Color Code	Code that identifies the primary color of a vehicle involved in the suspicious activity.
	Description	Text description of the entity. [free text field]
	Make Name	Code that identifies the manufacturer of the vehicle.
	Model Name	Code that identifies the specific design or type of vehicle made by a manufacturer—sometimes referred to as the series model.
	Style Code	Code that identifies the style of a vehicle. [free text field]
	Vehicle Year	A 4-digit year that is assigned to a vehicle by the manufacturer.
X	Vehicle Identification Number	Used to uniquely identify motor vehicles. [free text field]
X	US DOT Number	An assigned number sequence required by Federal Motor Carrier Safety Administration (FMCSA) for all interstate carriers. The identification number (found on the power unit, and assigned by the U.S. Department of Transportation or by a State) is a key element in the FMCSA databases for both carrier safety and regulatory purposes. [free text field]
	Vehicle Description	A text description of a vehicle. Can capture unique identifying information about a vehicle such as damage, custom paint, etc. [free text field]
	Related ISE-SAR	
	Fusion Center ID	Identifies the fusion center that is the source of the ISE-SAR. [free text field]
	Fusion Center ISE-SAR Record ID	Identifies the fusion center ISE-SAR record identifier for reports that are possibly related to the current report.
	Relationship Description Text	Describes how this ISE-SAR is related to another ISE-SAR. [free text field]
	Vessel	
X	Vessel Coast Guard Document Number	An identifying number assigned by the U.S. Coast Guard to commercial vessels and certain motor yachts over five tons. Number is encompassed within valid marine documents and permanently marked on the main beam of a documented vessel. [free text field]
X	Vessel ID	A unique identifier assigned to the boat record by the agency—used for referencing. [free text field]

Privacy Field	Source Class/Element	Source Definition
	Vessel ID Issuing Authority	Identifies the organization authorization over the issuance of a vessel identifier. Examples of this organization include the State Parks Department and the Fish and Wildlife department. [free text field]
	Vessel Make	Code that identifies the manufacturer of the boat.
	Vessel Model	Model name that identifies the specific design or type of boat made by a manufacturer—sometimes referred to as the series model.
	Vessel Model Year	A 4-digit year that is assigned to a boat by the manufacturer.
	Vessel Name	Complete boat name and any numerics. [free text field]
	Vessel Overall Length	The length measurement of the boat, bow to stern.
	Vessel Overall Length Measure	Code that identifies the measurement unit used to determine the boat length. [free text field]
X	Vessel Serial Number	The identification number of a boat involved in an incident. [free text field]
	Vessel Type Code	Code that identifies the type of boat.
	Vessel Propulsion Text	Text for use when the Boat Propulsion Code does not afford necessary code. [free text field]

B. Association Descriptions

This section defines specific data associations contained in the ISE-SAR data model structure. Reference Figure 3 (UML-based model) for the graphical depiction and detailed elements.

Table 3 – ISE-SAR Data Model Structure Associations

Link Between Associated Components	Target Element
Link From Suspicious Activity Report to Attachment	lexs:Digest/lexsdigest:Associations/lexsdigest:EntityAttachmentLinkAssociation
Link From Suspicious Activity Report to Sensitive Information Details	Hierarchical Association
Link From Suspicious Activity Report to ISE-SAR Submission	Hierarchical Association
Link From Suspicious Activity to Vehicle	lexs:Digest/lexsdigest:Associations/lexsdigest:IncidentInvolvedItemAssociation
Link From Vehicle to Registration	Hierarchical Association
Link From Suspicious Activity to Vessel	lexs:Digest/lexsdigest:Associations/lexsdigest:IncidentInvolvedItemAssociation
Link From Suspicious Activity to Aircraft	lexs:Digest/lexsdigest:Associations/lexsdigest:IncidentInvolvedItemAssociation
Link From Suspicious Activity to Location	lexs:Digest/lexsdigest:Associations/lexsdigest:ActivityLocationAssociation

Link Between Associated Components	Target Element
Link From Location to Location Coordinates	Hierarchical Association
Link From Location to Location Address	Hierarchical Association
Link From Suspicious Activity Report to Related ISE-SAR	Hierarchical Association
Link From Person to Location	lexs:Digest/lexsdigest:Associations/lexsdigest:PersonLocationAssociation
Link From Person to Contact Information	lexs:Digest/lexsdigest:Associations/lexsdigest:EntityEmailAssociation or lexs:Digest/lexsdigest:Associations/lexsdigest:EntityTelephoneNumberAssociation
Link From Person to Driver License	Hierarchical Association
Link From Person to Passport	Hierarchical Association
Link From Person to Other Identifier	Hierarchical Association
Link From Person to Physical Descriptors	Hierarchical Association
Link From Person to Physical Feature	Hierarchical Association
Link From Person to Person Name	Hierarchical Association
Link From Suspicious Activity Report to Follow-Up Action	Hierarchical Association
Link From Target to Location	loxs:Digest/lexsdigest:Associations/loxsdigest:ItemLocationAssociation
Link From Suspicious Activity Report to Organization	Hierarchical Association
Link From Suspicious Activity to Person [Witness]	lexs:Digest/lexsdigest:Associations/lexsdigest:IncidentWitnessAssociation
Link From Suspicious Activity to Person [Person Of Interest]	lexs:Digest/lexsdigest:Associations/lexsdigest:PersonOfInterestAssociation
Link From Organization to Target	ext:SuspiciousActivityReport/nc:OrganizationItemAssociation
Link from ISE-SAR Submission to Submitting Organization	Hierarchical Association
Link From Submitting Organization to Contact Information	Hierarchical Association (Note that the mapping indicates context and we are not reusing Contact Information components)

C. Extended XML Elements

Additional data elements are also identified as new elements outside of NIEM, Version 2.0. These elements are listed below:

AdditionalDetailsIndicator: Identifies whether more ISE-SAR details are available at the authoring/originating agency than what has been provided in the information exchange.

AssignedByText: Organizational identifier that describes the organization performing a follow-up activity. This is designed to keep all parties interested in a particular ISE-SAR informed of concurrent investigations.

AssignedToText: Text describing the person or sub-organization that will be performing the designated follow-up action.

ClassificationReasonText: A reason why the classification was made as such.

CriticalInfrastructureIndicator: Critical infrastructure, as defined by 42 USC Sec. 5195c, means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

PrivacyFieldIndicator: Data element that may be used to identify an individual and therefore is subject to protection from disclosure under applicable privacy rules. Removal of privacy fields from a detailed report will result in a summary report. This privacy field informs users of the summary information exchange that additional information may be available from the originator of the report.

ReportPurgeDate: The date by which the privacy fields will be purged from the record system; general observation data is retained. Purge policies vary from jurisdiction to jurisdiction and should be indicated as part of the guidelines.

ReportPurgeReviewDate: Date of review to determine the disposition of the privacy fields in a Detailed ISE-SAR record.

SECTION V – INFORMATION EXCHANGE IMPLEMENTATION ARTIFACTS

A. Domain Model

1. General Domain Model Overview

The domain model provides a visual representation of the business data requirements and relationships (Figure 3). This Unified Modeling Language (UML)-based Model represents the Exchange Model artifact required in the information exchange development methodology. The model is designed to demonstrate the organization of data elements and illustrate how these elements are grouped together into Classes. Furthermore, it describes relationships between these Classes. A key consideration in the development of a Domain Model is that it must be independent of the mechanism intended to implement the model. The domain model is actually a representation of how data is structured from a *business* context. As the technology changes and new functional standards emerge, developers can create new standards mapping documents and schema tied to a new standard without having to re-address business process requirements.

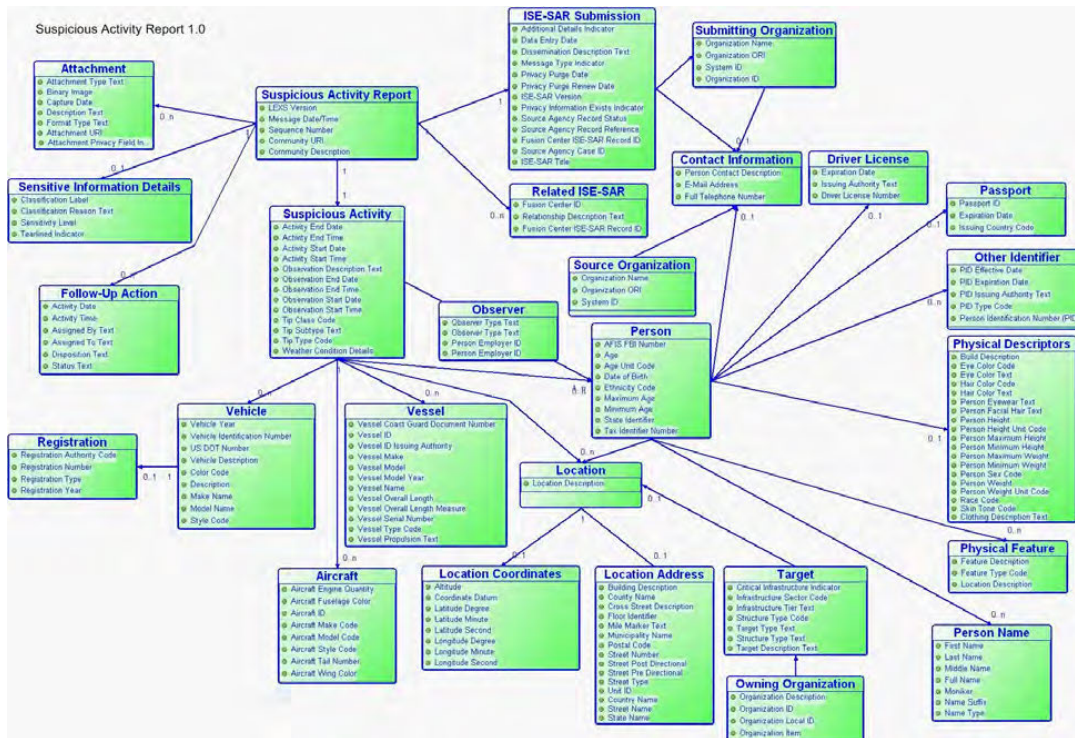


Figure 3 – UML-based Model⁶

B. General Mapping Overview

The detailed component mapping template provides a mechanism to cross-reference the business data requirements documented in the Domain Model to their corresponding XML Element in the XML Schema. It includes a number of items to help establish equivalency including the business definition and the corresponding XML Element Definition.

C. ISE-SAR Mapping Overview

The Mapping Spreadsheet contains seven unique items for each ISE-SAR data class and element. The Mapping Spreadsheet columns are described in this section.

⁶ This figure may be also found in the technical artifacts folder that is part of this functional standard.

Table 4 – Mapping Spreadsheet Column Descriptions

Spreadsheet Name & Row	Description
Privacy Field Indicator	This field indicates that the information may be used to identify an individual.
Source Class/ Element	Content in this column is either the data class (grouping of data elements) or the actual data elements. Classes are highlighted and denoted with cells that contain blue background while elements have a white background. The word "Source" is referring to the ISE-SAR information exchange.
Source Definition	The content in this column is the class or element definition defined for this ISE-SAR information exchange. The word "Source" is referring to the ISE-SAR information exchange definition.
Target Element	The content in this column is the actual namespace path deemed equal to the related ISE-SAR information exchange element.
Target Element Definition	The content in this column provides the definition of the target or NIEM element located at the aforementioned source path. "Target" is referring to the NIEM definition.
Target Element Base	Indicates the data type of the terminal element. Data types of niem-xsd:String or nc:TextType indicate free-form text fields.
Mapping Comments	Provides technical implementation information for developers and implementers of the information exchange.

D. Schemas

The ISE-SAR Functional Standard contains the following compliant schemas:

- Subset Schema
- Exchange Schema
- Extension Schema
- Wantlist

E. Examples

The ISE-SAR Functional Standard contains two samples that illustrate exchange content as listed below.

1. XSL Style Sheet

This information exchange artifact provides an implementer and users with a communication tool which captures the look and feel of a familiar form, screen, or like peripheral medium for schema translation testing and user validation of business rules.

2. XML Instance

This information exchange artifact provides an actual payload of information with data content defined by the schema(s).

This page intentionally blank.

PART B – ISE-SAR CRITERIA GUIDANCE

Category	Description
Eliciting Information	Questioning facility personnel about facility/infrastructure/personnel; this includes individuals probing employees in person on or off-site, over the phone, or via the Internet about particular structures, functions, and personnel procedures at the facility/infrastructure.
Breach/Attempted Intrusion	Unauthorized personnel attempting to or actually entering a restricted area or protected site. Impersonation of authorized personnel (e.g. police/security, janitor).
Misrepresentation	Presenting false or misusing insignia, documents, and/or identification, to misrepresent one's affiliation to cover possible illicit activity.
Photography	Taking pictures/video of facility/infrastructure/personnel or surrounding environment.
Observation	Showing unusual interest in facility/infrastructure/personnel; for example, observing it through binoculars, taking notes, drawing maps, or drawing structures of the facility.
Surveillance	Monitoring the activity of people, facilities, processes or systems.
Theft/Loss/Diversion	Stealing or diverting something associated with a facility/infrastructure (e.g., badges, uniforms, identification, emergency vehicles, technology or documents {classified or unclassified}, which are proprietary to the facility).
Sabotage/Tampering/ Vandalism	Damaging, manipulating, or defacing part of a facility/infrastructure or protected site.
Testing of Security	Interactions with, or challenges to installations, personnel, or systems that reveal physical, personnel or cyber security capabilities.
Cyber Attack	Compromising, or attempting to compromise or disrupt an organization's information technology infrastructure.
Expressed or Implied Threat	Communicating a spoken or written threat to damage or compromise a facility/infrastructure.
Flyover	Suspected over flight of a facility/infrastructure; this includes any type of flying vehicle (e.g., airplanes, helicopters, unmanned aerial vehicles, hang gliders).
Materials Acquisition/Storage	Acquisition of unusual quantities of precursor material (e.g., cell phones, pagers, fuel, timers), unauthorized/unlicensed individual/group attempts to obtain precursor chemicals/agents, or toxic materials, and rental of storage units for the purpose of storing chemicals or mixing apparatus.
Acquisition Of Expertise	Attempts to obtain or conduct training in security concepts; military weapons or tactics; or other, unusual, capabilities, such as specialized transport or handling capabilities.
Weapons Discovery	Discovery of weapons or explosives.
Sector-Specific Incident	Actions associated with a characteristic of unique concern to specific sectors (such as the public health sector), with regard to their personnel, facilities, systems or functions.
Recruiting	Building of operations teams and contacts, personnel data, banking data or travel data.
Other	Incidents not fitting any of the above categories.

This page intentionally blank.

PART C – ISE-SAR INFORMATION FLOW DESCRIPTION

Step	Activity	Process	Notes
1	Observation	The process begins when a person or persons observe unusual behavior. Such activities could include, but are not limited to, surveillance, photography of facilities, site breach or physical intrusion, cyber attacks, possible testing of security or security response, indications of unusual public health sector activity, unauthorized attempts to obtain precursor chemical/agents or toxic materials, or other unusual behavior or sector-specific incidents. ⁷	The observer may be a private citizen, a government official, or a law enforcement officer.
2	Initial Response and Investigation	An official of a Federal, State, or local agency with jurisdiction responds to the reported observation. ⁸ This official gathers additional facts through personal observations, interviews, and other investigative activities. In the context of priority information requirements, as provided by State and major urban area fusion centers, the officer/agent may use a number of fact based systems to continue the investigation. These fact based systems provide the officer/agent with a more complete picture of the activity being investigated. Some examples of fact based systems and the information they may provide include: Department of Motor Vehicles provides drivers license and vehicle registration information; National Crime Information Center provides wants and warrants information, criminal history information and access to the Terrorist Screening Center and the terrorist watch list, and Violent Gang/Terrorism Organization File (VGTOF); and Other Federal, State, and local systems can provide criminal checks within the immediate and surrounding jurisdictions. When the initial investigation is complete, the official documents the event. The report becomes the initial record for the law enforcement or Federal agency's records management system (RMS).	The event may be documented using a variety of reporting mechanisms and processes, including but not limited to, reports of investigation, event histories, field interviews (FI), citations, incident reports, and arrest reports. The record may be hard and/or soft copy and does not yet constitute an ISE-SAR.

⁷ Suspicious activity reporting (SAR) is an official documentation of observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention. ISE-SARs are a subset of all SARs that have been determined by an appropriate authority to have a potential nexus to terrorism.

⁸ If a suspicious activity has a direct connection to terrorist activity the flow moves along an operational path. Depending upon urgency, the information could move immediately into law enforcement operations and lead to action against the identified terrorist activity. In this case, the suspicious activity would travel from the initial law enforcement contact directly to the law enforcement agency with enforcement responsibility.

Step	Activity	Process	Notes
3	Local/Regional Processing	<p>The agency processes and stores the information in the RMS following agency policies and procedures. The flow will vary depending on whether the reporting organization is a State or local agency or a field element of a Federal agency.</p> <p>State and local: Based on specific criteria or the nature of the activity observed, the State or local law enforcement components forward the information to the State or major urban area fusion center for further analysis.</p> <p>Federal: Federal field components collecting suspicious activity would forward their reports to the appropriate resident, district, or division office. This information—still only fact information—would be reported to field intelligence groups or headquarters elements through processes that vary from agency to agency.</p> <p>In addition to providing the fact information to its headquarters, the Federal field component would provide an information copy to the State or major urban area fusion center in its geographic region. This information contributes to the assessment of all suspicious activity in the State or major urban area fusion center's area of responsibility.</p>	<p>The State or major urban area fusion center should have access to all suspicious activity reporting in its geographic region whether collected by SLT or Federal field components.</p>
4	Creation of an ISE-SAR	<p>The determination of an ISE-SAR is a two-part process. First, at the State or major urban area fusion center or Federal agency, an analyst or law enforcement officer reviews the newly reported information against ISE-SAR criteria. Second, based on available knowledge and information, the analyst or law enforcement officer determines whether the information meeting the criteria may have a nexus to terrorism.</p> <p>Once this determination is made, the information becomes an "ISE-SAR" and is formatted in accordance with ISE-FS-200 (ISE-SAR Functional Standard). The ISE-SAR would then be shared with appropriate law enforcement and homeland security personnel in the State or major urban area fusion center's area of responsibility.</p>	<p>Some of this information may be intelligence, which identifies trends and other terrorist related information and is derived from Federal agencies such as NCTC, DHS, and the FBI.</p> <p>For State, local, and tribal law enforcement, the ISE-SAR information, may be fact information or criminal intelligence and is handled in accordance with 28 CFR Part 23. It may be shared with State or Federal law enforcement personnel with the privacy field included.</p>
5	ISE-SAR Sharing and Dissemination	<p>In a State or major urban area fusion center, the ISE-SAR is shared with the appropriate FBI field components and the DHS representative and placed in the State or major urban area fusion center's Shared Space or otherwise made available to members of the ISE.</p> <p>The FBI field component enters the ISE-SAR information into the FBI system and sends the information to FBI Headquarters.</p> <p>The DHS representative enters the ISE-SAR information into the DHS system and sends the information to DHS, Office of Intelligence Analysis.</p>	

Step	Activity	Process	Notes
6	Federal Headquarters (HQ) Processing	At the Federal headquarters level, ISE-SAR information is combined with information from other State or major urban area fusion centers and Federal field components and incorporated into an agency-specific national threat assessment that is shared with ISE members. The ISE-SAR information may be provided to NCTC in the form of an agency-specific strategic threat assessment (e.g., strategic intelligence product).	When a State or local originated ISE-SAR is in the Federal system, the rules of sharing are no longer governed by 28 CFR Part 23, but rather by appropriate Federal privacy laws and guidelines.
7	NCTC Analysis	When product(s) containing the ISE-SAR information are made available to NCTC, they are processed, collated, and analyzed with terrorism information from across the five communities—intelligence, defense, law enforcement, homeland security, and foreign affairs—and open sources. NCTC has the primary responsibility within the Federal government for analysis of terrorism information. NCTC produces federally coordinated analytic products that are shared through NCTC Online, the NCTC secure web site. The Interagency Threat Assessment and Coordinating Group (ITACG), housed at NCTC, facilitates the production of coordinated terrorism-related products that are focused on issues and needs of State, local, and tribal entities and when appropriate private sector entities. ITACG is the mechanism that facilitates the sharing of counterterrorism information with SLT.	
8	NCTC Alerts, Warnings, Notifications	NCTC products ⁹ , informed by the ITACG as appropriate, are shared with all appropriate Federal departments and agencies and with SLT through the State or major urban area fusion centers. The sharing with SLT and private sector occurs through the Federal departments or agencies that have been assigned the responsibility and have connectivity with the State or major urban area fusion centers. Some State or major urban area fusion centers, with secure connectivity and an NCTC Online account, can access NCTC products directly. State or major urban area fusion centers will use NCTC and ITACG informed products to help develop geographic-specific risk assessments (GSRA) to facilitate regional counterterrorism efforts. The GSRA are shared with SLT organizations and the private sector as appropriate. The recipient of the GSRA may use the GSRA to develop information gathering priorities or requirements.	NCTC products form the foundation of informational needs and guide collection of additional information. NCTC products should be responsive to informational needs of State, local, and tribal entities.

⁹ NCTC product include: Alerts, warnings, and notifications—identifying time sensitive or strategic threats; Situational awareness reports; and Strategic and foundational assessments of terrorist risks and threats to the United States and related intelligence information.

UNCLASSIFIED

ISE-FS-200

Step	Activity	Process	Notes
9	Focused Collection	The information has come full circle and the process begins again, informed by an NCTC or other Federal organization's product and the identified information needs of State, local and tribal entities and Federal field components.	

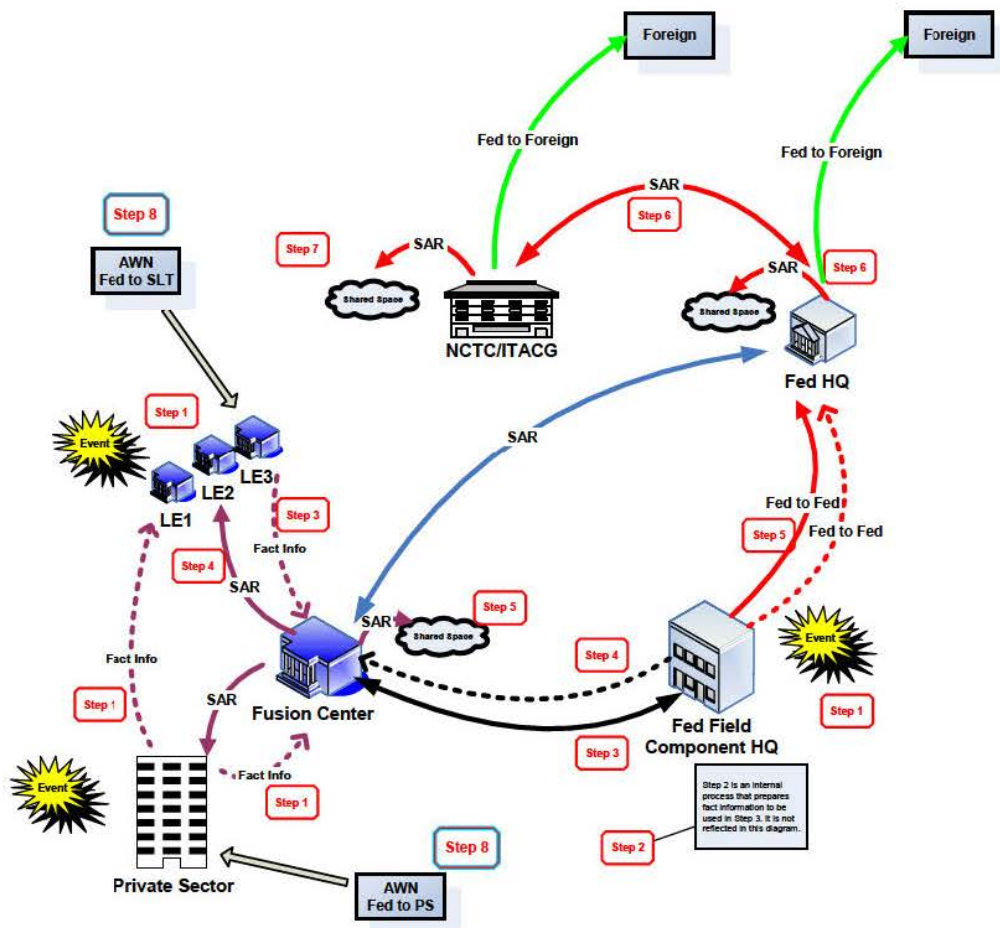


Figure 4 – SAR Information Flow Diagram

**INFORMATION SHARING ENVIRONMENT –
SUSPICIOUS ACTIVITY REPORTING FUNCTIONAL STANDARD
AND EVALUATION ENVIRONMENT**

Initial Privacy and Civil Liberties Analysis

September 2008—Version 1

Initial Privacy and Civil Liberties Analysis

Purpose

This analysis has been prepared for the purpose of conducting an initial examination of the privacy and civil liberties ramifications of the Information Sharing Environment – Suspicious Activity Reporting (ISE-SAR) Functional Standard and included Information Exchange Package Documentation (IEPD) component¹ and of the vision for deploying these in operating environments (ISE-SAR Evaluation Environment initiative), making recommendations to address issues identified as a result of the examination, and identifying policies and safeguards that should be implemented at the preliminary stages of this process. The overarching purpose of this analysis—as with all activities conducted in protecting the Nation from terrorism—is to help ensure those carrying out the activities contemplated by these plans do so in a manner that fully protects the legal rights of all United States persons, including information privacy, civil rights, and civil liberties guaranteed by the Constitution and laws of the United States.

Background

The Office of the Program Manager for the Information Sharing Environment (PM-ISE)—in consultation with the Civil Liberties and Privacy Office of the Office of the Director of National Intelligence (ODNI), the Office of Privacy and Civil Liberties of the Department of Justice (DOJ), and the Legal Issues Working Group of the ISE Privacy Guidelines Committee (PGC)—has prepared this Initial Privacy and Civil Liberties Analysis of the ISE-SAR Functional Standard and included IEPD component (ISE-FS-200).

This analysis consists of (i) an explanation of the ISE-SAR Functional Standard and associated IEPD components and plans to test the ISE-SAR Functional Standard at various sites, (ii) questions and answers exploring the privacy and civil liberties ramifications of the ISE-SAR data exchange model and of implementing the ISE-SAR initiative in the field, and (iii) conclusions and recommendations identifying key information privacy and civil liberties concerns that entities participating in the ISE-SAR Evaluation Environment initiative should address as they implement ISE-SAR sharing activities. This is an interim privacy and civil liberties analysis that will be updated as more information is obtained during the ISE-SAR Evaluation Environment initiative, including lessons learned from participants and feedback received from privacy and civil liberties advocates and other interested parties. Because the authors have conducted this analysis in order to help guide participants as they prepare key program documentation, the analysis and recommendations are necessarily general in nature.

The ISE-SAR Functional Standard and the IEPD are designed to enable a federated search of terrorism-related SARs originating at all levels of government. The search will occur within an unclassified information or controlled unclassified information (CUI) sharing environment. As the ISE-SAR Functional Standard deploys to the field, using the ISE Shared Space model

¹ The ISE-SAR Functional Standard was developed and released by the Office of the Program Manager for the Information Sharing Environment (PM-ISE) on January 25, 2008. The ISE-SAR Functional Standard constitutes the first of the Common Terrorism Information Sharing Standards (CTISS). More information on the CTISS Program can be found at <http://www.ise.gov/pages/ctiss.html>.

Initial Privacy and Civil Liberties Analysis

(explained below) at various proposed ISE-SAR Evaluation Environment sites, the authors of this report will work with the ISE-SAR Evaluation Environment sites to review and advise regarding the impact of ISE-SAR information sharing on the information privacy, civil rights, and civil liberties of Americans. Based on the experiences documented by the ISE-SAR Evaluation Environment sites, the PM-ISE, in consultation with the ODNI's Civil Liberties and Privacy Office, DOJ's Office of Privacy and Civil Liberties, and the ISE PGC's Legal Issues Working Group, will generate a Final ISE-SAR Privacy and Civil Liberties Analysis identifying how the various ISE-SAR Evaluation Environment sites, in implementing the ISE-SAR Functional Standard, addressed the "key issue" recommendations outlined below were addressed. This compilation of practices and experience from the ISE-SAR Evaluation Environments will inform future revisions to the ISE-SAR Functional Standard.

Introduction

On October 31, 2007, President George W. Bush issued the initial National Strategy for Information Sharing (NSIS) to prioritize and unify the Nation's efforts to advance the sharing of terrorism-related information among Federal, State, local, and tribal Governments, private sector entities, and foreign partners. The NSIS calls, in part, for the Federal Government to support a nationwide capability for the gathering, analysis, and sharing of information, including suspicious activity and incident reporting related to terrorism, with State, local, and tribal Governments and across the Federal Government. Consistent with the NSIS, and as a priority for the establishment of the Information Sharing Environment (ISE), the PM-ISE has helped coordinate a comprehensive effort to develop a nationwide network of state, regional, and major urban area fusion centers that will facilitate the sharing of terrorism-related information across the local, state, tribal, and federal communities. The ISE-SAR Functional Standard was developed and released by the PM-ISE on January 25, 2008, to specifically address the sharing of terrorism-related suspicious activity reports (hereinafter ISE-SAR information or ISE-SARs), with the overarching goal of enabling analysts and officers with counterterrorism responsibilities at all levels of government to discover and identify terrorist activities and trends.

The ISE-SAR Functional Standard (at "Definitions," Section 5 (g) of PM-ISE Memorandum, January 25, 2008) defines the term "suspicious activity report" (SAR) as "any official documentation of observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention."² The documenting of suspicious activity is well institutionalized in the law enforcement community, where federal and state, local, and tribal (SLT) agencies collect and document suspicious activities in support of their responsibilities to investigate and prevent potential crimes, protect citizens, and apprehend and prosecute criminals. Such reporting occurs with varying degrees of

² *Ballantine's Law Dictionary*, 1969, defines "illicit" as "unlawful, illegal, prohibited or forbidden by law." Because terrorism is defined as a criminal act, the suspicious behavior underlying an ISE-SAR must demonstrate a nexus to criminal activity or intent, as opposed to non-criminal, but illicit, activity or intent. This is further discussed in the Privacy and Civil Liberties Analysis Section, Q&A 1.

Initial Privacy and Civil Liberties Analysis

standardization and formality in other communities as well (intelligence, defense, homeland security), where entities document observed or reported suspicious activity as part of their mission or for the purpose of protecting personnel and facilities. In all of these arenas, some of the documented activities may bear a potential nexus to terrorism. In accordance with the NSIS, which identifies suspicious activity reports as one of the key information exchanges to be effected between the Federal and SLT Governments, the PM-ISE developed a standardized process (and associated data model) for identifying, documenting, and sharing ISE-SAR information to the maximum extent possible consistent with the protection of privacy and civil liberties.

The ISE-SAR Functional Standard envisions that agencies will share potential ISE-SAR information with a state or major urban area fusion center and, when appropriate and consistent with existing practice, the local FBI Joint Terrorism Task Force (JTTF). At the fusion center, analysts or law enforcement officers will evaluate the SAR against the ISE-SAR Functional Standard. If the SAR meets criteria as defined in the ISE-SAR Functional Standard, the fusion center will designate the SAR as an "ISE-SAR" and make it available to other ISE participants through the fusion center's Shared Space. Documenting, analyzing, and sharing of ISE-SAR information between and among SLT entities, state or major urban area fusion centers, JTTFs, and federal field components is designed to enable the identification of behaviors and indicators of criminal activity associated with terrorism.

Summary of the SAR Functional Standard for the ISE

The ISE-SAR Functional Standard

The ISE-SAR Functional Standard provides an important mechanism for representing details about terrorism-related suspicious activity in a consistent manner to help facilitate the identification of useful investigatory or trending information. The ISE-SAR Functional Standard is not intended to prescribe all processes, systems requirements, or other business rules governing the collection, processing, or sharing of SARs by law enforcement entities. The diverse entities that generate and use SARs have well-established processes and business rules for suspicious activity reporting.

The ISE-SAR Functional Standard sets forth a two-part "integration/consolidation" process for identifying, out of the thousands of suspicious activities documented through "organizational processing" activities conducted by source agencies each day, those that have a potential nexus to terrorism. The first step in the process of identifying an ISE-SAR is for a trained analyst or law enforcement officer at a fusion center, or JTTF, to determine whether suspicious activity falls within any of the criteria set forth in Part B – ISE-SAR Criteria Guidance of the ISE-SAR Functional Standard. These criteria describe behaviors and incidents identified by law enforcement officials and counterterrorism experts from across the country as being indicative of criminal activity associated with terrorism. The second step in the process is for a trained expert to determine, based on a combination of knowledge, experience, available information, and, importantly, personal judgment, whether the information has a potential nexus to

Initial Privacy and Civil Liberties Analysis

terrorism. When suspicious activity is determined to have a potential nexus to terrorism, fusion center personnel will document it in the data format and schema (information exchange package documentation) prescribed by the standard and make it available to all appropriate ISE participants in the Shared Space.

Thus, the implementation of the ISE-SAR Functional Standard is designed as a tool to enable fusion centers and federal agencies to build upon and optimize reporting activities already taking place at the SLT and federal levels. The ISE-SAR Functional Standard will be implemented for evaluation purposes at diverse ISE-SAR Evaluation Environment sites, including major city and other police departments and state and major urban area fusion centers. However, numerous privacy and civil liberty concerns arise when information regarding suspicious activities associated with terrorism is shared between federal and SLT authorities. The ISE-SAR Evaluation Environment initiative will address these concerns through the development and application of appropriate privacy, civil rights, and civil liberties protection policies and procedures.

The Information Exchange Package Documentation

The ISE-SAR Functional Standard is intended to support broad dissemination of ISE-SARs and sharing of the maximum relevant information. To facilitate this dissemination and sharing, two different data formats (information exchange packages) have been developed for packaging ISE-SAR information. The **Detailed format** includes information contained in all data elements set forth in Section IV of the ISE-SAR Functional Standard (“ISE-SAR Exchange Data Model”), including fields denoted as privacy fields. “Privacy fields” contain personal information that can be used to identify individual subjects, either alone or in combination with other information. The **Summary format** excludes fields or data elements identified as privacy fields in Part A – Section IV.³ The ISE-SAR Functional Standard identifies the minimum privacy fields that must be excluded from a Summary ISE-SAR. Each ISE participant may exclude additional privacy fields from its Summary ISE-SARs, in accordance with its own statutory or policy requirements. The goal is for ISE-SARs to be shared, to the maximum extent possible, among SLT and federal law enforcement, homeland security, and other appropriate organizations participating in the ISE while protecting information associated with the designated privacy fields.

ISE-SAR Evaluation Environment

ISE-SAR Functional Standard/IEPD Evaluation Environment Goals

To test the assumption that the ISE-SAR Functional Standard will facilitate the sharing of terrorism-related SAR information across multiple domains and levels of government, the PM-ISE, in concert with its federal partners and national associations of law enforcement

³ Because both Detailed and Summary formats contain contact information for the source organization, recipients of the Summary format could contact the source organization for additional information, as appropriate.

Initial Privacy and Civil Liberties Analysis

identification and designation of ISE-SARs. As appropriate, the next version of the ISE-SAR Functional Standard will be modified to reflect any changes in process and data format that are identified as necessary in the course of testing the ISE-SAR Functional Standard at the various Evaluation Environment sites.

4. How is the designation of an ISE-SAR made and by whom?

The ISE-SAR Functional Standard indicates the designation of an ISE-SAR as a two-part process (see Part C – ISE-SAR Information Flow Description, Step 4). First, at the state or major urban area fusion center or federal agency, a trained analyst or law enforcement officer reviews the newly reported information against ISE-SAR criteria (Part B of the ISE-SAR Functional Standard). Federal agency personnel with law enforcement or intelligence responsibilities, to include officials from DHS' Office of Intelligence and Analysis and the FBI, may be collocated or deployed to fusion centers and may participate in the review and designation of ISE-SARs at the fusion center level. Second, based on available information, knowledge and experience, the analyst or law enforcement officer determines whether the information may have a nexus to terrorism (i.e., the SAR information has been identified as potentially terrorism-related). (see ISE-SAR Functional Standard at C3.) The process requires human interaction and judgment and is not performed automatically by computer software. An ISE-SAR is created and shared with appropriate ISE participating organizations only when a trained expert has determined that the information meeting the criteria has a potential nexus to terrorism.¹⁶

The ISE-SAR Functional Standard does not prescribe processes at the source agency level to ensure that SAR information received is legally obtained and that suspicious incidents and activities are properly identified as having a potential terrorism nexus. Nor does the ISE-SAR Functional Standard provide more detailed guidance on how to apply the criteria in Part B. Those criteria are intended to be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention. Focusing attention on observable behaviors is important for intelligence purposes, as well as to avoid inappropriate reporting. The criteria, however, are general in nature, and while they may indeed be indicative of such intelligence gathering or pre-operational planning, they may also apply to innocent behavior. The purpose of requiring a separate determination, based on available information, knowledge and experience, that the SAR information is potentially terrorism-related, is to avoid a mechanical or automatic application of the Part B criteria to otherwise innocent behavior. However, more guidance on how to apply the Part B criteria to avoid over-inclusiveness, and to guard against inappropriate reporting, is important.

The authors of this report recommend that training programs and guidance documentation be developed on how to apply the Part B criteria to minimize the risks of over-inclusiveness and

¹⁶ In addition to evaluating the ISE-SAR Functional Standard, the Evaluation Environment project will also evaluate the utility of creating and making accessible a library of Summary SARs that may have a nexus to terrorism. The Summary SARs Library will contain a mix of SARs (both terrorism-related and non-terrorism related) in free text format. These Summary SARs are completely anonymous (i.e., all privacy information is removed).

Initial Privacy and Civil Liberties Analysis

As part of the Evaluation Environment effort, consistent with the Data Quality provision of the ISE Privacy Guidelines, sites will be asked to develop specific data quality and redress processes for correcting or purging information discovered or reported to be inaccurate. The authors of this report recommend that sites implement business processes, including steps to vet or validate the accuracy of observations, tips, leads, or other incident reporting and to remove from, or update in, an ISE Shared Space any ISE-SAR determined to be deficient or unfounded (e.g., redress) (see Recommendation B(1)(b)).

The authors of this report recommend that the ISE-SAR Evaluation Environment sites, under the CONOPS, require source agencies documenting suspicious activity to assess their confidence in the information they report, including source reliability and content validity (see Recommendation B(1)(g)). The assessment may rely on factors such as demeanor (e.g., intoxication level, mental state), credibility (based on prior experience, interview), or other indicia of reliability and validity. The assessed level of confidence will enable the fusion center or other recipient organizations to better gauge the value of the information to be designated an ISE-SAR and to ensure against erroneous reports or reports potentially motivated by racial, religious, or other animus. While no policy can completely eliminate the risk of such bias, responsible processes to validate and review possible suspicious activities before such activities are formally documented may reduce such risks. Repeated examination improves the quality of the information and also protects the information privacy and other legal rights of Americans.

9. What legal authorities govern the original collection of the information by government entities? Is “reasonable suspicion” required?

In order for documentation of suspicious activity to be considered an ISE-SAR under this Functional Standard, it must relate to “terrorism, criminal, or other illicit [i.e., illegal]¹⁷ intention.” Each government entity that collects and documents suspicious activities at the federal or SLT level must do so in accordance with applicable law and policy. Nothing in the ISE-SAR Functional Standard alters this fundamental requirement.

The determination to document a suspicious incident as an ISE-SAR cannot be based solely on a subject’s race, ethnicity, national origin, religious preference or the exercise of First Amendment or other constitutional rights. In addition, for federal agencies, the Privacy Act of 1974 prohibits the collection and maintenance of information in these categories except to the extent that the information is pertinent to and within the scope of an authorized law enforcement activity (5 U.S.C. 552a(e)(7)). Only reports of conduct consistent with criminal activities associated with terrorism, and regarding subjects whose potential involvement in that criminal activity cannot be discounted, will be designated an ISE-SAR. Absent a determination that a potential nexus to terrorism exists, the information will not become the subject of an ISE-SAR. The authors of this report recommend that business processes be implemented to incorporate training and guidance to implement these safeguards into the SAR process. (See Recommendations B(1)(b)

¹⁷ See Recommendation B(3)(c).

Initial Privacy and Civil Liberties Analysis

and B(3)(a)). These safeguards are intended to ensure that information, consideration of which could violate an individual's privacy, civil rights, and civil liberties by unjustifiably associating him/her with terrorism, will not be intentionally or inadvertently gathered, documented, or processed as an ISE-SAR and shared through the ISE.

"Reasonable suspicion" is not a separate requirement of the ISE-Functional Standard. The ISE-Functional Standard is based on the premise that agencies will generate SARs based on applicable laws and policies in their jurisdictions, and that the ISE-Functional Standard will then standardize the process for determining when a SAR has a potential terrorism nexus, and will provide the relevant data format and elements. It was not originally intended to address the legal standard to be used by each federal, state, local, and tribal entity for determining what level of evidence or certainty is necessary or sufficient for submitting a SAR. The authors of this report acknowledge that questions arise as to whether a SAR should meet the "reasonable suspicion" standard established for Criminal Intelligence Systems under 28 C.F.R. Part 23, and support the privacy and civil liberties finding and recommendation in *Findings and Recommendations of the SAR Support and Implementation Project*, that agencies should clearly articulate when 28 C.F.R Part 23 should be applied. The business processes, training, and documentation identified in this analysis provide additional safeguards for ISE-SARs. For example, the CONOPS will require the ISE-SAR Evaluation Environment sites to recognize only those inquiries that provide a case, incident, or other justification (see Recommendation B(1)(I)) – the justification for disclosing certain information could be a particularized showing, subject to audit, designed to avoid privacy and civil liberties harm to the individual. The authors of this report will continue to evaluate how to address privacy and civil liberties concerns of this type throughout the course of the Evaluation Environment.

10. Is the information subject to retention limits?

Each government entity that obtains and documents information concerning suspicious activities at the federal or SLT levels may retain such information only in accordance with applicable law and policy. Retention limits, if any, can vary significantly across ISE participant organizations and may depend upon the type of information contained in the ISE-SAR. For SLT law enforcement, ISE-SAR information is considered fact-based information rather than criminal intelligence and may be subject to the requirements of 28 CFR Part 23. If an ISE-SAR also meets 28 CFR Part 23 criteria, it may be submitted to a criminal intelligence information database, and the information in the criminal intelligence system would be subject to the five-year review and validation/purge requirement under 28 CFR Part 23.¹⁸ (Note that a state law, municipal code, or department policy may impose a more restrictive retention requirement on criminal intelligence information.) However, as a SAR, its retention would continue to be governed by state law, municipal ordinance, or agency policy.

¹⁸ At the time of this writing, 28 CFR Part 23 is currently under revision and the noted five-year review timeframe may change.

Initial Privacy and Civil Liberties Analysis

Detailed ISE-SARs privacy field information that cannot be provided to other users or classes of users. The submitting organization will ensure that its own ISE Shared Space system accommodates applicable privacy and other legal requirements.

As it relates to the ISE-SAR Evaluation Environment initiative, the sharing of ISE-SARs will take place between law enforcement, homeland security, public safety, and other credentialed personnel. The expectation is to share non-privacy related ISE-SAR information to the maximum extent through the Summary ISE-SAR format, while making available the Detailed ISE-SAR where appropriate and necessary, and subject to applicable legal and policy limits. The ISE Privacy Guidelines and any further guidance issued by the PM-ISE or the ISE Privacy Guidelines Committee also potentially govern the sharing of ISE-SARs.

Longstanding policies and rules governing how law enforcement information is shared with the Intelligence Community will be applied when determining how ISE-SARs will be made available to members of the Intelligence Community.

17. With whom (agencies, organizational elements, and personnel) is a Summary ISE-SAR shared?

The expectation is that Summary ISE-SARs shall be available via the agency SAR system or Shared Space to authorized personnel at all ISE participating organizations.

18. How will access to ISE-SARs be authorized and by whom?

See Q&A #14. The ISE-SAR Functional Standard contains a "Dissemination Description Code" (generally established locally) that permits the submitting organization to specify "who gets what." This code enables the submitting organization to limit the recipients of the ISE-SAR, based on applicable governing authorities. In the long term, the intent is to establish an ISE-wide system of attribute-based access controls that would manage access authorization based on the class or operational role of the ISE participant requesting access. Under such a system, it would be possible, for example, to grant full access (including privacy fields) to one set of users, where such users have a need for such fields, partial access (entire ISE-SAR minus privacy fields), or, in some cases, no access to ISE-SARs. Realization of this goal will require the development and issuance of common access standards and requirements across the ISE.

19. Are there use restrictions on ISE-SARs? Describe all uses of the data.

The ISE-SAR Functional Standard was not intended to cover restrictions on how ISE-SARs will be used once the information was inputted and formatted in accordance with the standard.

The ISE-SAR Evaluation Environment will contain use restrictions. As provided in the ISE-SAR Evaluation Environment CONOPS under development, ISE-SARs will be used only to support U.S. law enforcement (LE) and counterterrorism (CT) activities.

Initial Privacy and Civil Liberties Analysis

Authorized LE and CT uses include:

- **Investigation.** ISE-SARs can be used to support criminal investigations of possible terrorist activities by federal, state, and local law enforcement officers.
- **Analysis.** ISE-SARs are one source of information that analysts use to develop and issue terrorist threat reports for LE and CT activities. Analysts may use information from a number of sources in producing alerts, warnings, and notifications; situational awareness reporting; or strategic threat or risk assessments.
- **Information Needs.** ISE-SARs may be used to help develop priority information needs.

At SLT levels, the use and sharing of information for each of these purposes is governed by agency policy, municipal codes, state and tribal laws and constitutions, and the U.S. Constitution.

In its final draft report, the *SAR Support and Implementation Project*¹⁹ finds and recommends that participating agencies and entities should evaluate and update their privacy and civil liberties policies and related training to ensure that the information privacy, civil liberties, and other legal rights of Americans are protected in the use of SAR data. (See Recommendation B(2)(b))

To the extent that information contained in ISE-SARs, or that is derived from ISE-SARs, is made available to agencies within the Intelligence Community (IC), such information could be used, to the extent it contains U.S. person information, only in a manner consistent with the relevant agency's Attorney General-approved guidelines pursuant to Executive Order 12333. IC agencies should note that even Summary ISE-SARs may contain information identifying a U.S. organization or corporation. In addition, while ISE-SARs have been determined to have a nexus to terrorism, no determination has been made that such SARs are related to international terrorism (because homeland security information and law enforcement information related to terrorism, unlike "terrorism information" as defined for the ISE, need not be related to international terrorism). Thus ISE-SARs do not necessarily constitute foreign intelligence or counterintelligence information, the necessary threshold criterion for collection by an IC element.

Moreover, separate criteria exist for nominating individuals to the U.S. Government's Consolidated Terrorist Watch List. That watch list is administered by the Terrorist Screening Center of the FBI. An ISE-SAR is not a basis for placing an individual on the watch list.

The authors of this report recommend that business processes be developed to implement user restrictions for ISE-SARs. In particular, program documentation and business processes must make clear that documentation of information in an ISE-SAR cannot be used as the sole basis for action to be taken against an individual. ISE-SARs are for lead purposes only, and remain subject to all applicable laws and policies. Users of ISE-SARs should be trained on the inherent limitations of such information, and appropriate notices should be put in place advising users

¹⁹ The final draft can be found at <http://online.wsj.com/public/resources/documents/mccarecommendation-06132008.pdf>.

Initial Privacy and Civil Liberties Analysis

of such limitations (e.g., appropriate use-limitation markings could be placed on ISE-SAR documents; use-limitation notice screens could be used on ISE-SAR shared spaces) (see Recommendation B(1)(k)).

20. Does maintaining ISE-SARs in an ISE Shared Space create a Privacy Act system of records? If so, is there a routine use that covers sharing with relevant ISE participants?

Depending upon how the SAR systems or ISE Shared Spaces are implemented by the ISE participants, maintenance of ISE-SARs on such ISE Shared Spaces by federal entities may create a system of records under the Privacy Act, the existence and character of which must be published in the Federal Register. A Privacy Act “system of records” is a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, etc. Each federal ISE participant organization that administers a Detailed ISE-SAR Privacy Act system of records in its SAR system or ISE Shared Space must develop and publish a “routine use,” which authorizes it to disclose ISE-SAR information outside the agency. A routine use is a published statement by an agency that articulates, with respect to one or more system of records, to whom and for what purpose information from individuals’ Privacy Act records may be disclosed outside the agency.

21. Will there be a mechanism or requirement to notify the submitting organization of information believed to be inaccurate or information improperly designated as an ISE-SAR so that corrective action can be taken?

Currently, the process envisioned for notifying either the source organization or the submitting organization of information that may be inaccurate or improperly designated as having a terrorism nexus is set forth in Section 5b of the ISE Privacy Guidelines:

Notice of Errors. Each agency, consistent with its legal authorities and mission requirements, shall ensure that when it determines that protected information originating from another agency may be erroneous, includes incorrectly merged information, or lacks adequate context such that the rights of the individual may be affected, the potential error or deficiency will be communicated in writing to the other agency’s ISE privacy official...

Each entity participating in the ISE-SAR Evaluation Environment will be required to adopt an appropriate policy for error notification (as well as policies ensuring other privacy protections, as set forth in the ISE Privacy Guidelines). Feedback mechanisms may be kept simple, employing either telephone or e-mail.

Initial Privacy and Civil Liberties Analysis

must comply with the requirements of the Privacy Act to establish a Privacy Act System of Records Notice (see Q&A #20).

26. Can ISE-SAR data be merged with data from another system (e.g., reverse telephone directory)?

The ISE-SAR Functional Standard does not dictate how ISE-SAR data will be merged with data from other systems.

In the current ISE-SAR Evaluation Environment initiative, the answer is “no.” For example, while a fusion center could make a reverse telephone directory available for analytic or investigative use, separate from the ISE-SAR Evaluation Environment, the directory capability would not be integrated into the ISE-SAR Evaluation Environment. In the future, any merging of ISE-SAR data with data from other systems will be fully assessed in terms of business rules and privacy and civil liberties protections, including the merger provision of Section 5c.(i) of the ISE Privacy Guidelines.

27. Will analysis be conducted as part of the ISE-SAR Evaluation Environment initiative?

One of the purposes of developing the ISE-SAR Functional Standard and an integrated ISE-SAR process is to allow authorized ISE participants to identify and analyze incidents and observations that, taken together, may provide indicators of terrorist plans or activities. This analysis would be done locally by analysts. To this end, the ISE-SAR Functional Standard standardizes the format and content of an ISE-SAR. However, development and use of specific tools and techniques to support pattern and trend analysis are not part of the ISE-SAR process. ISE participants may employ local tools or techniques as appropriate. The ISE-SAR Evaluation Environment initiative is designed to provide controlled access to ISE-SAR information hosted by a state or major urban area fusion center through a federated search capability. A federated search allows a user to search all available data repositories for which they are authorized for specific information via a single search interface. The single federated search interface should allow a user the ability to formulate a query based on a set of parameters and subsequently narrow the search through more specific parameter refinement. Pursuant to the ISE-SAR Functional Standard, search results will be structured in the IEPD format so that such results may also be processed in other applications used by the analyst. The functionality may include a link analysis tool. To conduct a link analysis, users must separately enter their ISE-SAR search results into whatever software they have that enables that type of analysis.

28. What type of training will be required for users of the data?

The authors of this report recommend that users of ISE-SARs receive training about the basic ISE-SAR business process; the ISE-SAR information flow description (Part C of ISE-FS-200); guidance on the criteria for designating an ISE-SAR (Part B of ISE-FS-200); application of the ISE

Initial Privacy and Civil Liberties Analysis

Privacy Guidelines to the ISE-SAR business process and, as appropriate, guidance on other privacy and civil liberties implications of the ISE-SAR process (e.g., racial, ethnicity, national origin, or religion-based profiling concerns and other constitutional rights issues). (See Recommendations B(1)(a) and B(3)(a).) ISE-SAR training will be developed through the ISE-SAR governance structure. The ISE-SAR governance structure will be detailed in the CONOPS.

29. What auditing and technical safeguards are in place to prevent misuse of the data?

The ISE-SAR Functional Standard standardizes the format and content of an ISE-SAR but does not address the auditing and technical safeguards applicable to agencies' SAR systems or ISE Shared Spaces. These safeguards and procedures, such as retention of inquiry and access log data and frequency of audits, vary from state-to-state, agency-to-agency, and department-to-department. Accordingly, consistent with paragraph 11 of the ISE Privacy Guidelines, the authors of this report recommend that the CONOPS for the ISE-SAR Evaluation Environment require the Evaluation Environment sites to establish and implement auditing and technical safeguard requirements that are as comprehensive as those required by the ISE Privacy Guidelines (see Recommendations A(5) and B(1)(i)).

30. Is there a requirement to notify the submitting agency prior to further disclosure of the ISE-SAR?

The ISE-SAR Functional Standard does not embrace operational, on-the-ground, sharing practices by participating agencies. Initially, for purposes of the ISE-SAR Evaluation Environment initiative, access to information in the participants' ISE Shared Spaces will be based on a case, incident, or other justification; limit the number of records that can be accessed in response to the inquiry; and, permit "read only" access. However, in the future, if ISE participating organizations are authorized to access and incorporate data from other entities into their own databases, or collaborate by providing input to submitting agency ISE-SARs, the development of business rules for such sharing or record modification will need to be addressed. The CUI framework may govern secondary disclosure in some circumstances.

Summary

To enhance the utility of terrorism-related suspicious activity and incident reporting, both practically and analytically, the ISE-SAR Functional Standard provides a framework for the standardized documenting of ISE-SARs that are intended to be disseminated to ISE participants. Broad adoption of the ISE-SAR Functional Standard will facilitate increased ISE-SAR sharing, making protection of privacy and civil liberties critical to the ISE-SAR Evaluation Environment initiative.

That the ISE-SAR Functional Standard establishes a convention for representing ISE-SAR information using common criteria and data elements is both its strength and weakness from a privacy and civil liberties protection perspective. The ISE-SAR Functional Standard does not

Initial Privacy and Civil Liberties Analysis

prescribe the business rules (processes and procedures) that source organizations must follow for collecting, analyzing, maintaining, or sharing ISE-SAR data; these procedures and analytical processes remain organization-specific. Accordingly, the foregoing Q&A section identifies those areas where ISE-SAR entities must develop business rules and examine the attendant privacy and civil implications of proposed operational choices.

Recommendations

A. General

The authors of this report support the privacy and civil liberties measures recommended in the *Findings and Recommendations of the SAR Support and Implementation Project*. Based on site visits to and evaluations of the model of the LAPD and police departments in Boston, Chicago, and Miami, the *Findings and Recommendations of the SAR Support and Implementation Project* urge entities engaged in SARs activities to consider the following measures:

1. Promote a policy of openness and transparency when communicating to the public regarding their SAR process;
2. Integrate the management of terrorism-related suspicious information with processes and systems used to manage other crime-related information and criminal intelligence, thereby leveraging existing policies and protocols that protect the information privacy, civil liberties, and other legal rights of Americans; clearly articulate when 28 CFR Part 23 should be applied;
3. Ensure privacy and civil liberties policies address core privacy principles, such as accuracy, redress, retention/disposition, and disclosure of personally identifying information, consistent with federal, state, and local statutory and regulatory requirements;
4. Evaluate and, as necessary, update privacy and civil liberties policies to ensure that they specifically address the gathering, documenting, processing, and sharing of terrorism-related information;
5. Audit SARs for quality and substance to ensure that the integrity of the SAR program is maintained; and,
6. Use legal and privacy advisors in the development of the SAR process.

B. ISE-SAR Evaluation Environment

The authors of this report recommend that the program documentation for the ISE-SAR Evaluation Environment initiative (i.e., CONOPS, program guidance, participation agreements) require, as appropriate to the purpose and audience for each document, the following specific measures addressing “key” privacy and civil liberties issues:

**Feedback Session with Privacy and Civil Liberties Advocates:
Suspicious Activity Reporting (SAR) Line-Officer Training and
the ISE-SAR Functional Standard**

1:00 p.m. – 4:00p.m.

Wednesday, February 18, 2009

Office of the Program Manager, Information Sharing Environment
2100 K St, NW Suite 300, Washington, DC

AGENDA

Welcome and Introductions

██████████, Deputy Program Manager, Information Sharing Environment (ISE)

SAR Line Officer Training Demonstration

██████████ Senior Advisor, ISE

Discussion on Training

ALL

Overview of Functional Standard

██████████, ISE

Discussion on Criteria

ALL

Closing Roundtable Comments – 10 minutes

ALL

Next Steps

██████████, Senior Advisor, ISE

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
PROGRAM MANAGER, INFORMATION SHARING ENVIRONMENT
WASHINGTON, DC 20511

May 21, 2009

MEMORANDUM FOR HEADS OF DEPARTMENTS AND AGENCIES

SUBJECT: Release of the Information Sharing Environment (ISE) Functional Standard for Suspicious Activity Reporting, Version 1.5 (ISE-FS-200)

REFERENCE: 1) Presidential Memorandum of December 16, 2005, subject: Guidelines and Requirement in Support of the Information Sharing Environment
2) National Strategy for Information Sharing, October 2007

On January 25, 2008 I issued the first Common Terrorism Information Sharing Standard (CTISS) for Suspicious Activity Reporting (SAR) in accordance with Presidential Memorandum directing the development and issuance of common standards governing how terrorism information is acquired, accessed, shared, and used within the ISE. This updated version of the *ISE-SAR Functional Standard* incorporates suggestions provided by federal privacy and civil liberties attorneys and members of the privacy and civil liberties advocacy community, and:

- Refines the definition of Suspicious Activity as, “*observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.*”
- Clarifies that the same constitutional standards that apply when conducting ordinary criminal investigations also apply to law enforcement and homeland security officers conducting SAR inquiries.
- Further emphasizes a behavior-focused approach to identify suspicious activity and requires that factors such as race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion (except if used as part of a specific suspect description).
- Refines the ISE-SAR Criteria Guidance to distinguish between those activities that are Defined Criminal Activity and those that are Potentially Criminal or Non-Criminal Activity requiring additional fact information during investigation.
- Clarifies those categories of activity which are generally First Amendment-protected activities should not be reported in a SAR or ISE-SAR absent articulable facts and circumstances that support the source agency’s suspicion that the behavior observed is reasonably indicative of criminal activity associated with terrorism.
- Updates the operational process descriptions to align the standard with the *Nationwide SAR Initiative Concept of Operations*, released in December 2008.

All CTISS, to include this *ISE-SAR Functional Standard*, will be implemented by ISE participants into supporting infrastructures in accordance with the *ISE Enterprise Architecture*

Framework. This *ISE-SAR Functional Standard* is also in alignment with the *National Strategy for Information Sharing (NSIS)*, which outlines federal, state, local, and tribal responsibilities for sharing ISE-SAR data.

This *ISE-SAR Functional Standard* documents information sharing exchanges and business requirements, and describes the structure, content, and products associated with processing, integrating, and retrieving ISE-SAR by ISE participants. Each Information Sharing Council (ISC) member and other affected agencies responsible for the collection and processing of SARs with a nexus to terrorism must apply this Functional Standard when processing, integrating, and retrieving ISE-SAR, and incorporate this Functional Standard into their business processes development and information resource planning. In particular, ISC agencies should, as appropriate, incorporate this *ISE-SAR Functional Standard* and any subsequent implementation guidance into budgetary planning activities associated with current (operational) and future development efforts associated with relevant mission-specific programs, systems, or initiatives. As appropriate, departments and agencies may consider utilizing this standard as part of the grant application process.

This updated version of the *ISE-SAR Functional Standard* will continue to be tested and evaluated by the user community. Any resulting refinements, including changes to SAR business processes and data elements, will be incorporated in future versions. Privacy assessments will also be performed as appropriate to identify privacy issues that may arise in implementing this *ISE-SAR Functional Standard* and information flow. This *ISE-SAR Functional Standard* is not intended to address all the implementation issues associated with the reporting, tracking, processing, accessing, storage, and retrieval of SAR information within the ISE; it is one component of the overall Nationwide SAR Initiative.

Please address any questions associated with this *ISE-SAR Functional Standard* to your designated ISC Representative (Attachment B) or the Office of the Program Manager.



Thomas E. McNamara

Attachments:

- A. Information Sharing Environment (ISE) Functional Standard (FS) for Suspicious Activity Reporting (SAR), Version 1.5 (ISE-FS-200)
- B. Information Sharing Council Members
- C. Fact Sheet: Update to Suspicious Activity Reporting Functional Standard Provides Greater Privacy and Civil Liberties Protections

cc: Information Sharing Council

UNCLASSIFIED

ISE-FS-200

INFORMATION SHARING ENVIRONMENT (ISE)
FUNCTIONAL STANDARD (FS)
SUSPICIOUS ACTIVITY REPORTING (SAR)
VERSION 1.5

1. Authority. Homeland Security Act of 2002, as amended; The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended; Presidential Memorandum dated April 10, 2007 (Assignment of Functions Relating to the Information Sharing Environment); Presidential Memorandum dated December 16, 2005 (Guidelines and Requirements in Support of the Information Sharing Environment); DNI memorandum dated May 2, 2007 (Program Manager's Responsibilities); Executive Order 13388; and other applicable provisions of law, regulation, or policy.
2. Purpose. This issuance serves as the updated Functional Standard for ISE-SARs, and one of a series of Common Terrorism Information Sharing Standards (CTISS) issued by the PM-ISE. While limited to describing the ISE-SAR process and associated information exchanges, information from this process may support other ISE processes to include alerts, warnings, and notifications, situational awareness reporting, and terrorist watchlisting.
3. Applicability. This ISE-FS applies to all departments or agencies that possess or use terrorism or homeland security information, operate systems that support or interface with the ISE, or otherwise participate (or expect to participate) in the ISE, as specified in Section 1016(i) of the IRTPA.
4. References. ISE Implementation Plan, November 2006; ISE Enterprise Architecture Framework (EAF), Version 2.0, September 2008; Initial Privacy and Civil Liberties Analysis for the Information Sharing Environment, Version 1.0, September 2008; ISE-AM-300: Common Terrorism Information Standards Program, October 31, 2007; Common Terrorism Information Sharing Standards Program Manual, Version 1.0, October 2007; National Information Exchange Model, Concept of Operations, Version 0.5, January 9, 2007; 28 Code of Federal Regulations (CFR) Part 23; Executive Order 13292 (Further Amendment to Executive Order 12958, as Amended, Classified National Security Information); Nationwide Suspicious Activity Reporting Concept of Operations, December 2008; ISE Suspicious Activity Reporting Evaluation Environment (EE) Segment Architecture, December 2008.
5. Definitions.
 - a. Artifact: Detailed mission product documentation addressing information exchanges and data elements for ISE-SAR (data models, schemas, structures, etc.).

UNCLASSIFIED

ISE-FS-200

- b. CTISS: Business process-driven, performance-based “common standards” for preparing terrorism information for maximum distribution and access, to enable the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE. CTISS, such as this *ISE-SAR Functional Standard*, are implemented in ISE participant infrastructures that include ISE Shared Spaces as described in the *ISE EAF*. Two categories of common standards are formally identified under CTISS:
- (1) Functional Standards – set forth rules, conditions, guidelines, and characteristics of data and mission products supporting ISE business process areas.
 - (2) Technical Standards – document specific technical methodologies and practices to design and implement information sharing capability into ISE systems.
- c. Information Exchange: The transfer of information from one organization to another organization, in accordance with CTISS defined processes.
- d. ISE-Suspicious Activity Report (ISE-SAR): An ISE-SAR is a SAR (as defined below in 5i) that has been determined, pursuant to a two-part process, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism). ISE-SAR business, privacy, and civil liberties rules will serve as a unified process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.
- e. National Information Exchange Model (NIEM): A joint technical and functional standards program initiated by the Department of Homeland Security (DHS) and the Department of Justice (DOJ) that supports national-level interoperable information sharing.
- f. Personal Information: Information that may be used to identify an individual (i.e., data elements in the identified “privacy fields” of this *ISE-SAR Functional Standard*).
- g. Privacy Field: A data element that may be used to identify an individual and, therefore, may be subject to privacy protection.
- h. Suspicious Activity: Observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.
- i. Suspicious Activity Report (SAR): Official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.
- j. Universal Core (UCore): An interagency information exchange specification and implementation profile. It provides a framework for sharing the most commonly used data concepts of “who, what when, and where”. UCore serves as a starting point for data level integration and permits the development of richer domain specific exchanges. UCore was developed in concert with NIEM program office, and is a collaborative effort between Department of Defense (DOD), DOJ, DHS and the Intelligence Community.

UNCLASSIFIED

ISE-FS-200

6. Guidance. This Functional Standard is hereby established as the nationwide ISE Functional Standard for ISE-SARs. It is based on documented information exchanges and business requirements, and describes the structure, content, and products associated with processing, integrating, and retrieving ISE-SARs by ISE participants.

7. Responsibilities.

- a. The PM-ISE, in consultation with the Information Sharing Council (ISC), will:
 - (1) Maintain and administer this *ISE-SAR Functional Standard*, to include:
 - (a) Updating the business process and information flows for ISE-SAR.
 - (b) Updating data elements and product definitions for ISE-SAR.
 - (2) Publish and maintain configuration management of this *ISE-SAR Functional Standard*.
 - (3) Assist with the development of ISE-SAR implementation guidance and governance structure, as appropriate, to address privacy, civil rights, and civil liberties, policy, architecture, and legal issues.
 - (4) Work with ISE participants, through the CTISS Committee, to develop a new or modified *ISE-SAR Functional Standard*, as needed.
 - (5) Coordinate, publish, and monitor implementation and use of this *ISE-SAR Functional Standard*, and coordinate with the White House Office of Science and Technology Policy and with the National Institute of Standards and Technology (in the Department of Commerce) for broader publication, as appropriate.
- b. Each ISC member and other affected organizations shall:
 - (1) Propose modifications to the PM-ISE for this Functional Standard, as appropriate.
 - (2) As appropriate, incorporate this *ISE-SAR Functional Standard*, and any subsequent implementation guidance, into budget activities associated with relevant current (operational) mission specific programs, systems, or initiatives (e.g. operations and maintenance {O&M} or enhancements).
 - (3) As appropriate, incorporate this *ISE-SAR Functional Standard*, and any subsequent implementation guidance, into budget activities associated with future or new development efforts for relevant mission specific programs, systems, or initiatives (e.g. development, modernization, or enhancement {DME}).
 - (4) Ensure incorporation of this *ISE-SAR Functional Standard*, as set forth in 7.b (2) or 7.b (3) above, is done in compliance with ISE Privacy Guidelines and any additional guidance provided by the ISE Privacy Guidelines Committee.

UNCLASSIFIED

ISE-FS-200

8. Effective Date and Expiration. This ISE-FS is effective immediately and will remain in effect as the updated *ISE-SAR Functional Standard* until further updated, superseded, or cancelled.

A handwritten signature in black ink, appearing to read "Thomas E. McManis", written over a horizontal line.

Program Manager for the
Information Sharing Environment

Date: May 21, 2009

UNCLASSIFIED

ISE-FS-200

PART A – ISE-SAR FUNCTIONAL STANDARD ELEMENTS

SECTION I – DOCUMENT OVERVIEW

A. List of ISE-SAR Functional Standard Technical Artifacts

The full ISE-SAR information exchange contains five types of supporting technical artifacts. This documentation provides details of implementation processes and other relevant reference materials. A synopsis of the *ISE-SAR Functional Standard* technical artifacts is contained in Table 1 below.

Table 1 – Functional Standard Technical Artifacts¹

Artifact Type	Artifact	Artifact Description
Development and Implementation Tools	1. Component Mapping Template (CMT) (SAR-to-NIEM/UCore)	This spreadsheet captures the ISE-SAR information exchange class and data element (source) definitions and relates each data element to corresponding National Information Exchange Model (NIEM) Extensible Mark-Up Language (XML) elements and UCore elements, as appropriate.
	2. NIEM Wantlist	The Wantlist is an XML file that lists the elements selected from the NIEM data model for inclusion in the Schema Subset. The Schema Subset is a compliant version to both programs that has been reduced to only those elements actually used in the ISE-SAR document schema.
	3. XML Schemas	The XML Schema provides a technical representation of the business data requirements. They are a machine readable definition of the structure of an ISE-SAR-based XML Message.
	4. XML Sample Instance	The XML Sample Instance is a sample document that has been formatted to comply with the structures defined in the XML Schema. It provides the developer with an example of how the ISE-SAR schema is intended to be used.
	5. Codified Data Field Values	Listings, descriptions, and sources as prescribed by data fields in the <i>ISE-SAR Functional Standard</i> .

¹ Development and implementation tools may be accessible through www.ise.gov. Additionally, updated versions of this Functional Standard will incorporate the CTISS Universal Core which harmonizes the NIEM Universal Core with the DoD/IC UCore.

UNCLASSIFIED

ISE-FS-200

SECTION II – SUSPICIOUS ACTIVITY REPORTING EXCHANGES

A. ISE-SAR Purpose

This *ISE-SAR Functional Standard* is designed to support the sharing, throughout the Information Sharing Environment (ISE), of information about suspicious activity, incidents, or behavior (hereafter collectively referred to as suspicious activity or activities) that have a potential terrorism nexus. The ISE includes State and major urban area fusion centers and their law enforcement,² homeland security,³ or other information sharing partners at the Federal, State, local, and tribal levels to the full extent permitted by law. In addition to providing specific indications about possible terrorism-related crimes, ISE-SARs can be used to look for patterns and trends by analyzing information at a broader level than would typically be recognized within a single jurisdiction, State, or territory. Standardized and consistent sharing of suspicious activity information regarding criminal activity among State and major urban area fusion centers and Federal agencies is vital to assessing, deterring, preventing, or prosecuting those involved in criminal activities associated with terrorism. This *ISE-SAR Functional Standard* has been designed to incorporate key elements that describe potential criminal activity associated with terrorism and may be used by other communities to address other types of criminal activities where appropriate.

B. ISE-SAR Scope

Suspicious activity is defined as *observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity*. A determination that such suspicious activity constitutes an ISE-SAR is made as part of a two-part process by trained analysts using explicit criteria. Some examples of the criteria for identifying those SARs, with defined relationships to criminal activity that also have a potential terrorism nexus, are listed below. Part B (ISE-SAR Criteria Guidance) provides a more thorough explanation of ISE-SAR criteria, highlighting the importance of context in interpreting such behaviors;

- Expressed or implied threat
- Theft/loss/diversion
- Site breach or physical intrusion
- Cyber attacks
- Probing of security response

² All references to Federal, State, local and tribal law enforcement are intended to encompass civilian law enforcement, military police, and other security professionals.

³ All references to homeland security are intended to encompass public safety, emergency management, and other officials who routinely participate in the State or major urban area's homeland security preparedness activities.

UNCLASSIFIED

ISE-FS-200

It is important to stress that this *behavior-focused approach* to identifying suspicious activity requires that factors such as race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion (except if used as part of a specific suspect description). It is also important to recognize that many terrorism activities are now being funded via local or regional criminal organizations whose direct association with terrorism may be tenuous. This places law enforcement and homeland security professionals in the unique, yet demanding, position of identifying suspicious activities or materials as a byproduct or secondary element in a criminal enforcement or investigation activity. This means that, while some ISE-SARs may document activities or incidents to which local agencies have already responded, there is value in sharing them more broadly to facilitate aggregate trending or analysis.

Suspicious Activity Reports are not intended to be used to track or record ongoing enforcement, intelligence, or investigatory operations although they can provide information to these activities. The ISE-SAR effort offers a standardized means for sharing information regarding behavior potentially related to terrorism-related criminal activity and applying data analysis tools to the information. Any patterns identified during ISE-SAR data analysis may be investigated in cooperation with the reporting agency, Joint Terrorism Task Force (JTTF), or the State or major urban area fusion center in accordance with departmental policies and procedures. Moreover, the same constitutional standards that apply when conducting ordinary criminal investigations also apply to local law enforcement and homeland security officers conducting SAR inquiries. This means, for example, that constitutional protections and agency policies and procedures that apply to a law enforcement officer's authority to stop, stop and frisk ("Terry Stop")⁴, request identification, or detain and question an individual would apply in the same measure whether or not the observed behavior related to terrorism or any other criminal activity.

C. Overview of Nationwide SAR Cycle

As defined in the *Nationwide Suspicious Activity Reporting Initiative (NSI) Concept of Operations (CONOPS)*⁵ and shown in Figure 1, the nationwide SAR process involves a total of 12 discrete steps that are grouped under five standardized business process activities – Planning, Gathering and Processing, Analysis and Production, Dissemination, and Reevaluation. The top-level ISE-SAR business process described in this section has been revised to be consistent with the description in the *NSI CONOPS*. Consequently, the numbered steps in Figure 1 are the only ones that map directly to the nine-steps of the detailed information flow for nationwide SAR information sharing documented in Part C of this version of the *ISE-SAR Functional Standard*. For further detail on the 12 NSI steps, please refer to the *NSI CONOPS*.

⁴ "Terry Stop" refers to law enforcement circumstances related to Supreme Court of the United States ruling on "Terry v. Ohio (No. 67)" argued on December 12, 1967 and decided on June 10, 1968. This case allows a law enforcement officer to articulate reasonable suspicion as a result of a totality of circumstances (to include training and experience) and take action to frisk an individual for weapons that may endanger the officer. The Opinion of the Supreme Court regarding this case may be found at Internet site http://www.law.cornell.edu/supct/html/historics/USSC_CR_0392_0001_ZO.html.

⁵ PM-ISE, *Nationwide SAR Initiative Concept of Operations* (Washington: PM-ISE, 2008), available from www.ise.gov.

UNCLASSIFIED

ISE-FS-200

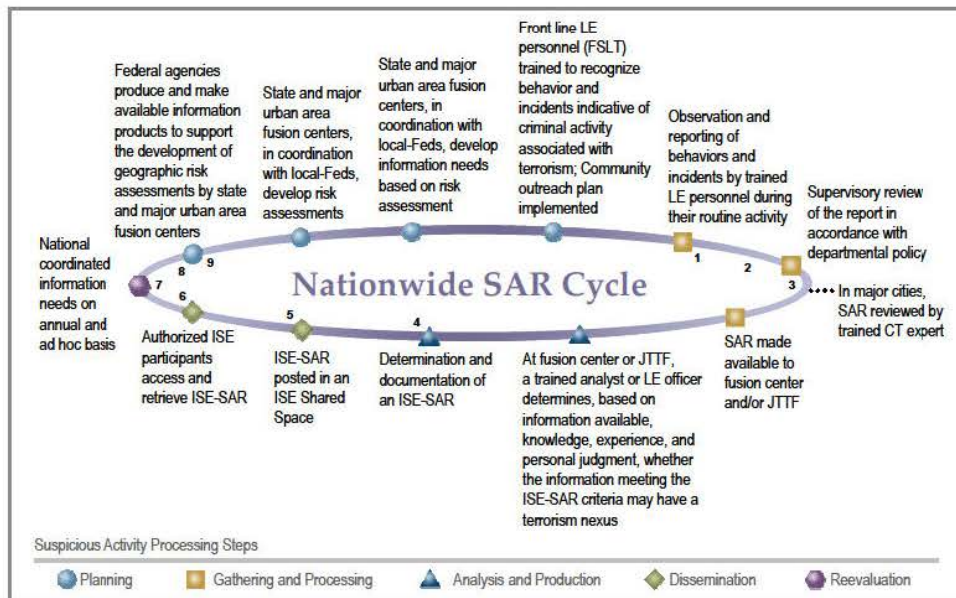


Figure 1. Overview of Nationwide SAR Process

D. ISE-SAR Top-Level Business Process

1. Planning

The activities in the planning phase of the NSI cycle, while integral to the overall NSI, are not discussed further in this Functional Standard. See the NSI CONOPS for more details.⁶

2. Gathering and Processing

Local law enforcement agencies or field elements of Federal agencies gather and document suspicious activity information in support of their responsibilities to investigate potential criminal activity, protect citizens, apprehend and prosecute criminals, and prevent crime. Information acquisition begins with an observation or report of unusual or suspicious behavior that may be indicative of criminal activity associated with terrorism. Such activities include, but are not limited to, theft, loss, or diversion, site breach or physical intrusion, cyber attacks, possible testing of physical response, or other unusual behavior or sector specific incidents. It is important to emphasize that context is an essential element of interpreting the relevance of such behaviors to criminal activity associated with terrorism. (See Part B for more details.)

⁶ Ibid., 17-18.

UNCLASSIFIED

ISE-FS-200

Regardless of whether the initial observer is a private citizen, a representative of a private sector partner, a government official, or a law enforcement officer, suspicious activity is eventually reported to either a local law enforcement agency or a local, regional, or national office of a Federal agency. When the initial investigation or fact gathering is completed, the investigating official documents the event in accordance with agency policy, local ordinances, and State and Federal laws and regulations.

The information is reviewed within a local or Federal agency by appropriately designated officials for linkages to other suspicious or criminal activity in accordance with departmental policy and procedures.⁷ Although there is always some level of local review, the degree varies from agency to agency. Smaller agencies may forward most SARs directly to the State or major urban area fusion center or JTTF with minimal local processing. Major cities, on the other hand, may have trained counterterrorism experts on staff that apply a more rigorous analytic review of the initial reports and filter out those that can be determined not to have a potential terrorism nexus.

After appropriate local processing, agencies make SARs available to the relevant State or major urban area fusion center. Field components of Federal agencies forward their reports to the appropriate regional, district, or headquarters office employing processes that vary from agency to agency. Depending on the nature of the activity, the information could cross the threshold of “suspicious” and move immediately into law enforcement operations channels for follow-on action against the identified terrorist activity. In those cases where the local agency can determine that an activity has a direct connection to criminal activity associated with terrorism, it will provide the information directly to the responsible JTTF for use as the basis for an assessment or investigation of a terrorism-related crime as appropriate.

3. Analysis and Production

The fusion center or Federal agency enters the SAR into its local information system and then performs an additional analytic review to establish or discount a potential terrorism nexus. First, an analyst or law enforcement officer reviews the newly reported information against ISE-SAR criteria outlined in Part B of this *ISE-SAR Functional Standard*. Second, the Terrorist Screening Center (TSC) should be contacted to determine if there is valuable information in the Terrorist Screening Database. Third, he or she will review the input against all available knowledge and information for linkages to other suspicious or criminal activity.

Based on this review, the officer or analyst will apply his or her professional judgment to determine whether the information has a potential nexus to terrorism. If the officer or analyst cannot make this explicit determination, the report will not be accessible by the ISE, although

⁷ If appropriate, the agency may consult with a Joint Terrorism Task Force, Field Intelligence Group, or fusion center.

UNCLASSIFIED

ISE-FS-200

it may be retained in local fusion center or Federal agency files in accordance with established retention policies and business rules.⁸

4. Dissemination

Once the determination of a potential terrorism nexus is made, the information becomes an ISE-SAR and is formatted in accordance with the ISE-SAR Information Exchange Package Document (IEPD) format described in Sections III and IV. This ISE-SAR is then stored in the fusion center, JTTF, or other Federal agency's ISE Shared Space⁹ where it can be accessed by authorized law enforcement and homeland security personnel in the State or major urban area fusion center's area of responsibility as well as other ISE participants, including JTTFs. This allows the fusion center to be cognizant of all terrorist-related suspicious activity in its area of responsibility, consistent with the information flow description in Part C. Although the information in ISE Shared Spaces is accessible by other ISE participants, it remains under the control of the submitting organization, i.e., the fusion center or Federal agency that made the initial determination that the activity constituted an ISE-SAR.

By this stage of the process, all initially reported SARs have been through multiple levels of review by trained personnel and, to the maximum extent possible, those reports without a potential terrorism nexus have been filtered out. Those reports posted in ISE Shared Spaces, therefore, can be presumed by Federal, State, and local analytic personnel to be terrorism-related and information derived from them can be used along with other sources to support counterterrorism operations or develop counterterrorism analytic products. As in any analytic process, however, all information is subject to further review and validation, and analysts must coordinate with the submitting organization to ensure that the information is still valid and obtain any available relevant supplementary material before incorporating it into an analytic product.

Once ISE-SARs are accessible, they can be used to support a range of counterterrorism analytic and operational activities. This step involves the actions necessary to integrate ISE-SAR information into existing counterterrorism analytic and operational processes, including efforts to "connect the dots," identify information gaps, and develop formal analytic products. Depending on privacy policy and procedures established for the NSI as a whole or by agencies responsible for individual ISE Shared Spaces, requestors may only be able to view reports in the Summary ISE-SAR Information format, i.e., without privacy fields. In these cases, requestors should contact the submitting organization directly to discuss the particular report more fully and obtain access, where appropriate, to the information in the privacy fields.

⁸ As was already noted in the discussion of processing by local agencies, where the fusion center or Federal agency can determine that an activity has a direct connection to a possible terrorism-related crime, it will provide the information directly to the responsible JTTF for use as the basis for an assessment or investigation.

⁹ PM-ISE, *ISE Enterprise Architecture Framework, Version 2.0*, (Washington: PM-ISE, 2008), 61-63

UNCLASSIFIED

ISE-FS-200

5. Reevaluation¹⁰

Operational feedback on the status of ISE-SARs is an essential element of an effective NSI process with important implications for privacy and civil liberties. First of all, it is important to notify source organizations when information they provide is designated as an ISE-SAR by a submitting organization and made available for sharing—a form of positive feedback that lets organizations know that their initial suspicions have some validity. Moreover, the process must support notification of all ISE participants when further evidence determines that an ISE-SAR was designated incorrectly so that the original information does not continue to be used as the basis for analysis or action. This type of feedback can support organizational redress processes and procedures where appropriate.

E. Broader ISE-SAR Applicability

Consistent with the ISE Privacy Guidelines and Presidential Guideline 2, and to the full extent permitted by law, this *ISE-SAR Functional Standard* is designed to support the sharing of unclassified information or sensitive but unclassified (SBU)/controlled unclassified information (CUI) within the ISE. There is also a provision for using a data element indicator for designating classified national security information as part of the ISE-SAR record, as necessary. This condition could be required under special circumstances for protecting the context of the event, or specifics or organizational associations of affected locations. The State or major urban area fusion center shall act as the key conduit between the State, local, and tribal (SLT) agencies and other ISE participants. It is also important to note that the ISE Shared Spaces implementation concept is focused exclusively on terrorism-related information. However many SAR originators and consumers have responsibilities beyond terrorist activities. Of special note, there is no intention to modify or otherwise affect, through this *ISE-SAR Functional Standard*, the currently supported or mandated direct interactions between State, local, and tribal law enforcement and investigatory personnel and the Joint Terrorism Task Forces (JTTFs) or Field Intelligence Groups (FIGs).

This *ISE-SAR Functional Standard* will be used as the ISE-SAR information exchange standard for all ISE participants. Although the extensibility of this *ISE-SAR Functional Standard* does support customization for unique communities, jurisdictions planning to modify this *ISE-SAR Functional Standard* must carefully consider the consequences of customization. The PM-ISE requests that modification follow a formal change request process through the ISE-SAR Steering Committee and CTISS Committee under the Information Sharing Council, for both community coordination and consideration. Furthermore, messages that do not conform to this Functional Standard may not be consumable by the receiving organization and may require modifications by the nonconforming organizations.

¹⁰ The Reevaluation Phase also encompasses the establishment of an integrated counterterrorism information needs process, a process that does not relate directly to information exchanges through this standard. See page 23 of the *NSI CONOPS* for more details.

UNCLASSIFIED

ISE-FS-200

F. Protecting Privacy

Laws that prohibit or otherwise limit the sharing of personal information vary considerably between the Federal, State, local, and tribal levels. The Privacy Act of 1974 (5 USC §552a) as amended, other statutes such as the E-Government Act, and many government-wide or departmental regulations establish a framework and criteria for protecting information privacy in the Federal Government. The ISE must facilitate the sharing of information in a lawful manner, which by its nature must recognize, in addition to Federal statutes and regulations, different State, local or tribal laws, regulations, or policies that affect privacy. One method for protecting privacy while enabling the broadest possible sharing is to anonymize ISE-SAR reports by excluding data elements that contain personal information. Accordingly, two different formats are available for ISE-SAR information. The **Detailed ISE-SAR IEPD** format includes personal information contained in the data fields set forth in Section IV of this *ISE-SAR Functional Standard* (“ISE-SAR Exchange Data Model”), including “privacy fields” denoted as containing personal information. If an ISE participant is not authorized to disseminate personal information from an ISE Shared Space (e.g., the requester site does not have a compliant privacy policy) or the SAR does not evidence the necessary nexus to terrorism-related crime (as required by this *ISE-SAR Functional Standard*), information from the privacy fields will not be loaded into the responsive document (search results) from the ISE Shared Space. This personal information will not be passed to the ISE participant. The **Summary ISE-SAR Information** format excludes privacy fields or data elements identified in Section IV of this *ISE-SAR Functional Standard* as containing personal information. Each ISE participant can exclude additional data elements from the **Summary ISE-SAR Information** format in accordance with its own legal and policy requirements. It is believed the data contained within a **Summary ISE-SAR Information** format will support sufficient trending and pattern recognition to trigger further analysis and/or investigation where additional information can be requested from the sending organization. Because of variances of data expected within ISE-SAR exchanges, only the minimum elements are considered mandatory. These are enumerated in the READ ME document in the technical artifacts folder that is part of this *ISE-SAR Functional Standard*.

Currently, the privacy fields identified in the ISE-SAR exchange data model (Section IV, below) are the minimum fields that should be removed from a **Detailed ISE-SAR IEPD**.

SECTION III – INFORMATION EXCHANGE DEVELOPMENT

This *ISE-SAR Functional Standard* is a collection of artifacts that support an implementer’s creation of ISE-SAR information exchanges, whether **Detailed ISE-SAR IEPD** or **Summary ISE-SAR Information**. The basic ISE-SAR information exchange is documented using five unique artifacts giving implementers tangible products that can be leveraged for local implementation. A domain model provides a graphical depiction of those data elements required for implementing an exchange and the cardinality between those data elements. Second, a Component Mapping Template is a spreadsheet that associates each required data element with its corresponding XML data element. Third, information exchanges include the schemas which consist of a document, extension, and constraint schema. Fourth, at least one sample XML Instance and associated style-sheet is included to help practitioners validate the model, mapping,

UNCLASSIFIED

ISE-FS-200

and schemas in a more intuitive way. Fifth, a codified data field values listing provides listings, descriptions, and sources as prescribed by the data fields.

SECTION IV – ISE-SAR EXCHANGE DATA MODEL

A. Summary of Elements

This section contains a full inventory of all ISE-SAR information exchange data classes, elements, and definitions. Items and definitions contained in cells with a light purple background are data classes, while items and definition contained in cells with a white background are data elements. A wider representation of data class and element mappings to source (ISE-SAR information exchange) and target is contained in the Component Mapping Template located in the technical artifacts folder.

Cardinality between objects in the model is indicated on the line in the domain model (see Section 5A). Cardinality indicates how many times an entity can occur in the model. For example, Vehicle, Vessel, and Aircraft all have cardinality of 0..n. This means that they are optional, but may occur multiple times if multiple suspect vehicles are identified.

Clarification of Organizations used in the exchange:

- The **Source Organization** is the agency or entity that originates the SAR report (examples include a local police department, a private security firm handling security for a power plant, and a security force at a military installation). The Source Organization will not change throughout the life of the SAR.
- The **Submitting Organization** is the organization providing the ISE-SAR to the community through their ISE Shared Space. The Submitting Organization and the Source Organization may be the same.
- The **Owning Organization** is the organization that owns the target associated with the suspicious activity.

Table 2 – ISE-SAR Information Exchange Data Classes, Elements, and Definitions

Privacy Field	Source Class/Element	Source Definition
	Aircraft	
	Aircraft Engine Quantity	The number of engines on an observed aircraft.
	Aircraft Fuselage Color	A code identifying a color of a fuselage of an aircraft.
	Aircraft Wing Color	A code identifying a color of a wing of an aircraft.
X	Aircraft ID	A unique identifier assigned to the aircraft by the observing organization—used for referencing. *If this identifier can be used to identify a specific aircraft, for instance, by using the aircraft tail number, then this element is a privacy field. [free text field]
	Aircraft Make Code	A code identifying a manufacturer of an aircraft.
	Aircraft Model Code	A code identifying a specific design or type of aircraft made by a manufacturer

UNCLASSIFIED

ISE-FS-200

Privacy Field	Source Class/Element	Source Definition
	Aircraft Style Code	A code identifying a style of an aircraft.
X	Aircraft Tail Number	An aircraft identification number prominently displayed at various locations on an aircraft, such as on the tail and along the fuselage. [free text field]
	Attachment	
	Attachment Type Text	Describes the type of attachment (e.g., surveillance video, mug shot, evidence). [free text field]
	Binary Image	Binary encoding of the attachment.
	Capture Date	The date that the attachment was created.
	Description Text	Text description of the attachment. [free text field]
	Format Type Text	Format of attachment (e.g., mpeg, jpg, avi). [free text field]
	Attachment URI	Uniform Resource Identifier (URI) for the attachment. Used to match the attachment link to the attachment itself. Standard representation type that can be used for Uniform Resource Locators (URLs) and Uniform Resource Names (URNs).
	Attachment Privacy Field Indicator	Identifies whether the binary attachment contains information that may be used to identify an individual.
	Contact Information	
	Person First Name	Person to contact at the organization.
	Person Last Name	Person to contact at the organization.
	E-Mail Address	An email address of a person or organization. [free text field]
	Full Telephone Number	A full length telephone identifier representing the digits to be dialed to reach a specific telephone instrument. [free text field]
	Driver License	
X	Expiration Date	The month, date, and year that the document expires.
	Expiration Year	The year the document expires.
	Issuing Authority Text	Code identifying the organization that issued the driver license assigned to the person. Examples include Department of Motor Vehicles, Department of Public Safety and Department of Highway Safety and Motor Vehicles. [free text field]
X	Driver License Number	A driver license identifier or driver license permit identifier of the observer or observed person of interest involved with the suspicious activity. [free text field]
	Follow-Up Action	
	Activity Date	Date that the follow-up activity started.
	Activity Time	Time that the follow up activity started.
	Assigned By Text	Organizational identifier that describes the organization performing a follow-up activity. This is designed to keep all parties interested in a particular ISE-SAR informed of concurrent investigations. [free text field]
	Assigned To Text	Text describing the person or sub-organization that will be performing the designated action. [free text field]
	Disposition Text	Description of disposition of suspicious activity investigation. [free text field]
	Status Text	Description of the state of follow-up activity. [free text field]
	Location	

UNCLASSIFIED

ISE-FS-200

Privacy Field	Source Class/Element	Source Definition
X	Location Description	A description of a location where the suspicious activity occurred. If the location is an address that is not broken into its component parts (e.g., 1234 Main Street), this field may be used to store the compound address. [free text field]
	Location Address	
	Building Description	A complete reference that identifies a building. [free text field]
	County Name	A name of a county, parish, or vicinage. [free text field]
	Country Name	A country name or other identifier. [free text field]
	Cross Street Description	A description of an intersecting street. [free text field]
	Floor Identifier	A reference that identifies an actual level within a building. [free text field]
	ICAO Airfield Code for Departure	An International Civil Aviation Organization (ICAO) airfield code for departure, indicates aircraft, crew, passengers, and cargo-on conveyance location information. [free text field]
	ICAO Airfield Code for Planned Destination	An airfield code for planned destination, indicates aircraft, crew, passengers, and cargo on conveyance location information [free text field]
	ICAO for Actual Destination	An airfield code for actual destination. Indicates aircraft, crew, passengers, and cargo on conveyance location information. [free text field]
	ICAO Airfield for Alternate	An airfield code for Alternate. Indicates aircraft, crew, passengers, and cargo on conveyance location information. [free text field]
	Mile Marker Text	Identifies the sequentially numbered marker on a roadside that is closest to the intended location. Also known as milepost, or mile post. [free text field]
	Municipality Name	The name of the city or town. [free text field]
	Postal Code	The zip code or postal code. [free text field]
	State Name	Code identifying the state.
	Street Name	A name that identifies a particular street. [free text field]
X	Street Number	A number that identifies a particular unit or location within a street. [free text field]
	Street Post Directional	A direction that appears after a street name. [free text field]
	Street Pre Directional	A direction that appears before a street name. [free text field]
	Street Type	A type of street, e.g., Street, Boulevard, Avenue, Highway. [free text field]
X	Unit ID	A particular unit within the location. [free text field]
	Location Coordinates	
	Altitude	Height above or below sea-level of a location.
	Coordinate Datum	Coordinate system used for plotting location.
	Latitude Degree	A value that specifies the degree of a latitude. The value comes from a restricted range between -90 (inclusive) and +90 (inclusive).
	Latitude Minute	A value that specifies a minute of a degree. The value comes from a restricted range of 0 (inclusive) to 60 (exclusive).
	Latitude Second	A value that specifies a second of a minute. The value comes from a restricted range of 0 (inclusive) to 60 (exclusive).

UNCLASSIFIED

ISE-FS-200

Privacy Field	Source Class/Element	Source Definition
	Longitude Degree	A value that specifies the degree of a longitude. The value comes from a restricted range between -180 (inclusive) and +180 (exclusive).
	Longitude Minute	A value that specifies a minute of a degree. The value comes from a restricted range of 0 (inclusive) to 60 (exclusive).
	Longitude Second	A value that specifies a second of a minute. The value comes from a restricted range of 0 (inclusive) to 60 (exclusive).
	Conveyance track/intent	A direction by heading and speed or enroute route and/or waypoint of conveyance [free text field]
	Observer	
	Observer Type Text	Indicates the relative expertise of an observer to the suspicious activity (e.g., professional observer versus layman). Example: a security guard at a utility plant recording the activity, or a citizen driving by viewing suspicious activity. [free text field]
X	Person Employer ID	Number assigned by an employer for a person such as badge number. [free text field]
	Owning Organization	
	Organization Item	A name of an organization that owns the target. [free text field]
	Organization Description	A text description of organization that owns the target. The description may indicate the type of organization such as State Bureau of Investigation, Highway Patrol, etc. [free text field]
X	Organization ID	A federal tax identifier assigned to an organization. Sometimes referred to as a Federal Employer Identification Number (FEIN), or an Employer Identification Number (EIN). [free text field]
	Organization Local ID	An identifier assigned on a local level to an organization. [free text field]
	Other Identifier	
X	Person Identification Number (PID)	An identifying number assigned to the person, e.g., military serial numbers. [free text field]
X	PID Effective Date	The month, date, and year that the PID number became active or accurate.
	PID Effective Year	The year that the PID number became active or accurate.
X	PID Expiration Date	The month, date, and year that the PID number expires.
	PID Expiration Year	The year that the PID number expires.
	PID Issuing Authority Text	The issuing authority of the identifier. This may be a State, military organization, etc.
	PID Type Code	Code identifying the type of identifier assigned to the person. [free text field]
	Passport	
X	Passport ID	Document Unique Identifier. [free text field]
X	Expiration Date	The month, date, and year that the document expires.
	Expiration Year	The year the document expires.
	Issuing Country Code	Code identifying the issuing country. [free text field]
	Person	
X	AFIS FBI Number	A number issued by the FBI's Automated Fingerprint Identification System (AFIS) based on submitted fingerprints. [free text field]

UNCLASSIFIED

ISE-FS-200

Privacy Field	Source Class/Element	Source Definition
	Age	A precise measurement of the age of a person.
	Age Unit Code	Code that identifies the unit of measure of an age of a person (e.g., years, months). [free text field]
X	Date of Birth	The month, date, and year that a person was born.
	Year of Birth	The year a person was born.
	Ethnicity Code	Code that identifies the person's cultural lineage.
	Maximum Age	The maximum age measurement in an estimated range.
	Minimum Age	The minimum age measurement in an estimated range.
X	State Identifier	Number assigned by the State based on biometric identifiers or other matching algorithms. [free text field]
X	Tax Identifier Number	A 9-digit numeric identifier assigned to a living person by the U.S. Social Security Administration. A social security number of the person. [free text field]
	Person Name	
X	First Name	A first name or given name of the person. [free text field]
X	Last Name	A last name or family name of the person. [free text field]
X	Middle Name	A middle name of a person. [free text field]
X	Full Name	Used to designate the compound name of a person that includes all name parts. This field should only be used when the name cannot be broken down into its component parts or if the information is not available in its component parts. [free text field]
X	Moniker	Alternative, or gang name for a person. [free text field]
	Name Suffix	A component that is appended after the family name that distinguishes members of a family with the same given, middle, and last name, or otherwise qualifies the name. [free text field]
	Name Type	Text identifying the type of name for the person. For example, maiden name, professional name, nick name.
	Physical Descriptors	
	Build Description	Text describing the physique or shape of a person. [free text field]
	Eye Color Code	Code identifying the color of the person's eyes.
	Eye Color Text	Text describing the color of a person's eyes. [free text field]
	Hair Color Code	Code identifying the color of the person's hair.
	Hair Color Text	Text describing the color of a person's hair. [free text field]
	Person Eyewear Text	A description of glasses or other eyewear a person wears. [free text field]
	Person Facial Hair Text	A kind of facial hair of a person. [free text field]
	Person Height	A measurement of the height of a person.
	Person Height Unit Code	Code that identifies the unit of measure of a height of a person. [free text field]
	Person Maximum Height	The maximum measure value on an estimated range of the height of the person.
	Person Minimum Height	The minimum measure value on an estimated range of the height of the person.
	Person Maximum Weight	The maximum measure value on an estimated range of the weight of the person.

UNCLASSIFIED

ISE-FS-200

Privacy Field	Source Class/Element	Source Definition
	Person Minimum Weight	The minimum measure value on an estimated range of the weight of the person.
	Person Sex Code	A code identifying the gender or sex of a person (e.g., Male or Female).
	Person Weight	A measurement of the weight of a person.
	Person Weight Unit Code	Code that identifies the unit of measure of a weight of a person. [free text field]
	Race Code	Code that identifies the race of the person.
	Skin Tone Code	Code identifying the color or tone of a person's skin.
	Clothing Description Text	A description of an article of clothing. [free text field]
	Physical Feature	
	Feature Description	A text description of a physical feature of the person. [free text field]
	Feature Type Code	A special kind of physical feature or any distinguishing feature. Examples include scars, marks, tattoos, or a missing ear. [free text field]
	Location Description	A description of a location. If the location is an address that is not broken into its component parts (e.g., 1234 Main Street), this field may be used to store the compound address. [free text field]
	Registration	
	Registration Authority Code	Text describing the organization or entity authorizing the issuance of a registration for the vehicle involved with the suspicious activity. [free text field]
X	Registration Number	The number on a metal plate fixed to/assigned to a vehicle. The purpose of the registration number is to uniquely identify each vehicle within a state. [free text field]
	Registration Type	Code that identifies the type of registration plate or license plate of a vehicle. [free text field]
	Registration Year	A 4-digit year as shown on the registration decal issued for the vehicle.
	ISE-SAR Submission	
	Additional Details Indicator	Identifies whether more ISE-SAR details are available at the authoring/originating agency than what has been provided in the information exchange.
	Data Entry Date	Date the data was entered into the reporting system (e.g., the Records Management System).
	Dissemination Code	Generally established locally, this code describes the authorized recipients of the data. Examples include Law Enforcement Use, Do Not Disseminate, etc.
	Fusion Center Contact First Name	Identifies the first name of the person to contact at the fusion center. [free text field]
	Fusion Center Contact Last Name	Identifies the last name of the person to contact at the fusion center. [free text field]
	Fusion Center Contact E-Mail Address	Identifies the email address of the person to contact at the fusion center. [free text field]
	Fusion Center Contact Telephone Number	The full phone number of the person at the fusion center that is familiar with the record (e.g., law enforcement officer).

UNCLASSIFIED

ISE-FS-200

Privacy Field	Source Class/Element	Source Definition
	Message Type Indicator	e.g., Add, Update, Purge.
	Privacy Purge Date	The date by which the privacy information will be purged from the record system; general observation data is retained.
	Privacy Purge Review Date	Date of review to determine the disposition of the privacy fields in a Detailed ISE-SAR IEPD record.
	Submitting ISE-SAR Record ID	Identifies the Fusion Center ISE-SAR Record identifier for reports that are possibly related to the current report. [free text field]
	ISE-SAR Submission Date	Date of submission for the ISE-SAR Record.
	ISE-SAR Title	Plain language title (e.g., Bomb threat at the "X" Hotel). [free text field]
	ISE-SAR Version	Indicates the specific version of the ISE-SAR that the XML Instance corresponds. [free text field]
	Source Agency Case ID	The case identifier for the agency that originated the SAR. Often, this will be a local law enforcement agency. [free text field]
	Source Agency Record Reference Name	The case identifier that is commonly used by the source agency—may be the same as the System ID. [free text field]
	Source Agency Record Status Code	The current status of the record within the source agency system.
	Privacy Information Exists Indicator	Indicates whether privacy information is available from the source fusion center. This indicator may be used to guide people who only have access to the summary information exchange as to whether or not they can follow-up with the originating fusion center to obtain more information.
	Sensitive Information Details	
	Classification Label	A classification of information. Includes Confidential, Secret, Top Secret, no markings. [free text field]
	Classification Reason Text	A reason why the classification was made as such. [free text field]
	Sensitivity Level	Local information security categorization level (Controlled Unclassified Information-CUI, including Sensitive But Unclassified or Law Enforcement Sensitive). [free text field]
	Tearlined Indicator	Identifies whether a report is free of classified information.
	Source Organization	
	Organization Name	The name used to refer to the agency originating the SAR. [free text field]
	Organization ORI	Originating Agency Identification (ORI) used to refer to the agency.
	System ID	The system that the case identifier (e.g., Records Management System, Computer Aided Dispatch) relates to within or the organization that originated the Suspicious Activity Report. [free text field]
	Fusion Center Submission Date	Date of submission to the Fusion Center.
	Source Agency Contact First Name	The first name of the person at the agency that is familiar with the record (e.g., law enforcement officer). [free text field]
	Source Agency Contact Last Name	The last name of the person at the agency that is familiar with the record (e.g., law enforcement officer). [free text field]
	Source Agency Contact Email Address	The email address of the person at the agency that is familiar with the record (e.g., law enforcement officer). [free text field]

UNCLASSIFIED

ISE-FS-200

Privacy Field	Source Class/Element	Source Definition
	Source Agency Contact Phone Number	The full phone number of the person at the agency that is familiar with the record (e.g., law enforcement officer).
	Suspicious Activity Report	
	Community Description	Describes the intended audience of the document. [free text field]
	Community URI	The URL to resolve the ISE-SAR information exchange payload namespace.
	LEXS Version	Identifies the version of Department of Justice LEISP Exchange Specification (LEXS) used to publish this document. ISE-FS-200 has been built using LEXS version 3.1. The schema was developed by starting with the basic LEXS schema and extending that definition by adding those elements not included in LEXS. [free text field]
	Message Date/Time	A timestamp identifying when this message was received.
	Sequence Number	A number that uniquely identifies this message.
	Source Reliability Code	Reliability of the source, in the assessment of the reporting organization: could be one of 'reliable', 'unreliable', or 'unknown'
	Content Validity Code	Validity of the content, in the assessment of the reporting organization: could be one of 'confirmed', 'doubtful', or 'cannot be judged'
	Nature of Source-Code	Nature of the source: Could be one of 'anonymous tip', 'confidential source', 'trained interviewer', 'written statement – victim, witness, other', 'private sector', or 'other source'
	Nature of Source-Text	Optional information of 'other source' is selected above. [free text field]
	Submitting Organization	
	Organization Name	Common Name of the fusion center or ISE participant that submitted the ISE-SAR record to the ISE. [free text field]
	Organization ID	Fusion center or ISE participant's alpha-numeric identifier. [free text field]
	Organization ORI	ORI for the submitting fusion center or ISE participant. [free text field]
	System ID	Identifies the system within the fusion center or ISE participant that is submitting the ISE-SAR. [free text field]
	Suspicious Activity	
	Activity End Date	The end or completion date in Greenwich Mean Time (GMT) of an incident that occurs over a duration of time.
	Activity End Time	The end or completion time in GMT of day of an incident that occurs over a duration of time.
	Activity Start Date	The date in GMT when the incident occurred or the start date if the incident occurs over a period of time.
	Activity Start Time	The time of day in GMT that the incident occurred or started.
	Observation Description Text	Description of the activity including rationale for potential terrorism nexus. [free text field]
	Observation End Date	The end or completion date in GMT of the observation of an activity that occurs over a duration of time.
	Observation End Time	The end or completion time of day in GMT of the observation of an activity that occurred over a period of time.

UNCLASSIFIED

ISE-FS-200

Privacy Field	Source Class/Element	Source Definition
	Observation Start Date	The date in GMT when the observation of an activity occurred or the start date if the observation of the activity occurred over a period of time.
	Observation Start Time	The time of day in GMT that the observation of an activity occurred or started.
	Threat Type Code	Broad category of threat to which the tip or lead pertains. Includes Financial Incident, Suspicious Activity, and Cyber Crime.
	Threat Type Detail Text	Breakdown of the Tip Type, it indicates the type of threat to which the tip or lead pertains. The subtype is often dependent on the Tip Type. For example, the subtypes for a nuclear/radiological tip class might be Nuclear Explosive or a Radiological Dispersal Device. [free text field]
	Suspicious Activity Code	Indicates the type of threat to which the tip or lead pertains. Examples include a biological or chemical threat.
	Weather Condition Details	The weather at the time of the suspicious activity. The weather may be described using codified lists or text.
	Target	
	Critical Infrastructure Indicator	Critical infrastructure, as defined by 42 USC Sec. 5195c, means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
	Infrastructure Sector Code	The broad categorization of the infrastructure type. These include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government.
	Infrastructure Tier Text	Provides additional detail that enhances the Target Sector Code. For example, if the target sector is Utilities, this field would indicate the type of utility that has been targeted such as power station or power transmission. [free text field]
	Structure Type Code	National Data Exchange (N-DEx) Code that identifies the type of Structure that was involved in the incident.
	Target Type Text	Describes the target type if an appropriate sector code is not available. [free text field]
	Structure Type Text	Text for use when the Structure Type Code does not afford necessary code. [free text field]
	Target Description Text	Text describing the target (e.g., Lincoln Bridge). [free text field]
	Vehicle	
	Color Code	Code that identifies the primary color of a vehicle involved in the suspicious activity.
	Description	Text description of the entity. [free text field]
	Make Name	Code that identifies the manufacturer of the vehicle.
	Model Name	Code that identifies the specific design or type of vehicle made by a manufacturer—sometimes referred to as the series model.
	Style Code	Code that identifies the style of a vehicle. [free text field]
	Vehicle Year	A 4-digit year that is assigned to a vehicle by the manufacturer.

UNCLASSIFIED

ISE-FS-200

Privacy Field	Source Class/Element	Source Definition
X	Vehicle Identification Number	Used to uniquely identify motor vehicles. [free text field]
X	US DOT Number	An assigned number sequence required by Federal Motor Carrier Safety Administration (FMCSA) for all interstate carriers. The identification number (found on the power unit, and assigned by the U.S. Department of Transportation or by a State) is a key element in the FMCSA databases for both carrier safety and regulatory purposes. [free text field]
	Vehicle Description	A text description of a vehicle. Can capture unique identifying information about a vehicle such as damage, custom paint, etc. [free text field]
	Related ISE-SAR	
	Fusion Center ID	Identifies the fusion center that is the source of the ISE-SAR. [free text field]
	Fusion Center ISE-SAR Record ID	Identifies the fusion center ISE-SAR record identifier for reports that are possibly related to the current report.
	Relationship Description Text	Describes how this ISE-SAR is related to another ISE-SAR. [free text field]
	Vessel	
X	Vessel Official Coast Guard Number Identification	An identification for the Official (U.S. Coast Guard Number of a vessel). Number is encompassed within valid marine documents and permanently marked on the main beam of a documented vessel. [free text field]
X	Vessel ID	A unique identifier assigned to the boat record by the agency—used for referencing [free text field]
	Vessel ID Issuing Authority	Identifies the organization authorization over the issuance of a vessel identifier. Examples of this organization include the State Parks Department and the Fish and Wildlife department. [free text field]
X	Vessel IMO Number Identification	An identification for an International Maritime Organization Number (IMO number) of a vessel [free text field]
	Vessel MMSI Identification	An identification for the Maritime Mobile Service Identity (MMSI) or a vessel [free text field]
	Vessel Make	Code that identifies the manufacturer of the boat.
	Vessel Model	Model name that identifies the specific design or type of boat made by a manufacturer—sometimes referred to as the series model.
	Vessel Model Year	A 4-digit year that is assigned to a boat by the manufacturer.
	Vessel Name	Complete boat name and any numerics. [free text field]
	Vessel Hailing Port	The identifying attributes of the hailing port of a vessel [free text field]
	Vessel National Flag	A data concept for a country under which a vessel sails. [free text field]
	Vessel Overall Length	The length measurement of the boat, bow to stern.
	Vessel Overall Length Measure	Code that identifies the measurement unit used to determine the boat length. [free text field]
X	Vessel Serial Number	The identification number of a boat involved in an incident. [free text field]
	Vessel Type Code	Code that identifies the type of boat.

UNCLASSIFIED

ISE-FS-200

Privacy Field	Source Class/Element	Source Definition
	Vessel Propulsion Text	Text for use when the Boat Propulsion Code does not afford necessary code. [free text field]

B. Association Descriptions

This section defines specific data associations contained in the ISE-SAR data model structure. Reference Figure 2 (UML-based model) for the graphical depiction and detailed elements.

Table 3 – ISE-SAR Data Model Structure Associations

Link Between Associated Components	Target Element
Link From Suspicious Activity Report to Attachment	lexs:Digest/lexsdigest:Associations/lexsdigest:EntityAttachmentLinkAssociation
Link From Suspicious Activity Report to Sensitive Information Details	Hierarchical Association
Link From Suspicious Activity Report to ISE-SAR Submission	Hierarchical Association
Link From Suspicious Activity to Vehicle	lexs:Digest/lexsdigest:Associations/lexsdigest:IncidentInvolvedItemAssociation
Link From Vehicle to Registration	Hierarchical Association
Link From Suspicious Activity to Vessel	lexs:Digest/lexsdigest:Associations/lexsdigest:IncidentInvolvedItemAssociation
Link From Suspicious Activity to Aircraft	lexs:Digest/lexsdigest:Associations/lexsdigest:IncidentInvolvedItemAssociation
Link From Suspicious Activity to Location	lexs:Digest/lexsdigest:Associations/lexsdigest:ActivityLocationAssociation
Link From Suspicious Activity to Target	Hierarchical Association
Link From Location to Location Coordinates	Hierarchical Association
Link From Location to Location Address	Hierarchical Association
Link From Suspicious Activity Report to Related ISE-SAR	Hierarchical Association
Link From Person to Location	lexs:Digest/lexsdigest:Associations/lexsdigest:PersonLocationAssociation
Link From Person to Contact Information	lexs:Digest/lexsdigest:Associations/lexsdigest:EntityEmailAssociation or lexs:Digest/lexsdigest:Associations/lexsdigest:EntityTelephoneNumberAssociation
Link From Person to Driver License	Hierarchical Association
Link From Person to Passport	Hierarchical Association
Link From Person to Other Identifier	Hierarchical Association

UNCLASSIFIED

ISE-FS-200

Link Between Associated Components	Target Element
Link From Person to Physical Descriptors	Hierarchical Association
Link From Person to Physical Feature	Hierarchical Association
Link From Person to Person Name	Hierarchical Association
Link From Suspicious Activity Report to Follow-Up Action	Hierarchical Association
Link From Target to Location	lexs:Digest/lexsdigest:Associations/lexsdigest:ItemLocationAssociation
Link From Suspicious Activity Report to Organization	Hierarchical Association
Link From Suspicious Activity to Person [Witness]	lexs:Digest/lexsdigest:Associations/lexsdigest:IncidentWitnessAssociation
Link From Suspicious Activity to Person [Person Of Interest]	lexs:Digest/lexsdigest:Associations/lexsdigest:PersonOfInterestAssociation
Link From Organization to Target	ext:SuspiciousActivityReport/nc:OrganizationItemAssociation
Link from ISE-SAR Submission to Submitting Organization	Hierarchical Association
Link From Submitting Organization to Contact Information	Hierarchical Association (Note that the mapping indicates context and we are not reusing Contact Information components)

C. Extended XML Elements

Additional data elements are also identified as new elements outside of NIEM, Version 2.0. These elements are listed below:

AdditionalDetailsIndicator: Identifies whether more ISE-SAR details are available at the authoring/originating agency than what has been provided in the information exchange.

AssignedByText: Organizational identifier that describes the organization performing a follow-up activity. This is designed to keep all parties interested in a particular ISE-SAR informed of concurrent investigations.

AssignedToText: Text describing the person or sub-organization that will be performing the designated follow-up action.

ClassificationReasonText: A reason why the classification was made as such.

ContentValidityCode: Validity of the content, in the assessment of the reporting organization: could be one of 'confirmed', 'doubtful', or 'cannot be judged'.

UNCLASSIFIED

ISE-FS-200

Conveyance track/intent: A direction by heading and speed or enroute route and/or waypoint of conveyance.

Critical Infrastructure Indicator: Critical infrastructure, as defined by 42 USC Sec. 5195c, means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

ICAO Airfield Code for Departure: An International Civil Aviation Organization (ICAO) airfield code for departure, indicates aircraft, crew, passengers, and cargo-on conveyance location information.

ICAO Airfield Code for Planned Destination: An airfield code for planned destination, indicates aircraft, crew, passengers, and cargo on conveyance location information.

ICAO for Actual Destination: An airfield code for actual destination. Indicates aircraft, crew, passengers, and cargo on conveyance location information.

ICAO Airfield for Alternate: An airfield code for Alternate. Indicates aircraft, crew, passengers, and cargo on conveyance location information.

Nature of Source-Code: Nature of the source: Could be one of ‘anonymous tip’, ‘confidential source’, ‘trained interviewer’, ‘written statement – victim, witness, other’, ‘private sector’, or ‘other source’.

Privacy Field Indicator: Data element that may be used to identify an individual and therefore is subject to protection from disclosure under applicable privacy rules. Removal of privacy fields from a detailed report will result in a summary report. This privacy field informs users of the summary information exchange that additional information may be available from the originator of the report.

Report Purge Date: The date by which the privacy fields will be purged from the record system; general observation data is retained. Purge policies vary from jurisdiction to jurisdiction and should be indicated as part of the guidelines.

Report Purge Review Date: Date of review to determine the disposition of the privacy fields in a Detailed ISE-SAR IEPD record.

Source Reliability Code: Reliability of the source, in the assessment of the reporting organization: could be one of ‘reliable’, ‘unreliable’, or ‘unknown’.

Vessel Hailing Port: The identifying attributes of the hailing port of a vessel.

Vessel National Flag: A data concept for a country under which a vessel sails.

UNCLASSIFIED

ISE-FS-200

SECTION V – INFORMATION EXCHANGE IMPLEMENTATION ARTIFACTS

A. Domain Model

1. General Domain Model Overview

The domain model provides a visual representation of the business data requirements and relationships (Figure 2). This Unified Modeling Language (UML)-based Model represents the Exchange Model artifact required in the information exchange development methodology. The model is designed to demonstrate the organization of data elements and illustrate how these elements are grouped together into Classes. Furthermore, it describes relationships between these Classes. A key consideration in the development of a Domain Model is that it must be independent of the mechanism intended to implement the model. The domain model is actually a representation of how data is structured from a *business* context. As the technology changes and new Functional Standards emerge, developers can create new standards mapping documents and schema tied to a new standard without having to re-address business process requirements.

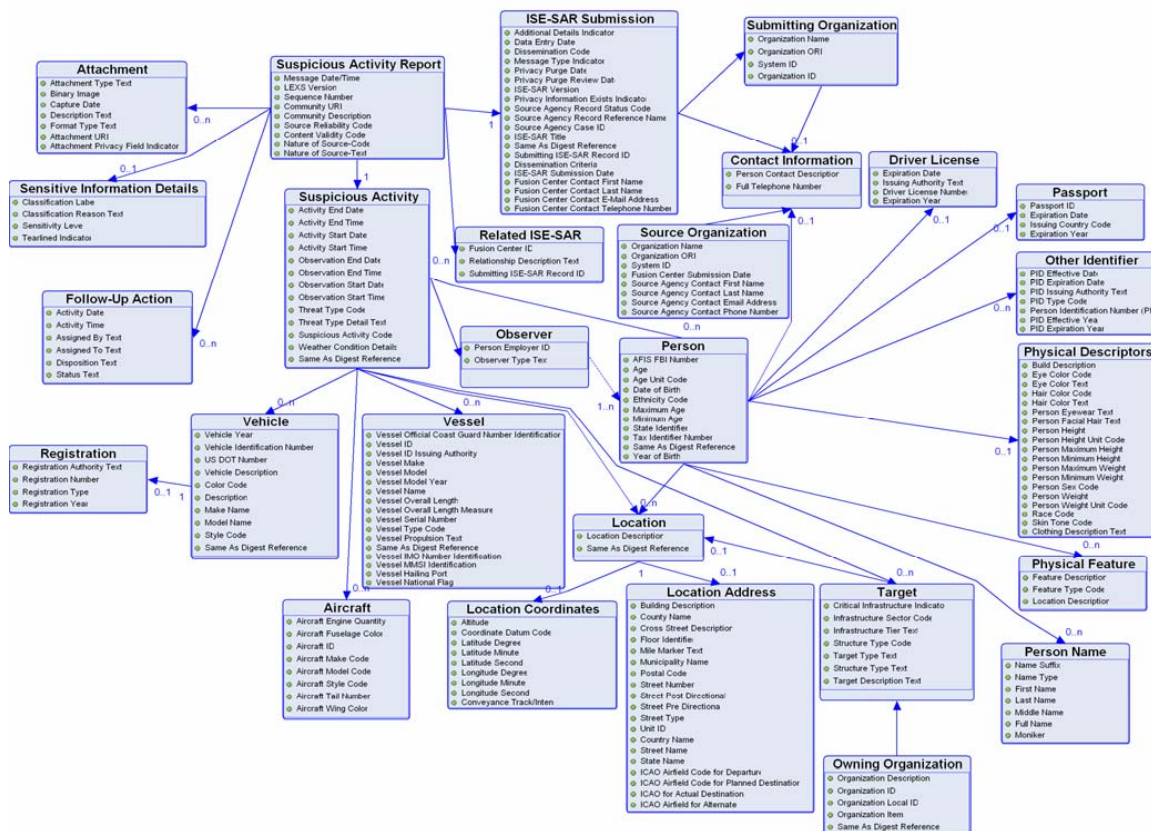


Figure 2 – UML-based Model

UNCLASSIFIED

ISE-FS-200

B. General Mapping Overview

The detailed component mapping template provides a mechanism to cross-reference the business data requirements documented in the Domain Model to their corresponding XML Element in the XML Schema. It includes a number of items to help establish equivalency including the business definition and the corresponding XML Element Definition.

C. ISE-SAR Mapping Overview

The Mapping Spreadsheet contains seven unique items for each ISE-SAR data class and element. The Mapping Spreadsheet columns are described in this section.

Table 4 – Mapping Spreadsheet Column Descriptions

Spreadsheet Name & Row	Description
Privacy Field Indicator	This field indicates that the information may be used to identify an individual.
Source Class/Element	Content in this column is either the data class (grouping of data elements) or the actual data elements. Classes are highlighted and denoted with cells that contain blue background while elements have a white background. The word "Source" is referring to the ISE-SAR information exchange.
Source Definition	The content in this column is the class or element definition defined for this ISE-SAR information exchange. The word "Source" is referring to the ISE-SAR information exchange definition.
Target Element	The content in this column is the actual namespace path deemed equal to the related ISE-SAR information exchange element.
Target Element Definition	The content in this column provides the definition of the target or NIEM element located at the aforementioned source path. "Target" is referring to the NIEM definition.
Target Element Base	Indicates the data type of the terminal element. Data types of niem-xsd:String or nc:TextType indicate free-form text fields.
Mapping Comments	Provides technical implementation information for developers and implementers of the information exchange.

D. Schemas

The *ISE-SAR Functional Standard* contains the following compliant schemas;

- Subset Schema
- Exchange Schema
- Extension Schema
- Wantlist

UNCLASSIFIED

ISE-FS-200

E. Examples

The *ISE-SAR Functional Standard* contains two samples that illustrate exchange content as listed below.

1. XSL Style Sheet

This information exchange artifact provides an implementer and users with a communication tool which captures the look and feel of a familiar form, screen, or like peripheral medium for schema translation testing and user validation of business rules.

2. XML Instance

This information exchange artifact provides an actual payload of information with data content defined by the schema(s).

UNCLASSIFIED

ISE-FS-200

PART B – ISE-SAR CRITERIA GUIDANCE

Category	Description
DEFINED CRIMINAL ACTIVITY AND POTENTIAL TERRORISM NEXUS ACTIVITY	
Breach/Attempted Intrusion	Unauthorized personnel attempting to or actually entering a restricted area or protected site. Impersonation of authorized personnel (e.g. police/security, janitor).
Misrepresentation	Presenting false or misusing insignia, documents, and/or identification, to misrepresent one's affiliation to cover possible illicit activity.
Theft/Loss/Diversion	Stealing or diverting something associated with a facility/infrastructure (e.g., badges, uniforms, identification, emergency vehicles, technology or documents (classified or unclassified), which are proprietary to the facility).
Sabotage/Tampering/Vandalism	Damaging, manipulating, or defacing part of a facility/infrastructure or protected site.
Cyber Attack	Compromising, or attempting to compromise or disrupt an organization's information technology infrastructure.
Expressed or Implied Threat	Communicating a spoken or written threat to damage or compromise a facility/infrastructure.
Aviation Activity	Operation of an aircraft in a manner that reasonably may be interpreted as suspicious, or posing a threat to people or property. Such operation may or may not be a violation of Federal Aviation Regulations.
POTENTIAL CRIMINAL OR NON-CRIMINAL ACTIVITY REQUIRING ADDITIONAL FACT INFORMATION DURING INVESTIGATION¹¹	
Eliciting Information	Questioning individuals at a level beyond mere curiosity about particular facets of a facility's or building's purpose, operations, security procedures, etc., that would arouse suspicion in a reasonable person.
Testing or Probing of Security	Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel or cyber security capabilities.
Photography	Taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person. Examples include taking pictures or video of infrequently used access points, personnel performing security functions (patrols, badge/vehicle checking), security-related equipment (perimeter fencing, security cameras), etc.

¹¹ Note: These activities are generally First Amendment-protected activities and should not be reported in a SAR or ISE-SAR absent articulable facts and circumstances that support the source agency's suspicion that the behavior observed is not innocent, but rather reasonably indicative of criminal activity associated with terrorism, including evidence of pre-operational planning related to terrorism. Race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion (although these factors may be used as specific suspect descriptions).

UNCLASSIFIED

ISE-FS-200

Category	Description
Observation/Surveillance	Demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional (e.g. engineers) interest such that a reasonable person would consider the activity suspicious. Examples include observation through binoculars, taking notes, attempting to measure distances, etc.
Materials Acquisition/Storage	Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, fuel, chemicals, toxic materials, and timers, such that a reasonable person would suspect possible criminal activity.
Acquisition of Expertise	Attempts to obtain or conduct training in security concepts; military weapons or tactics; or other unusual capabilities that would arouse suspicion in a reasonable person.
Weapons Discovery	Discovery of unusual amounts of weapons or explosives that would arouse suspicion in a reasonable person.
Sector-Specific Incident	Actions associated with a characteristic of unique concern to specific sectors (such as the public health sector), with regard to their personnel, facilities, systems or functions.

UNCLASSIFIED

ISE-FS-200

PART C – ISE-SAR INFORMATION FLOW DESCRIPTION

Step	Activity	Process	Notes
1	Observation	The information flow begins when a person observes behavior or activities that would appear suspicious to a reasonable person. Such activities could include, but are not limited to, expressed or implied threats, probing of security responses, site breach or physical intrusion, cyber attacks, indications of unusual public health sector activity, unauthorized attempts to obtain precursor chemical/agents or toxic materials, or other usual behavior or sector-specific incidents. ¹²	The observer may be a private citizen, a government official, or a law enforcement officer.

¹² Suspicious activity reporting (SAR) is official documentation of observed behavior that may be reasonably indicative of intelligence gathering and/or pre-operational planning related to terrorism or other criminal activity. ISE-SARs are a subset of all SARs that have been determined by an appropriate authority to have a potential nexus to terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism).

UNCLASSIFIED

ISE-FS-200

Step	Activity	Process	Notes
2	Initial Response and Investigation	<p>An official of a Federal, State, local, or tribal agency with jurisdiction responds to the reported observation.¹³ This official gathers additional facts through personal observations, interviews, and other investigative activities. This may, at the discretion of the official, require further observation or engaging the subject in conversation. Additional information acquired from such limited investigative activity could then be used to determine whether to dismiss the activity as innocent or escalate to the next step of the process. In the context of priority information requirements, as provided by State and major urban area fusion centers, the officer/agent may use a number of information systems to continue the investigation. These systems provide the officer/agent with a more complete picture of the activity being investigated. Some examples of such systems and the information they may provide include:</p> <p>Department of Motor Vehicles provides drivers license and vehicle registration information; National Crime Information Center provides wants and warrants information, criminal history information and access to the Terrorist Screening Center and the terrorist watch list, Violent Gang/Terrorism Organization File (VGTOF), and Regional Information Sharing System (RISS); Other Federal, State, local, and tribal systems can provide criminal checks within the immediate and surrounding jurisdictions.</p> <p>When the initial investigation is complete, the official documents the event. The report becomes the initial record for the law enforcement or Federal agency's records management system (RMS).</p>	<p>The event may be documented using a variety of reporting mechanisms and processes, including but not limited to, reports of investigation, event histories, field interviews (FI), citations, incident reports, and arrest reports.</p> <p>The record may be hard and/or soft copy and does not yet constitute an ISE-SAR.</p>

¹³ If a suspicious activity has a direct connection to terrorist activity the flow moves along an operational path. Depending upon urgency, the information could move immediately into law enforcement operations and lead to action against the identified terrorist activity. In this case, the suspicious activity would travel from the initial law enforcement contact directly to the law enforcement agency with enforcement responsibility.

UNCLASSIFIED

ISE-FS-200

Step	Activity	Process	Notes
3	Local/Regional Processing	<p>The agency processes and stores the information in the RMS following agency policies and procedures. The flow will vary depending on whether the reporting organization is a State or local agency or a field element of a Federal agency.</p> <p>State, local, and tribal: Based on specific criteria or the nature of the activity observed, the State, local, and tribal law enforcement components forward the information to the State or major urban area fusion center for further analysis.</p> <p>Federal: Federal field components collecting suspicious activity would forward their reports to the appropriate resident, district, or division office. This information would be reported to field intelligence groups or headquarters elements through processes that vary from agency to agency.</p> <p>In addition to providing the information to its headquarters, the Federal field component would provide an information copy to the State or major urban area fusion center in its geographic region. This information contributes to the assessment of all suspicious activity in the State or major urban area fusion center's area of responsibility.</p>	<p>The State or major urban area fusion center should have access to all suspicious activity reporting in its geographic region whether collected by State, local, or tribal entities, or Federal field components.</p>
4	Creation of an ISE-SAR	<p>The determination of an ISE-SAR is a two-part process. First, at the State or major urban area fusion center or Federal agency, an analyst or law enforcement officer reviews the newly reported information against ISE-SAR behavior criteria. Second, based on available knowledge and information, the analyst or law enforcement officer determines whether the information meeting the criteria has a potential nexus to terrorism.</p> <p>Once this determination is made, the information becomes an "ISE-SAR" and is formatted in accordance with ISE-FS-200 (<i>ISE-SAR Functional Standard</i>). The ISE-SAR would then be shared with appropriate law enforcement and homeland security personnel in the State or major urban area fusion center's area of responsibility.</p>	<p>Some of this information may be used to develop criminal intelligence information or intelligence products which identifies trends and other terrorism related information and is derived from Federal agencies such as NCTC, DHS, and the FBI.</p> <p>For State, local, and tribal law enforcement, the ISE-SAR information may or may not meet the reasonable suspicion standard for criminal intelligence information. If it does, the information may also be submitted to a criminal intelligence information database and handled in accordance with 28 CFR Part 23.</p>

UNCLASSIFIED

ISE-FS-200

Step	Activity	Process	Notes
5	ISE-SAR Sharing and Dissemination	<p>In a State or major urban area fusion center, the ISE-SAR is shared with the appropriate FBI field components and the DHS representative and placed in the State or major urban area fusion center's ISE Shared Space or otherwise made available to members of the ISE.</p> <p>The FBI field component enters the ISE-SAR information into the FBI system and sends the information to FBI Headquarters.</p> <p>The DHS representative enters the ISE-SAR information into the DHS system and sends the information to DHS, Office of Intelligence Analysis.</p>	
6	Federal Headquarters (HQ) Processing	<p>At the Federal headquarters level, ISE-SAR information is combined with information from other State or major urban area fusion centers and Federal field components and incorporated into an agency-specific national threat assessment that is shared with ISE members.</p> <p>The ISE-SAR information may be provided to NCTC in the form of an agency-specific strategic threat assessment (e.g., strategic intelligence product).</p>	

UNCLASSIFIED

ISE-FS-200

Step	Activity	Process	Notes
7	NCTC Analysis	<p>When product(s) containing the ISE-SAR information are made available to NCTC, they are processed, collated, and analyzed with terrorism information from across the five communities—intelligence, defense, law enforcement, homeland security, and foreign affairs—and open sources.</p> <p>NCTC has the primary responsibility within the Federal government for analysis of terrorism information. NCTC produces federally coordinated analytic products that are shared through NCTC Online, the NCTC secure web site.</p> <p>The Interagency Threat Assessment and Coordinating Group (ITACG), housed at NCTC, facilitates the production of coordinated terrorism-related products that are focused on issues and needs of State, local, and tribal entities and when appropriate private sector entities. ITACG is the mechanism that facilitates the sharing of counterterrorism information with State, local, and tribal entities.</p>	
8	NCTC Alerts, Warnings, Notifications	<p>NCTC products¹⁴, informed by the ITACG as appropriate, are shared with all appropriate Federal departments and agencies and with State, local, and tribal entities through the State or major urban area fusion centers. The sharing with State, local, and tribal entities and private sector occurs through the Federal departments or agencies that have been assigned the responsibility and have connectivity with the State or major urban area fusion centers. Some State or major urban area fusion centers, with secure connectivity and an NCTC Online account, can access NCTC products directly. State or major urban area fusion centers will use NCTC and ITACG informed products to help develop geographic-specific risk assessments (GSRA) to facilitate regional counterterrorism efforts. The GSRA are shared with State, local, and tribal entities and the private sector as appropriate. The recipient of the GSRA may use the GSRA to develop information gathering priorities or requirements.</p>	<p>NCTC products form the foundation of informational needs and guide collection of additional information.</p> <p>NCTC products should be responsive to informational needs of State, local, and tribal entities.</p>
9	Focused Collection	<p>The information has come full circle and the process begins again, informed by an NCTC or other Federal organization's product and the identified information needs of State, local and tribal entities and Federal field components.</p>	

¹⁴ NCTC product include: Alerts, warnings, and notifications—identifying time sensitive or strategic threats; Situational awareness reports; and Strategic and foundational assessments of terrorist risks and threats to the United States and related intelligence information.

UNCLASSIFIED

ISE-FS-200

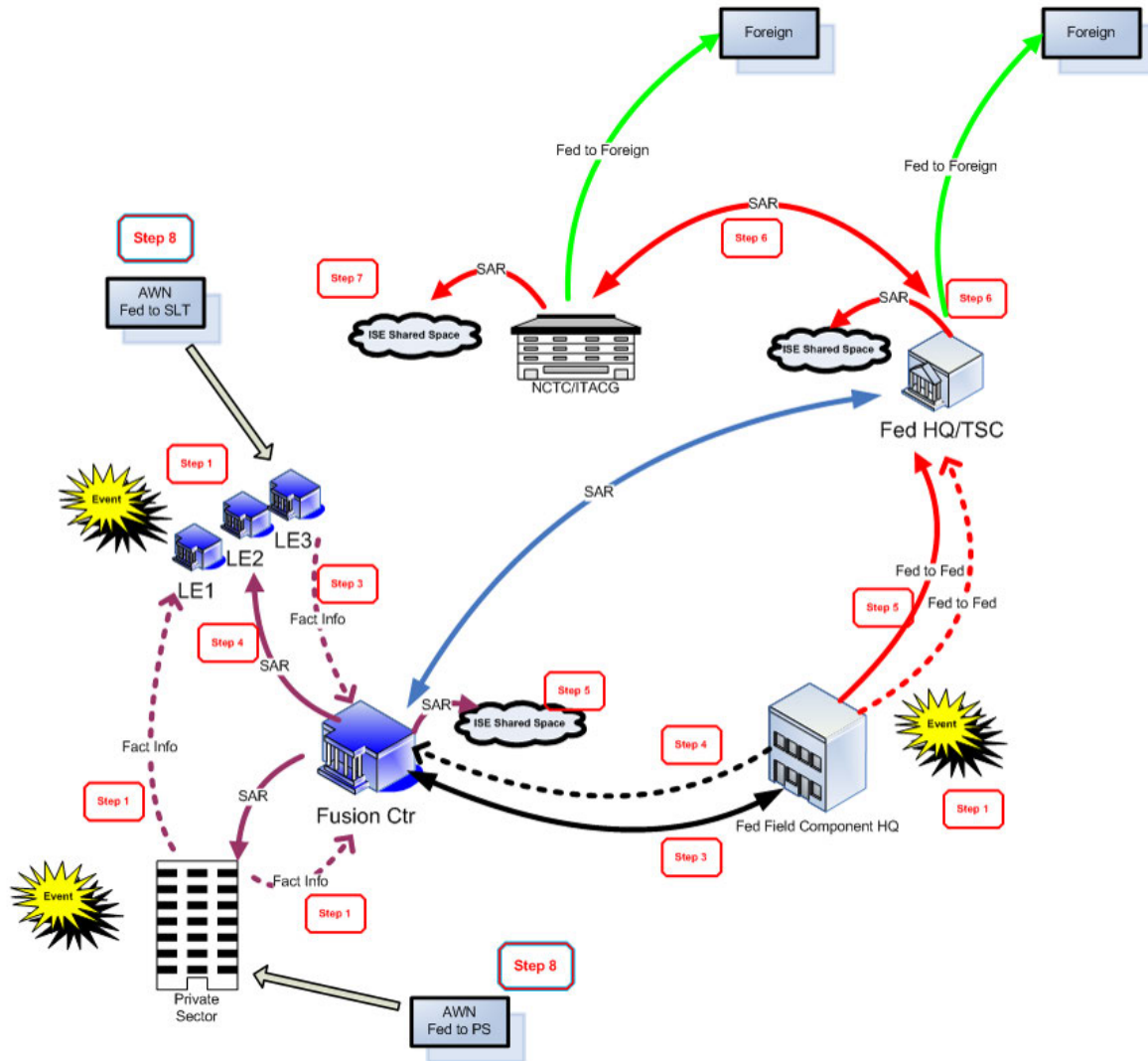


Figure 3 – SAR Information Flow Diagram



Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations

Nationwide Suspicious Activity Reporting Initiative

Prepared by the
Program Manager, Information Sharing Environment

July 2010

For more information, go to:

www.ise.gov

NSI Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations

experiences varied,¹¹ all sites recognized the importance of maintaining strong privacy, civil rights, and civil liberties protections in every facet of the SAR process, including implementation of both privacy policies and the requirements of the Functional Standard. The experiences of the EE participating sites helped to shape the following recommendations which must be integrated into the nationwide implementation of the NSI.

RECOMMENDATION 1: The NSI Privacy Protection Framework must be adopted and implemented as a condition of participation in the NSI, with careful consideration of the resources necessary for full implementation.

The ISE-SAR EE required each EE participating site to develop and adopt a written policy that satisfies applicable ISE Privacy Guideline requirements as a precondition to sharing or receiving any personal information contained in the Privacy Fields that are part of the Detailed ISE-SAR format.¹² The Federal partners' insistence on compliance with this requirement ensured that robust privacy policies were in place to protect the information before information sharing activities began; it also meant that the EE participating sites were delayed in sharing or receiving Privacy Field information, due to the fact that the EE participating sites typically spent an average length of six months developing and implementing their respective privacy policies.

To assist the EE participating sites and to promote a standardized approach for developing site ISE-SAR specific privacy policies, the Joint DHS/DOJ Privacy Technical Assistance Program developed privacy policy templates, offered technical assistance, and reviewed each EE participating site's privacy policy. Additionally, the EE participating sites availed themselves of legal and compliance experts at both the state and local levels to ensure that site ISE-SAR policies complied with state open records laws and other requirements.¹³

Going forward, NSI sites should anticipate that they will need to dedicate sufficient resources and attention to facilitate the full and uniform implementation of the NSI Privacy Framework. In addition to addressing all aspects of the framework in their policies and processes, NSI sites should also implement the following:

¹¹ ISE-SAR EE participating site experiences based upon such factors as the successful development of a privacy policy, the alignment of business processes, and the availability of training resources. For further information regarding the experiences of the EE participating sites, see Appendix B, Section C.

¹² EE participating sites were given three options for developing privacy policies that would qualify them to share and receive personal information contained in privacy fields. The options are set forth in Section IV (D) of this Analysis. Each EE participating site developed and provided a draft privacy policy to the Privacy Policy Review Team for assessment and feedback. Once the site's policies satisfied the privacy requirements of the review team, the completed policy was recommended for approval to the Privacy Guidelines Committee Co-Chairs (privacy officials from the Office of the Director of National Intelligence, the Department of Justice, and the Department of Homeland Security) and the PM-ISE. Upon approval, DOJ/BJA was formally notified that the EE participant was authorized to "go live" in sharing and receiving privacy field information in Shared Spaces under the EE.

¹³ See Appendix B, Section C (1) for further discussion.

NSI Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations

- a. At the beginning of the privacy development process, training on the NSI Privacy Framework and technical assistance must be provided to the designated privacy officer and the legal advisors at each NSI site;
- b. Each NSI participating site must conduct the NSI process pursuant to its statutory authorities and its privacy, civil rights, and civil liberties policies and procedures that are “at least as comprehensive” as the ISE Privacy Guidelines and the *Baseline Capabilities for State and Major Urban Area Fusion Centers* (Baseline Capabilities);
- c. Each NSI site must adopt and incorporate into existing business processes a formal and multi-layered vetting process in which each SAR is reviewed by a front-line supervisor and by an experienced investigator or analyst specifically trained in counterterrorism issues before it can be designated as an ISE-SAR;
- d. Standardized training for front-line officers, investigators, analytic, and supervisory personnel must be provided and required in order to educate personnel on the purpose and use of the multi-layered vetting process required in the Functional Standard; line officers, in particular, should receive specialized training to strengthen their ability to recognize the types of behavior that may be indicative of criminal activity associated with terrorism; and
- e. Local privacy, civil rights, and civil liberties advocates must be engaged at an early stage in the process to build trusted relationships between partners, the local community, and the public.

RECOMMENDATION 2: Going forward, it is imperative that each NSI site engage in outreach to members of the public, private sector partners, and privacy, civil rights, and civil liberties advocacy groups during its privacy policy development and updating process.

The ISE-SAR EE emphasized the importance of a transparent process and collaboration with the public and with privacy, civil rights, and civil liberties advocacy groups. During the EE, sites worked to provide transparency and to collaborate with the public in various ways, including:

- a. EE participating sites with formalized community outreach programs successfully leveraged this resource for communicating the SAR process to the public;
- b. Several sites noted plans to implement a community outreach model similar to Los Angeles Police Department’s (LAPD) iWatch program;
- c. Three sites took advantage of the Building Communities of Trust initiative pilot which provided sites with opportunities to engage with community advocacy groups through planning meetings and roundtable events;¹⁴

¹⁴ The Building Communities of Trust initiative aims to build bridges and mutual understanding among the community groups, local law enforcement agencies, and state and major urban area fusion centers as a way of better protecting our local communities. The intent is that law enforcement officers, public safety personnel, community leaders, and citizens will be better

ISE information. This would enable the government to achieve efficiencies and to better integrate operations that use all sources of information to carry out agency missions.

IV. Policies and Processes Supporting the NSI Privacy Framework

A. Recommendations of the *Initial Privacy and Civil Liberties Analysis*

The *Initial Privacy and Civil Liberties Analysis* included a number of recommendations to ISE-SAR EE participating sites designed to ensure the protection of privacy, civil rights, and civil liberties in the SAR EE. The recommendations urged the ISE-SAR EE participants to:

1. Promote a policy of openness and transparency when communicating to the public regarding their SAR process;
2. Integrate the management of terrorism-related suspicious information with processes and systems used to manage other crime-related information and criminal intelligence, thereby leveraging existing policies and protocols that protect the information privacy, civil liberties, and other legal rights of Americans; clearly articulate when 28 CFR Part 23 should be applied;
3. Ensure privacy and civil liberties policies address core privacy principles, such as accuracy, redress, retention/disposition, and disclosure of personally identifying information, consistent with Federal, State, and local statutory and regulatory requirements;
4. Evaluate and, as necessary, update privacy and civil liberties policies to ensure that they specifically address the gathering, documenting, processing, and sharing of terrorism-related information;
5. Audit SARs for quality and substance to ensure that the integrity of the SAR program is maintained; and
6. Use legal and privacy advisors in the development of the SAR process.

These recommendations were integrated into the EE participating sites' privacy policies, procedures, and business processes as the ISE-SAR EE evolved and now serve as the foundation for the NSI Privacy Framework.

B. Strengthening the NSI Privacy Framework through Collaboration with Privacy, Civil Rights, and Civil Liberties Advocacy Groups

The Program Manager for the Information Sharing Environment (PM-ISE) and its Federal partners ensured transparency of and strengthened privacy, civil rights, and civil liberties protective measures for the NSI through consultation and collaboration with privacy, civil

throughout the NSI process, but also improve the quality of the information on which analytic and investigative judgments are based.

C. The Revised ISE-SAR Functional Standard

The *National Strategy for Information Sharing*¹⁸ identified “suspicious activity reporting” as one of the key information exchanges to be effected between and among Federal and SLT governments. In furtherance of this strategy, the PM-ISE led the development of a standardized process known as the ISE-SAR Functional Standard¹⁹ and an associated data model. This standard enables government analysts and officers with law enforcement, homeland security, and counterterrorism responsibilities to discover and identify potential terrorist activities and trends.

The ISE-SAR Functional Standard supports the identification, documentation, and sharing of ISE-SAR information to the maximum extent possible, and in a manner that is consistent with privacy, civil rights, and civil liberties protections. Following extensive collaboration with privacy, civil rights, and civil liberties advocates, the PM-ISE implemented key revisions to the ISE-SAR Functional Standard in May 2009. The revisions refined the SAR information collection and SAR/ISE-SAR determination process in order to ensure that ISE-SARs are “reasonably indicative of criminal activity associated with terrorism.” Simply put, the “reasonably indicative” language applies to the identification of SAR information and, when coupled with the two-step review and vetting process at the fusion center, defines the permissible scope of what information may be included in the shared space environment.²⁰

1. *The Process for Identifying, Documenting, and Sharing SAR Information and the Protection of Privacy, Civil Rights, and Civil Liberties of Americans*

The revisions to the Functional Standard enable NSI sites to better detect and prevent terrorism-related crime with increased safeguards for protecting privacy, civil rights, and civil liberties.

The revised Functional Standard delineates the process for identifying, documenting, and sharing ISE-SAR information by identifying the types of behavior that may be terrorism-related and the circumstances under which such information may be retained and shared.²¹

¹⁸ *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing* (October 2007).

¹⁹ See Version 1.5 of the ISE-SAR Functional Standard.

²⁰ It does not set a standard for permissible police investigations -- investigations and detentions continue to be governed by applicable law and source agency policy.

²¹ The EE partners worked closely with privacy and civil liberties advocates to address and mitigate privacy and civil liberties concerns raised by the original Functional Standard (Version 1.0). One area of concern focused on the requirement that SARs and

The revision of the Functional Standard establishes that “reasonably indicative” determinations apply to both the collection of SAR information and the identification of an ISE-SAR to be shared with law enforcement, homeland security, and counterterrorism agencies. To be considered an ISE-SAR, the terrorism-related activity must conform to one or more of the criteria identified in Part B of the ISE-SAR Functional Standard.²²

The use of the “reasonably indicative” determination process allows supervisors at source agencies and trained analysts and investigators at fusion centers and other agencies to have a uniform process that will result in better quality SARs and the posting of more reliable ISE-SARs to the ISE Shared Spaces, while at the same time enhancing privacy, civil rights, and civil liberties protections. Furthermore, this revision improves mission effectiveness and enables NSI participating agency personnel to identify and address, in a more efficient manner, potential criminal and terrorism threats by using more narrowly targeted language. Finally, better quality SARs should result in a sufficiently high quality of information enabling agencies and analysts to “connect the dots” while not producing so much information as to overwhelm agency analytical capacity.

In addition, the “reasonably indicative” determination is an essential privacy, civil rights, and civil liberties protection because it emphasizes a behavior-focused approach to identifying

ISE-SARs be based on “[o]fficial documentation of observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention.” SARs and ISE-SARs are distinguishable in that ISE-SARs would also be coupled with a determination that the SAR has a “potential terrorism nexus.” The advocates’ concern was that language in Version 1.0 (“may be indicative”) was too loose, allowing “mere suspicion” to be the basis for a SAR or an ISE-SAR to be collected and shared by a law enforcement or counter-terrorism agency. One response to this concern was to revise the language; under Version 1.5, the language “reasonably indicative of pre-operational planning related to terrorism or other criminal activity” applies to the collection of SAR information and the identification of an ISE-SAR based on the two-step review process to determine if it has a potential terrorism nexus.

Other changes reflected in Version 1.5 of the Functional Standard include: (1) Clarifying that the same constitutional standards that apply when conducting ordinary criminal investigations also apply to law enforcement and homeland security officers conducting SAR inquiries; (2) Refining the ISE-SAR Criteria Guidance to distinguish between those activities that are “Defined Criminal Activity” and those that are “Potentially Criminal or Non-Criminal Activity,” requiring additional fact information during investigation; and (3) Clarifying those activities which are generally protected by the First Amendment that should not be reported in a SAR or ISE-SAR, absent facts and circumstances that can be clearly articulated and that support the source agency’s suspicion that the behavior observed is reasonably indicative of criminal activity associated with terrorism.

²² Before an agency can move SARs from the agency systems to the ISE, two forms of vetting must occur. Supervisors who initially receive a SAR from law enforcement officers, public safety agencies, private sector partners, or citizens must initially review the SAR to determine whether it has a nexus to terrorism and whether it includes the behaviors identified in the ISE-SAR Functional Standard. Trained analysts must then analyze the SAR against the behaviors identified in Part B of the ISE-SAR Functional Standard. Throughout the vetting process, privacy, civil rights, and civil liberties are vigilantly and actively protected through the training that analysts receive and through the system attributes that are a part of the NSI.

suspicious activity and mitigates the risk of profiling based upon race, ethnicity, national origin, or religious affiliation or activity.²³

2. *The Standardized, Multi-Level Vetting Process*

The implementation of the revised ISE-SAR Functional Standard (Version 1.5) constitutes an essential safeguard supporting the NSI Privacy Framework. This standard requires the use of a multi-level business process to identify information with a potential nexus to terrorism out of the thousands of suspicious activities documented by source agencies each day. Following information gathering by law enforcement officers who have been trained to recognize terrorism-related behaviors and a preliminary review by a local agency, a trained analyst or law enforcement officer at a fusion center or Federal agency would determine whether the suspicious activity is indicative of criminal behavior or activity associated with terrorism.²⁴ The analyst or officer would then determine whether the facts and circumstances, taken as a whole, support a determination that "... the information has a potential nexus to terrorism."²⁵ If this determination is made, the SAR will be documented and made available as an ISE-SAR to all appropriate ISE participants in the agency's Shared Space.²⁶

The enhancements to the ISE-SAR Functional Standard (Version 1.5) protect privacy, civil rights, and civil liberties by ensuring that information is submitted by trained staff; is gathered for a valid law enforcement or counterterrorism purpose; is subject to front-line supervisory review; and undergoes a formal two-step vetting process by an experienced investigator or analyst specifically trained in counterterrorism issues before being designated as an ISE-SAR.

²³ The revised Functional Standard expressly states that factors such as race, ethnicity, national origin, or religious affiliation or activity should not be considered as factors that create suspicion (except if used as part of a specific suspect description).

²⁴ The criteria for making this determination are set forth in Part B of the revised ISE-SAR Functional Standard (Version 1.5).

²⁵ An additional safeguard in the revised Functional Standard is the separation of potential terrorism-related behaviors into two categories: (1) those observed behaviors that are inherently criminal; and (2) those that involve the exercise of a constitutionally protected activity, but which may be criminal in nature. The revised Functional Standard provides that when the constitutionally protected behaviors are involved, there must be articulable facts and circumstances that support the officer or agency's suspicion that the behavior is not innocent, but rather reasonably indicative of criminal activity associated with terrorism.

²⁶ It is envisioned that agencies will share potential ISE-SAR information with State or major urban area fusion centers and, when appropriate and consistent with existing practice, the local FBI Joint Terrorism Task Force (JTTF). At the fusion center, analysts or law enforcement officers will evaluate the SAR against the ISE-SAR Functional Standard. If it meets criteria as defined in Part B of the revised ISE-SAR Functional Standard (Version 1.5), the fusion center will designate the SAR as an "ISE-SAR" and make it available to other ISE participants through the fusion center's ISE Shared Space. Documenting, analyzing, and sharing of ISE-SAR information between and among State, local, and tribal organizations, State or major urban area fusion centers, JTTFs, and other Federal field components is designed to provide early indications to all NSI participating agencies of behaviors and indicators of criminal activity associated with terrorism.

**EXECUTIVE SUMMARY OF KEY POLICY CHANGES
INCORPORATED IN THE PROPOSED INTERIM *ISE-SAR FUNCTIONAL STANDARD V. 1.5.5***

PURPOSE OF INTERIM UPDATE

The purpose for updating the 2009 *ISE-SAR Functional Standard Version 1.5* (FS v. 1.5) to version 1.5.5 (FS v. 1.5.5) is to develop an interim version of FS v. 1.5, clarifying a number of policy, operational, and technical issues that were identified in the implementation of the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), while reserving major substantive changes for FS v. 2.0. This process towards an interim solution has been underway for approximately three years.

PROCESS FOLLOWED FOR UPDATING FS v. 1.5

Since October 2012, the PM-ISE has facilitated discussions with key federal NSI stakeholders to identify appropriate updates to FS v. 1.5 and to reach interagency consensus on the proposed changes. The Office of the Director of National Intelligence, the Department of Homeland Security (DHS), the Department of Justice, the Federal Bureau of Investigation (FBI), and the NSI Program Management Office provided guidance and input on proposed language changes. This process included ISA IPC representatives, P/CRCL officials and staff, and operational staff. Following five major rounds of review, the stakeholders reached agreement on key policy updates for FS v. 1.5.5. The input provided represented the Department or agency's consensus position.

With the key policy updates in FS v. 1.5.5 completed, the National Security Council Staff hosted a Restricted Interagency Policy Committee (IPC) for the NSI on December 10, 2013, to consider next steps. During that meeting, the Restricted IPC participants agreed to delay the issuance of FS v. 1.5.5, pending: (1) necessary updates to the eGuardian Privacy Impact Assessment (PIA), to support the technical transition of the NSI, under which eGuardian will be used as a SAR Data Repository (SDR) for terrorism-related SARs (ISE-SARs); and (2) the completion of the new NSI technology plan and architecture. Since that meeting, the FBI has issued an interim update of the PIA for the eGuardian system, and the FBI and DHS have issued the revised NSI Concept of Operations (CONOPS).¹ The technology transition has been completed, and the recommended technical updates proposed by the FBI and DHS were incorporated in FS v. 1.5.5 in June 2014.

A number of substantive nontechnical updates were also offered by the FBI and DHS during this round, but most were not accepted since they exceeded the scope for the updates or reopened previously resolved substantive issues. The June 2014 draft version of the FS v. 1.5.5 was provided to the Privacy and Civil Liberties Oversight Board (PCLOB) for review in early July 2014. A limited number of advisory comments were received from the PCLOB in September 2014.

¹ The NSI CONOPS is not publicly available, but it is accessible to users with access to the Law Enforcement Online (LEO) network.

The federal interagency process culminated in November 2014 with a joint meeting of representatives from the Fusion Center/Suspicious Activity Reporting (FC/SAR) Subcommittee, the Privacy and Civil Liberties (P/CL) Subcommittee, and the PM-ISE. During the joint meeting, representatives of ODNI, DHS, DOJ, and the FBI reviewed and concurred with the proposed language contained in the current proposed version of ISE-SAR FS v. 1.5.5. DHS and FBI agreed to lead outreach and communication to state, local, tribal, and territorial mission partners regarding FS v. 1.5.5.

IMPROVEMENTS

A full summary of the updates to FS v. 1.5 can be found below. These updates improve the ISE-SAR FS by:

- A. Describing the current state of NSI implementation and providing a clear statement of NSI operational principles.
- B. Clarifying the ISE-SAR process and the P/CRCL protections incorporated into the FS.
- C. Clarifying key operational concepts, including providing a definition of “reasonably indicative.”
- D. Offering clarifying language for and descriptive examples of the 16 pre-operational behaviors that may have a potential nexus to terrorism.

These improvements benefit the American public and NSI operational stakeholders by providing:

- A. Transparency: The interim update accurately represents the current operational state of the NSI and allows the American public to clearly understand the NSI-wide policies and procedures under which NSI operational stakeholders are vetting SARs and submitting and sharing ISE-SARs.
- B. Clearer Guidance: The clarifications contained in FS v. 1.5.5 will improve the mission effectiveness of NSI operational stakeholders in vetting SARs to identify ISE-SARs and will enhance their understanding of the P/CRCL protections that have been integrated into the SAR vetting process and the sharing of ISE-SARs.

SUMMARY OF KEY CHANGES

Part A

- A. A number of administrative changes were required for technical and governance references, including the following:
 1. References to NIEM/UCore were replaced with NIEM.

2. References to CTISS Committee were changed to ISA IPC.
 3. References to the NSI PMO, the ISA IPC, and the P/CL Subcommittee were updated.
- B. Definitions were changed or added, including the following:
1. Definition of the key operational concept “reasonably indicative” was added.
 - a. Issue: ISE mission partners in the field requested that the updated FS define “reasonably indicative” to ensure a more consistent interpretation of this pivotal term by analysts/investigators and supervisors.
 - b. Anticipated Impact of Proposed Change: FS v. 1.5.5 clarifies that the “reasonably indicative” concept requires consideration during the vetting of a SAR of “the circumstances in which that observation is made, which creates in the mind of the reasonable observer, including a law enforcement officer, an articulable concern that the behavior may *indicate* pre-operational planning associated with terrorism or other criminal activity [note: emphasis added to indicate wording change for readers]. It also takes into account the training and experience of a reasonable law enforcement officer, in cases where an officer is the observer or documenter of the observed behavior reported to a law enforcement agency.” FS v. 1.5.5 also clarifies that for purposes of the evaluation and documentation of an ISE-SAR (See 5. h., above), the term “other criminal activity” must refer to criminal activity associated with terrorism, and must fall within the scope of the 16 terrorism pre-operational behaviors identified in Part B of this Functional Standard.
 2. Definition of “Nationwide SAR Initiative (NSI) SAR Data Repository (SDR)” was added to explain that the “NSI SDR consists of a single data repository, built to respect and support originator control and local stewardship of data, which incorporates federal, state and local retention policies. Within the SDR, hosted data enclaves extend this approach to information management and safeguarding practices by ensuring a separation of data across participating agencies.”
 3. Definition of “pre-operational planning” was added to clarify that this term refers to “the activities associated with a known or particular planned criminal operation or with terrorist operations generally.”
 4. Definitions for entities that are part of the NSI ecosystem were added, including “eGuardian,” “Field Intelligence Groups,” “fusion centers,” and “Joint Terrorism Task Forces.”
 5. Definitions for “owning agency/organization,” “source agency/organization” and “submitting agency/organization” were added.
- C. Language throughout Section II was updated to align with definitional language.
- D. A new section titled “Other Information Sharing Authorities” was added:

1. Issue: Mission partners solicited clarification of language in the FS regarding the sharing of other information or intelligence outside the ISE-SAR process.
2. This section explicitly recognizes that:
 - a. The ISE-SAR process does not supersede other information or intelligence gathering, collection, or sharing authority, including the authority to share information between and among Federal agencies and SLTT agencies where the information is related to homeland security, terrorism, or other Federal crimes.
 - b. Multiple Federal agencies have authority to collect terrorism-related tips and leads. Only those tips and leads which comply with the ISE-SAR Functional Standard are broadly shared with NSI participants. At the SLTT level, crime and terrorism information, including terrorism-related non-ISE-SAR information, can and should be reported to appropriate Federal agencies based on their relevant legal authorities.
 - c. Reports determined not to be ISE-SARs will be handled and shared in accordance with applicable SLTT and other agencies' authorities, policies, and procedures.
3. Anticipated Impact of Change: Mission partners and the public will understand that multi-directional sharing of non-ISE-SAR information takes place outside the NSI. Consequently, while systems involved in the NSI can be used in the exercise of other agency authorities related to information and intelligence collection, sharing, and analysis, information sharing outside the scope of the ISE-SAR Functional Standard must be done in accordance with other agency legal authorities, policies and procedures, and interagency agreements.
- E. Technical changes were incorporated to align FS v. 1.5.5 with the technical and business process changes to the NSI that were implemented in January 2014.
- F. Three additional protected categories for "gender," "gender identity," and "sexual orientation" were added to prohibitions against profiling to align FS v. 1.5.5 language with DOJ's *Guidance for Federal Law Enforcement Agencies regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity* (December 2014).

Part B

- A. The ISE-SAR criteria guidance is revised to:
 1. Further clarify the use of Part B for analysts/investigators.
 - a. Issue: The NSI stakeholders determined that additional guidance on the behavior categories and criteria would help analysts/investigators in the review, documentation, and submission of an ISE-SAR.
 - b. Anticipated Impact of Proposed Change: Part B now includes a more thorough explanation of ISE-SAR pre-operational behavioral categories and criteria. This

guidance will help the NSI mission partners better understand the importance of having a trained analyst or investigator take into account the context, facts, and circumstances in reviewing SARs to identify those with a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism).

2. Identify a new dual-track process to be used to update Part B, including a formal ISA IPC process for reviewing and updating the 16 behavioral categories and the behavioral criteria and a separate, less formal process guided by the DHS, in conjunction with the FBI, to allow for interim updates to the ISE-SAR descriptive examples.
 - a. Issue: Terrorism is not static. New behaviors and additional examples may appear as behavior patterns or tactics are changed and ISE-SARs are documented. The ISE-SAR FS needed new and more agile processes to allow for timely and responsive updates to Part B.
 - b. Anticipated Impact of the Proposed Change: The dual track process allows for a more deliberative and comprehensive review of the 16 behavioral categories and criteria, while allowing the descriptive examples to be updated as needed to respond to analyst/supervisor needs. The updates will be based on the new or evolving threat picture, using work and performance data to inform the process.
3. Clarify the behavioral criteria, as appropriate.
 - a. Issue: Analysts/investigators and supervisors have questioned their flexibility in interpreting the criteria describing each of the Part B behavioral categories.
 - b. Anticipated Impact of the Proposed Change: The clarifications will improve the vetting process by ensuring a more consistent interpretation of the pre-operational behavioral criteria.
4. Identify two descriptive examples, based on actual ISE-SARs, for each of the 16 pre-operational behaviors that may be determined to have a potential nexus to terrorism.
 - a. Issue: Analysts/investigators and supervisors have asked for descriptive examples.
 - b. Anticipated Impact of Proposed Change: The examples will provide context to analysts/investigators and supervisors and enhance their ability to assess the application of the 16 pre-operational behavior categories and criteria. They will also understand that the descriptive examples contained in the third column of Part B do not represent all possible examples that relate to ISE-SAR submissions. The examples are provided as a nonexhaustive list of illustrations of pre-operational behaviors that may support the documentation and submission of an ISE-SAR based on the contextual assessment of the reviewing analyst or investigator.

- B. A “change management chart” has been added to record future revisions to the descriptive examples in Part B. It will be used to reflect interim updates to the behavior examples without the need to issue a new version of the FS. It should be noted, however, that the formal ISA IPC process for reviewing and updating the behavioral categories and criteria will require the reissuance/update of the ISE-SAR Functional Standard under the PM’s authority.

SUMMARY OF MAJOR SUBSTANTIVE PROPOSALS WHICH WERE NOT INCORPORATED IN ISE-SAR FS 1.5.5

1. Proposed changes to core FS definitions, including “suspicious activity report (SAR)” and “information sharing environment suspicious activity report (ISE-SAR)” [*issue was deferred to FS v. 2.0 consideration*].
 - a. Issue: During the five rounds of adjudication of comments, the PM-ISE repeatedly rejected edits that would have broadened or fundamentally altered the definition of an ISE-SAR. The latest variation on this proposal recommended the following changes:

An ISE-SAR is a SAR...that has been determined, pursuant to a two-part process, to be reasonably indicative of criminal activity associated with terrorism or other criminal activity. ISE-SAR business, privacy, and civil liberties rules will serve as a unified process to support the reporting, tracking, processing, storage, and retrieval of Suspicious Activity Reporting across the ISE.
 - b. Decision and potential adverse impact: The PM-ISE determined that the ISE-SAR definition should remain intact. Early in this process, Federal partners agreed to defer major substantive updates to version 2.0. The proposed edits to the ISE-SAR definition were deferred on the grounds that the edits would have undermined the current vetting process by making Part 2 of the two-part process for identifying an ISE-SAR identical to the identification of a SAR and eliminating the requirement to determine that the behavior has “a potential nexus to terrorism.” The impact of this proposal would have been drastic because it would have meant that an ISE-SAR could include nonterrorism-related criminal activity. The FS 1.5.5 draft was intended to extend the “reasonably indicative” concept to this part of the process, but it was not intended to include “other criminal activity” in the NSI enclave of the SDR.
2. Proposal to identify the 16 pre-operational behaviors that may have a potential nexus to terrorism as “terrorism-related.”
 - a. Decision and Impact: This proposal was not incorporated because the term is overly broad. The term “terrorism-related” would have included within its ambit *any information* related to terrorism rather than limiting the behaviors to those that are “reasonably indicative of terrorism or other criminal activity.”
3. Proposal to limit the determination of a “potential nexus to terrorism” solely to consideration of the observed behavior reported in the SAR.
 - a. Decision and Impact: This proposal was not incorporated. The proposal to limit the analyst/investigator’s determination to the observed behavior in the SAR, rather than considering the entirety of the available context, facts, and circumstances would have prevented the analyst/investigator from taking into account other available and relevant information (e.g., specific or general threat bulletins, trip wire reports, or other information or intelligence).

RESPONSES TO KEY ADVOCATES' CONCERNS REGARDING THE NSI AND FUSION CENTERS

During the process of identifying appropriate updates to the ISE-SAR FS 1.5, NSI stakeholders evaluated the definition of an "ISE-SAR" and determined that "reasonably indicative" remains a core operational concept while leaving the ISE-SAR definition intact. Advocates have recommended that the NSI and ISE-SAR FS require "reasonable suspicion of specified criminal activity" in order to collect, retain, or disseminate SARs containing personally identifiable information, as required by federal regulation 28 CFR Part 23. Although this recommendation was discussed by the stakeholders, no stakeholders suggested changing the operational concept for a SAR from "reasonably indicative" to "reasonable suspicion."

It is critical to recognize that SAR and ISE-SAR information is not criminal intelligence information and represents information about suspicious behavior that has been observed and reported to or by law enforcement officers or other NSI participants. Because the information has a potential criminal nexus, there is a valid law enforcement purpose for retaining the information and engaging in follow-up information gathering (investigation) and evaluation. In contrast to SAR and ISE-SAR information, criminal intelligence information focuses on the investigative stage once a tip or lead has been received and on identifying the specific criminal subject(s), the criminal activity in which they are engaged, and the evaluation of facts to determine that the reasonable suspicion standard has been met. Criminal intelligence information is a product of investigation. Consequently, the ISE-SAR FS does not establish "reasonable suspicion," as defined by 28 CFR Part 23, as the standard for the sharing of this information in the NSI SAR Data Repository (SDR). Further, the FS need not do so because "reasonable suspicion" is not a required standard for information gathering or collection, processing, retention, or sharing.

The advocates have also questioned the FBI's interpretation of its legal authorities with respect to eGuardian data collections and data flows, raising concerns about the sharing of crime and terrorism information (including terrorism-related non-ISE-SAR information) with Federal agencies. The interim, updated FS v. 1.5.5 includes a section to clarify the sharing of other information or intelligence outside the ISE-SAR process. See "Summary of Key Changes: Part A" (D)(1)-(3)(above).

INFORMATION SHARING ENVIRONMENT (ISE)**FUNCTIONAL STANDARD (FS)****SUSPICIOUS ACTIVITY REPORTING (SAR)****VERSION 1.5.5**

1. Authority. Homeland Security Act of 2002, as amended; The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended; Presidential Memorandum dated April 10, 2007 (Assignment of Functions Relating to the Information Sharing Environment); Presidential Memorandum dated December 16, 2005 (Guidelines and Requirements in Support of the Information Sharing Environment); DNI memorandum dated May 2, 2007 (Program Manager's Responsibilities); Executive Order 13388; and other applicable provisions of law, regulation, or policy.
2. Purpose. This issuance updates the Functional Standard for ISE-SARs and is one of a series of Common Terrorism Information Sharing Standards (CTISS) issued by the Program Manager for the Information Sharing Environment (PM-ISE). While limited to describing the ISE-SAR process and associated information exchanges, information from this process may support other ISE processes, to include alerts, warnings, and notifications; situational awareness reporting; and terrorist watchlisting.
3. Applicability. This *ISE-SAR Functional Standard* applies to all departments or agencies that possess or use terrorism or homeland security information or intelligence, operate systems that support or interface with the ISE, or otherwise participate (or expect to participate) in the ISE, as specified in Section 1016(i) of the IRTPA, and in the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI).
4. References. ISE Implementation Plan, November 2006; ISE Enterprise Architecture Framework (EAF), Version 2.0, September 2008; Initial Privacy and Civil Liberties Analysis for the Information Sharing Environment, Version 1.0, September 2008; Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations, Nationwide Suspicious Activity Reporting Initiative (July 2010); ISE-AM-300: Common Terrorism Information Standards Program, October 31, 2007; Common Terrorism Information Sharing Standards Program Manual, Version 1.0, October 2007; National Information Exchange Model, Concept of Operations (CONOPS), Version 0.5, January 9, 2007; 28 Code of Federal Regulations (CFR) Part 23; Executive Order 13526 (Classified National Security Information), December 29, 2009; Nationwide Suspicious Activity Reporting Concept of Operations, December 2008; ISE Suspicious Activity Reporting Evaluation Environment (EE) Segment Architecture, December 2008; *ISE-SAR Functional Standard v. 1.5* (2009); and the National Strategy for Information Sharing and Safeguarding, December 2012; NSI SAR Data Repository (SDR) CONOPS, January 2014.

5. Definitions.

- a. **Artifact:** Detailed mission product documentation addressing information exchanges and data elements for ISE-SAR (data models, schemas, structures, etc.).
- b. **Common Terrorism Information Sharing Standards (CTISS):** Business process-driven, performance-based “common standards” for preparing terrorism-related (and other) information for maximum distribution and access, to enable the acquisition, access, retention, production, use, management, and sharing of terrorism-related information within the ISE. CTISS, such as this *ISE-SAR Functional Standard*, are implemented in ISE participants’ infrastructures as described in the *ISE EAF*. CTISS identifies two categories of common standards:
 1. **Functional standards**—set forth rules, conditions, guidelines, and characteristics of data and mission products supporting ISE business process areas.
 2. **Technical standards**—document specific technical methodologies and practices to design and implement information sharing capability into ISE systems.
- c. **Nationwide SAR Initiative (NSI) SAR Data Repository (SDR):** The NSI SDR consists of a single data repository, built to respect and support originator control and local stewardship of data, which incorporates Federal, State, and local retention policies. Within the SDR, hosted data enclaves extend this approach to information management and safeguarding practices by ensuring a separation of data across participating agencies.
- d. **eGuardian:** eGuardian is the FBI’s unclassified, Web-based system for receiving, tracking, and sharing ISE-SARs in the NSI as well as receiving and documenting other terrorism-related information, such as watchlist encounters or terrorism-related events, and other cyber or criminal threat information. (All information that is available to NSI participants through the eGuardian SDR will be vetted by a trained fusion center or Federal agency analyst or investigator to ensure that it meets the vetting standard for an ISE-SAR (i.e., a SAR that has been determined, pursuant to a two-part process, to have a potential nexus to terrorism). ISE-SARs loaded into eGuardian are pushed to the FBI’s Guardian system, a classified counterpart to eGuardian, in which the FBI and its JTTFs compare investigative lead information with other holdings available to the FBI in its capacity as a member of the Intelligence Community.
- e. **Field Intelligence Groups (FIGs):** The hub of the FBI’s intelligence program in the field, FIGs are the primary mechanism through which FBI field offices identify, evaluate, and prioritize threats within their territories. Using dissemination protocols, FIGs contribute to regional and local perspectives on threats and serve as the FBI’s link among fusion centers, the JTTFs, and the Intelligence Community.
- f. **Fusion center:** “A collaborative effort of two or more Federal, State, local, tribal, or territorial (SLTT) government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent,

investigate, apprehend, and respond to criminal or terrorist activity.” (Source: Section 511 of the 9/11 Commission Act). State and major urban area fusion centers serve as focal points within the State and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the Federal government and SLTT and private-sector partners.

- g. Information exchange: The transfer of information from one organization to another organization, in accordance with CTISS defined processes.
- h. Information Sharing Environment-Suspicious Activity Report (ISE-SAR): An ISE-SAR is a SAR (as defined below in 5.t) that has been determined, pursuant to a two-part process, to have a potential nexus to terrorism (i.e., to be reasonably indicative of criminal activity associated with terrorism). ISE-SAR business rules and privacy and civil liberties requirements will serve as a unified process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.
- i. Joint Terrorism Task Forces (JTTFs): The FBI’s JTTFs are interagency task forces designed to enhance communication, coordination, and cooperation in countering terrorist threats. They combine the resources, talents, skills, and knowledge of Federal, State, territorial, tribal, and local law enforcement and homeland security agencies, as well as the Intelligence Community, into a single team that investigates and/or responds to terrorist threats. The JTTFs execute the FBI’s lead Federal agency responsibility for investigating terrorist acts or terrorist threats against the United States.
- j. National Information Exchange Model (NIEM): A joint technical and functional standards program initiated by the Department of Homeland Security (DHS) and the Department of Justice (DOJ) that supports national-level interoperable information sharing.
- k. Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI): The NSI establishes standardized processes and policies that provide the capability for Federal, SLTT, campus, and railroad law enforcement and homeland security agencies to share timely, relevant ISE-SARs through a distributed information sharing system that protects privacy, civil rights, and civil liberties.
- l. Owning agency/organization: The organization that owns the target associated with the suspicious activity.
- m. Personally identifiable information: Information that may be used to identify an individual (i.e., data elements in the identified “privacy fields” of this *ISE-SAR Functional Standard*).
- n. Pre-operational planning: Pre-operational planning describes activities associated with a known or particular planned criminal operation or with terrorist operations generally.

- o. Privacy field: A data element that may be used to identify an individual and, therefore, is subject to privacy protection.
 - p. Reasonably indicative: This operational concept for documenting and sharing suspicious activity report takes into account the circumstances in which that observation is made, which creates in the mind of the reasonable observer, including a law enforcement officer, an articulable concern that the behavior may indicate pre-operational planning associated with terrorism or other criminal activity.¹ It also takes into account the training and experience of a reasonable law enforcement officer, in cases in which an officer is the observer or documenter of the observed behavior reported to a law enforcement agency.
 - q. Source agency/organization: The agency or entity that originates the SAR report (examples include a local police department, a private security firm handling security for a power plant, and a security force at a military installation). The source organization will not change throughout the life of the SAR.
 - r. Submitting agency/organization: The organization that actuates the push of the ISE-SAR to the NSI community. The submitting organization and the source organization may be the same.
 - s. Suspicious activity: Observed behavior reasonably indicative of pre-operational planning associated with terrorism or other criminal activity.
 - t. Suspicious Activity Report (SAR): Official documentation of observed behavior reasonably indicative of pre-operational planning associated with terrorism or other criminal activity.
6. Guidance. This Functional Standard is hereby established as the nationwide ISE Functional Standard for identifying ISE-SARs. It is based on documented information exchanges and business requirements and describes the structure, content, and products associated with processing, integrating, and retrieving ISE-SARs by ISE agencies participating in the NSI.
7. Responsibilities.
- a. The PM-ISE, in consultation with the Information Sharing and Access Interagency Policy Committee (ISA IPC), will:
 - (1) Maintain and administer this *ISE-SAR Functional Standard*, to include:
 - (a) Updating the business process and information flows for ISE-SAR.

¹ It should be noted that for purposes of the evaluation and documentation of an ISE-SAR (See 5. h., above), the term “other criminal activity” must refer to criminal activity associated with terrorism and must fall within the scope of the 16 terrorism pre-operational behaviors identified in Part B of this Functional Standard.

- (b) Updating data elements and product definitions for ISE-SAR.
 - (2) Publish and maintain configuration management of this *ISE-SAR Functional Standard*.
 - (3) Assist with the development of ISE-SAR implementation guidance, training, and governance structure, as appropriate, to address privacy, civil rights, and civil liberties-related policy, architecture, and legal issues.
 - (4) Work with ISE agencies participating in the NSI, through the ISA IPC governance process, to develop a new or modified *ISE-SAR Functional Standard*, as needed and recognize the separate process for DHS and the FBI to update the behavioral examples in Part B ISE-SAR Criteria Guidance to rapidly reflect emerging threats and trends.
 - (5) Coordinate, publish, and monitor implementation and use of this *ISE-SAR Functional Standard*, and coordinate with the White House Office of Science and Technology Policy and with the National Institute of Standards and Technology (in the Department of Commerce) for broader publication, as appropriate.
- b. Each ISA IPC member and other affected organizations shall:
- (1) Propose modifications to the PM-ISE for this Functional Standard, as appropriate.
 - (2) As appropriate, incorporate this *ISE-SAR Functional Standard*, and any subsequent implementation guidance, into budget activities associated with relevant current (operational) mission specific programs, systems, or initiatives (e.g., operations and maintenance [O&M] or enhancements).
 - (3) As appropriate, incorporate this *ISE-SAR Functional Standard*, and any subsequent implementation guidance, into budget activities associated with future or new development efforts for relevant mission-specific programs, systems, or initiatives (e.g., development, modernization, or enhancement [DME]).
 - (4) Ensure that incorporation of this ISE-SAR Functional Standard, as set forth in 7.b (2) or 7.b (3) above, is done in compliance with *ISE Privacy Guidelines* and any additional guidance provided by the ISA IPC Privacy and Civil Liberties Subcommittee (P/CL Subcommittee).
 - (5) Ensure that incorporation of this ISE-SAR Functional Standard, as set forth in 7.b (1) or 7.b (2) above, is done without impact on federal agencies' lawful collection, maintenance, dissemination, and use of information, as provided by federal law.

ISE-FS-200

8. Effective Date and Expiration. This *ISE-SAR Functional Standard* supersedes the Information Sharing Environment, Functional Standard, Suspicious Activity Reporting, v. 1.5 (2009), is effective immediately, and will remain in effect as the updated ISE-SAR Functional Standard until further updated, superseded, or cancelled.



Program Manager for the
Information Sharing Environment

Date: February 23, 2015

Document Change History	
Document Title	ISE-SAR Functional Standard
Document Owner	PM-ISE
Document Responsibility	PM-ISE
Document Version	1.5.5
Document Status	

Version Control Summary			
Date	Version	Changed by	Change Description
2/23/15	1.5.5		Update to version 1.5 promulgated

Future Releases		
Date	Version	Proposed

PART A—ISE-SAR FUNCTIONAL STANDARD ELEMENTS

SECTION I: DOCUMENT OVERVIEW**List of ISE-SAR Functional Standard Technical Artifacts**

The full ISE-SAR information exchange contains five types of supporting technical artifacts. This documentation provides details of implementation processes and other relevant reference materials. A synopsis of the *ISE-SAR Functional Standard* technical artifacts is contained in Table 1 below.

Table 1 – Functional Standard Technical Artifacts²

Artifact Type	Artifact	Artifact Description
Development and Implementation Tools	1. Component Mapping Template (CMT) (SAR-to-NIEM)	This spreadsheet captures the ISE-SAR information exchange class and data element (source) definitions and relates each data element to corresponding National Information Exchange Model (NIEM) Extensible Mark-Up Language (XML) elements and NIEM elements, as appropriate.
	2. NIEM Wantlist	The Wantlist is an XML file that lists the elements selected from the NIEM data model for inclusion in the Schema Subset. The Schema Subset is a compliant version to both programs that has been reduced to only those elements actually used in the ISE-SAR document schema.
	3. XML Schemas	The XML Schema provides a technical representation of the business data requirements. They are a machine-readable definition of the structure of an ISE-SAR-based XML Message.
	4. XML Sample Instance	The XML Sample Instance is a sample document that has been formatted to comply with the structures defined in the XML Schema. It provides the developer with an example of how the ISE-SAR schema is intended to be used.
	5. Codified Data Field Values	Listings, descriptions, and sources as prescribed by data fields in the <i>ISE-SAR Functional Standard</i> .

² Development and implementation tools may be accessible through www.ise.gov. In addition, updated versions of this Functional Standard should conform with NIEM.

SECTION II: SUSPICIOUS ACTIVITY REPORTING EXCHANGES

A. ISE-SAR Purpose

This *ISE-SAR Functional Standard* has been designed to incorporate key elements that describe pre-operational behaviors that are criminal in nature and have historically been associated with terrorism.³ The NSI includes law enforcement,⁴ homeland security,⁵ and other information sharing partners at the Federal, SLTT levels, including State and major urban area fusion centers, to the full extent permitted by law. In addition to providing specific indications about possible terrorism-related behaviors, ISE-SARs can be used to look for patterns and trends by analyzing information at a broader level than would typically be recognized within a single jurisdiction, including SLTT jurisdictions. Standardized and consistent sharing of ISE-SARs among State and major urban area fusion centers and Federal agencies participating in the NSI is vital to assessing, deterring, preventing, or prosecuting those involved in criminal activities with a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism). This *ISE-SAR Functional Standard* has been designed to incorporate key elements that describe pre-operational behaviors historically associated with terrorism.

B. ISE-SAR Scope

An ISE-SAR is a SAR that has been determined by a trained analyst or investigator, pursuant to a two-part process,⁶ to have a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism). (See Section II. D. 3. below, Analysis and Production). “Reasonably indicative” is a determination that takes into account (1) the circumstances in which the observation is made, which creates in the mind of the reasonable observer an articulable concern that the behavior may indicate pre-operational planning associated with terrorism or other criminal activity; and (2) the training and expertise of a reasonable law enforcement officer, in cases in which an officer is the observer or documenter of the SAR, who may be informed by specific or general threat bulletins, trip wire reports, or other information or intelligence. The term “pre-operational planning” refers to those activities that are associated with a known or particular planned criminal operation or with terrorist operations generally.

³ Identified in Part B of this Functional Standard, the 16 pre-operational behaviors are criminal in nature either because they are inherently criminal (e.g., breach, theft, sabotage) or because they are being engaged in to further a terrorism operation (e.g., testing or probing of security, observation/surveillance, materials acquisition). The pre-operational behavioral criteria and categories are listed in Part B of this Functional Standard.

⁴ All references to Federal and SLTT law enforcement agencies are intended to encompass civilian law enforcement, military police, and other security professionals.

⁵ All references to homeland security are intended to encompass public safety, emergency management, and other officials who routinely participate in the State or major urban area’s homeland security preparedness activities.

⁶ The determination of an ISE-SAR is a two-part process: (1) at the State or major urban area fusion center or Federal agency, an analyst or law enforcement officer reviews the newly reported information for suspicious behavior based on his or her training and expertise and against ISE-SAR behavior criteria; and (2) based on the context, facts, and circumstances, the analyst or investigator determines whether the information meeting the criteria has a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism).

A determination that a SAR constitutes an ISE-SAR is made as part of a two-part vetting process by a trained analyst or investigator who takes into account the reported circumstances of the SAR, including both the training and experience of the law enforcement or homeland security personnel reporting the behavior, to confirm that the reasonably indicative determination has been met.⁷ The analyst or investigator then compares the SAR with information from available databases and resources, reviews the behavior against the Part B (ISE-SAR Criteria Guidance) pre-operational terrorism behaviors, and then makes a judgment as to whether, given the context, facts, and circumstances available, there is a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism). Part B provides a more thorough explanation of ISE-SAR pre-operational behavior criteria and highlights the importance of the trained analyst or investigator taking into account the context, facts, and circumstances in reviewing suspicious behaviors to identify those SARs with a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism). The following are select examples of the 16 terrorism pre-operational behavioral categories, set forth in Part B, that may be reasonably indicative of terrorism:

- Expressed or implied threat
- Theft/loss/diversion
- Breach/attempted intrusion
- Cyberattacks
- Testing or probing of security⁸

It is important to stress that this *behavior-focused approach* to identifying suspicious activity requires that factors such as race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity must not be considered as factors creating suspicion (but attributes may be documented in specific suspect descriptions for identification purposes).⁹ The same constitutional standards that apply when conducting ordinary criminal investigations also apply to Federal and SLTT law enforcement and homeland security officers collecting information about suspicious activity. The ISE-SAR Functional Standard does not alter law enforcement officers' constitutional obligations when interacting with the public. This means, for example, that constitutional protections and agency policies and procedures that apply to a law

⁷ In assessing whether behavior constitutes "suspicious activity," law enforcement and homeland security personnel should consider all of the circumstances in which the behavior was observed, including knowledge such personnel may have had of any emerging threats or tradecraft, such as those based on specific or general threat bulletins, trip wire reports, or other information or intelligence.

⁸ For a full list and explanation of the behavioral categories, behavioral criteria, and descriptive examples, see Part B.

⁹ Consideration and documentation of race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity shall be consistent with applicable guidance, including, for federal law enforcement officers, [Guidance for Federal Law Enforcement Agencies regarding the Use of Race Ethnicity Gender National Origin Religion Sexual Orientation or Gender Identity](#) (December 2014).

enforcement officer's authority to stop, stop and frisk ("Terry Stop")¹⁰, request identification, or detain and question an individual apply in the same measure to observed behavior that is reasonably indicative of pre-operational planning associated with terrorism or other criminal activity. It is also important to recognize that many terrorism-related activities are now being funded via local or regional criminal organizations whose direct association with terrorism may be tenuous. This places law enforcement and homeland security professionals in the unique, yet demanding, position of identifying suspicious behaviors as a by-product or secondary element in a criminal enforcement or investigative activity. This means that, while some ISE-SARs may document observed behaviors to which local agencies have already responded, there is value in sharing them more broadly to facilitate aggregate trending or analysis of potential terrorist activities.

ISE-SARs are not intended to be used to track or record ongoing enforcement, intelligence, or investigatory operations, although they can provide information on these activities. The ISE-SAR process offers a standardized means for identifying and sharing ISE-SARs and applying data analytic tools to the information. Any patterns identified during ISE-SAR data analysis must be investigated in cooperation with the FBI's JTTFs. If the information originates with the JTTF, the JTTF should work in coordination with the State or major urban area fusion center unless departmental policies and procedures dictate otherwise (e.g., the information is classified).

C. Overview of Nationwide SAR Cycle

As defined in the *Nationwide Suspicious Activity Reporting Initiative (NSI) Concept of Operations (CONOPS)*,¹¹ the Nationwide SAR process consists of five standardized business process categories: (1) planning; (2) gathering and processing; (3) analysis and production; (4) dissemination; and (4) reevaluation. Under these five categories are nine steps that complete the Nationwide SAR cycle, as illustrated below in Figure 1. Figure 1 relates to the detailed ISE-SAR flowchart outlined in Part C of this version of the *ISE-SAR Functional Standard*. For further detail on the 12 NSI steps, please refer to the *NSI CONOPS*.

¹⁰ "Terry Stop" refers to the U.S. Supreme Court ruling in *Terry v. Ohio*, 392 U.S. 1 (1968), which held that a law enforcement officer may stop and frisk an individual for weapons that may endanger the officer when the officer has a reasonable and articulable suspicion, based on a totality of the circumstances, that the individual may be armed and dangerous.

¹¹ PM-ISE, *Nationwide SAR Initiative Concept of Operations* (2008), available from http://ise.gov/sites/default/files/NSI_CONOPS_Version_1_FINAL_2008-12-11_r1.0.pdf.

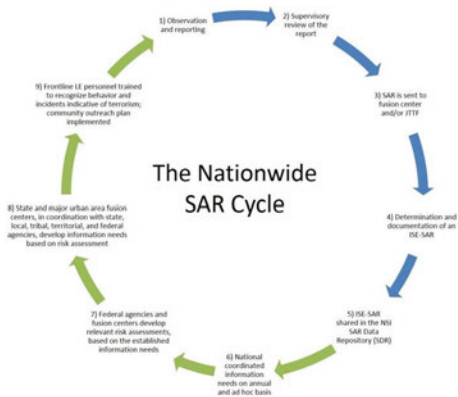


Figure 1 – ISE-SAR Flowchart

The technical framework of the SAR vetting and approval process that may produce an ISE-SAR is discussed in the *Nationwide Suspicious Activity Reporting (SAR) Initiative SAR Data Repository (SDR) Concept of Operations (NSI SDR CONOPS)*¹² The NSI SDR CONOPS explains the technical solution and associated user and training requirements supporting the NSI and details the enhanced platform that offers new efficiencies and deploys distributed capabilities to the NSI user community. The NSI SDR CONOPS provides an overview of the rules, regulations, policies, and training associated with accessing, submitting, and searching SAR data residing in the NSI SDR and the various tools that enable those submissions and searches.

D. ISE-SAR Top-Level Business Process

1. Planning

The activities in the planning phase of the NSI cycle, while integral to the overall NSI, are not discussed further in this Functional Standard. See the NSI CONOPS for more details.

¹² The NSI SDR CONOPS, (2014), available from https://leo.cjis.gov/leoContent/docs/gen/lesig/e_guard/fbi_reports/2014/201401_nsi_sar_data_repository_conops.pdf.

2. Gathering and Processing

SLTT law enforcement agencies, homeland security agencies, or field elements of Federal agencies participating in the NSI gather, document, and report information about suspicious activity in support of their responsibilities to investigate potential criminal activity, protect citizens, apprehend and prosecute criminals, and prevent crime. Information acquisition begins with an observation or report of unusual or suspicious behavior which, under the circumstances, is reasonably indicative of pre-operational planning associated with terrorism or other criminal activity. Behaviors that may be reasonably indicative of pre-operational planning associated with terrorism include, but are not limited to, theft, loss, or diversion, site breach or physical intrusion, cyberattacks, possible testing of physical response, or other unusual behavior or sector-specific incidents. It is important to emphasize that context, facts, and circumstances are essential elements for determining the relevance of suspicious behaviors to criminal activity with a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism). (See Part B for more details.)

Regardless of whether the initial observer is a private citizen, a representative of a private-sector partner, a government official, or a law enforcement or homeland security officer, suspicious activity may be reported to an SLTT law enforcement agency, a fusion center, or a local, regional, or national office of a Federal agency. When the initial investigation or fact gathering is completed, the investigating officer or official documents the event as a SAR, in accordance with the *ISE-SAR Functional Standard*, agency policy, local ordinances, and State and Federal laws and regulations.

The SAR is then reviewed within an SLTT or Federal agency by appropriately designated supervisors or other officials, who may have operational, privacy, and civil liberties responsibilities, for linkages to other suspicious or criminal activity in accordance with agency or departmental policy and procedures.¹³ Although there is always some level of local review, the degree varies from agency to agency. Smaller agencies may forward most SARs directly to their State or major urban area fusion centers or their local FBI JTTF, where further analysis can take place to determine whether the SAR reflects a Part B terrorism pre-operational behavior, has a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism), and is therefore an ISE-SAR. Major cities, on the other hand, may have trained counterterrorism experts on staff that perform analytic review of the initial reports and filter out those that can be determined not to have a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism).

After appropriate local processing, SLTT agencies make SARs available to their relevant State or major urban area fusion centers. Field components of Federal agencies participating in the NSI forward their SARs to the appropriate regional, district, or headquarters office, employing processes that vary from agency to agency. In those cases in which a local agency can determine that an activity has a direct connection to terrorism, it should immediately provide the

¹³ If appropriate, the agency should consult with a JTTF, FIG, or State or major urban area fusion center.

information directly to the responsible FBI JTTF¹⁴ for follow-on action against the identified terrorist activity. In those cases in which the local agency can determine that an activity has a direct connection to a terrorist event or pre-operational planning associated with terrorism, it will provide the information directly to the responsible JTTF for use as the basis for an assessment or investigation of a terrorism-related crime as appropriate.

3. Analysis and Production

The SLTT agency, fusion center, or Federal agency enters the SAR into an NSI SDR-connected platform. The SAR undergoes a two-part review process by a trained analyst or an investigator to establish or discount a potential nexus to terrorism (i.e., discount that it is reasonably indicative of pre-operational planning associated with terrorism). First, the trained analyst or law enforcement investigator reviews the newly reported SAR information against 16 pre-operational behaviors associated with terrorism that are identified in Part B of this ISE-SAR Functional Standard, keeping in mind—when interpreting the behaviors—the importance of context, facts, and circumstances.¹⁵ The analyst or investigator will then review the input against all available knowledge and information for linkages to other suspicious or criminal activity and determine whether the information reflects Part B behaviors.

Second, if the information reflects one or more Part B behaviors, the officer or analyst will apply his or her professional judgment to determine whether, based on the available context, facts, and circumstances, the information has a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism). If the officer or analyst cannot make this explicit determination, the report will not be accessible in the NSI SDR, although it may be retained in local fusion center or Federal agency files in accordance with established retention policies and business rules or reported to the FBI or other law enforcement or homeland security agencies under other legal authorities. However, if that determination is made by the analyst or investigator, the SAR will either be submitted immediately to the NSI SDR or forwarded for secondary review and approval, which may lead to submission to the NSI SDR.

As described in Part B, the activities listed as “Potential Criminal or Non-Criminal Activity” are not inherently criminal behaviors and are potentially constitutionally protected; thus, additional facts or circumstances must be articulated in the incident.

4. Dissemination

Once a SAR has been determined to meet Part B behavior criteria and have a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism), the SAR becomes an ISE-SAR and is formatted in accordance with the ISE-SAR Information Exchange Package Document (IEPD) format described in Sections III and IV. The ISE-SAR is

¹⁴ SARs that do not require an immediate law enforcement response should nonetheless be made available to JTTFs for a coordinated evaluation, including, but not limited to, comparing the information with other holdings available to the FBI as a member of the Intelligence Community.

¹⁵ It is important to note that the analyst or investigator should not make assumptions or presumptions as to why an individual acted or failed to act in a certain way; rather, the determination that the behavior is suspicious should be based on the behavior observed or on documented circumstances.

then uploaded by the submitting agency, where it is immediately provided to the FBI for an assessment-level investigation and made available to all other NSI participants. This allows authorized law enforcement agencies and fusion centers to be cognizant of all terrorism-related suspicious activity in their respective areas of responsibility, consistent with the information flow description in Part C, and allows the FBI to take investigative action as appropriate and in coordination with or with the knowledge of the source agency. Although the ISE-SAR has been shared with all NSI participants, it remains under the ownership and control of the submitting organization (i.e., SLTT law enforcement agency, fusion center, or Federal agency that made the initial determination that the activity constituted an ISE-SAR) and the ISE-SAR is then uploaded to the NSI SDR.

By this stage of the process, all initially reported SARs have been through multiple levels of review by trained personnel and, to the maximum extent possible, those SARs without a potential nexus to terrorism have been filtered out. SARs that are vetted, approved, and made available for sharing in the NSI SDR are ISE-SARs and can be presumed by Federal, State, and local analytic personnel to have a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism), and information derived from them can be used along with other sources to support JTTF or other counterterrorism operations or to develop counterterrorism analytic products. As in any analytic process, however, all information is subject to further review and validation. Analysts must coordinate with the submitting organization for deconfliction and are responsible for obtaining and using any available relevant information in the applicable analytic product. To appropriately safeguard privacy, civil rights, and civil liberties, analytical programs should be conducted in accordance with agency policies and procedures, including privacy policies, and records management schedules and should implement auditing and accountability measures.

Once ISE-SARs are accessible in the NSI SDR, they can be used to support a range of counterterrorism analytic and operational activities. This step involves the actions necessary to integrate ISE-SAR information into existing counterterrorism analytic and operational processes, including efforts to “connect the dots,” identify information gaps, and develop formal analytic products.

5. Reevaluation¹⁶

Operational feedback on the status of ISE-SARs is an essential element of an effective NSI process with important implications for privacy, civil rights, and civil liberties. First of all, it is important to notify source organizations when information they provide is designated as an ISE-SAR by a submitting organization and made available for sharing—a form of positive feedback that lets organizations know that their initial suspicions have some validity. Second, once the FBI assigns and assesses an ISE-SAR, the submitting organization is electronically notified of the FBI field office investigating the SAR and the results of the assessment. These results are maintained in the disposition section of the ISE-SAR for all NSI participants to review.

¹⁶ The reevaluation phase also encompasses the establishment of an integrated counterterrorism information needs process, a process that does not relate directly to information exchanges through this standard. See page 23 of the 2008 *NSI CONOPS* for more details.

E. Broader ISE-SAR Applicability

Consistent with the *ISE Privacy Guidelines* and Presidential Guideline 2, and to the full extent permitted by law, this *ISE-SAR Functional Standard* is designed to support the sharing of unclassified information or sensitive but unclassified (SBU)/controlled unclassified information (CUI) within the NSI SDR. There is also a provision for using a data element indicator for designating classified national security information as part of the ISE-SAR record, as necessary. This condition could be required under special circumstances for protecting the context of the event, or specifics or organizational associations of affected locations. The State or major urban area fusion center or the FBI's Guardian Management Unit (GMU) or JTTF acts as a key conduit between the SLTT agencies and other NSI participants. It is important to note that, although many SAR source agencies and ISE-SAR consumers have responsibilities beyond terrorist activities, the NSI ISE-SAR concept is focused exclusively on terrorism-related information. Of special note, there is no intention to modify or otherwise affect, through this *ISE-SAR Functional Standard*, the currently supported or mandated direct interactions between SLTT law enforcement and investigatory personnel and the FBI's JTTFs and/or FIGs.

This *ISE-SAR Functional Standard* will be used as the ISE-SAR information exchange standard for all NSI participants. Although the extensibility of this *ISE-SAR Functional Standard* does support customization for unique communities, jurisdictions planning to modify this *ISE-SAR Functional Standard* must carefully consider the consequences of customization. The PM-ISE requests that modification follow a formal change request process through the ISA IPC as appropriate, for both community coordination and consideration. Further, messages that do not conform to this Functional Standard may not be consumable by the receiving organization and may require modifications by the nonconforming organizations.

F. Other Information Sharing Authorities

The ISE-SAR process does not supersede other information or intelligence gathering, collection, or sharing authority, including the authority to share information between and among Federal agencies and SLTT agencies where the information is related to homeland security, terrorism, or other Federal crimes.

Multiple Federal agencies currently have the authority to collect terrorism-related tips and leads. However, only those tips and leads that comply with the ISE-SAR Functional Standard are broadly shared with NSI participants. At the SLTT level, crime and terrorism information, including terrorism-related non-ISE-SAR information, can and should be reported to appropriate Federal agencies based on their relevant legal authorities.¹⁷

¹⁷ As an example, SLTT agencies may provide terrorism-related source data that leads to the creation of an Intelligence Information Report (IIR), which is ultimately shared with the federal Intelligence Community. In addition, SLTT agencies often enhance existing federal data by providing local context for an assortment of Intelligence Community partners (e.g., Drug Enforcement Administration and DHS components). A third example relates to terrorism-related leads that do not meet the requirements of the *ISE-SAR Functional Standard* but may require investigative follow-up by the FBI. Under the latter circumstance, non-ISE-SAR information may be submitted electronically to the FBI.

It is important to recognize that the multidirectional sharing of non-ISE-SAR information takes place outside the NSI SDR. Consequently, while systems involved in the NSI can be used in the exercise of other agency authorities related to information and intelligence collection, sharing, and analysis, information sharing outside the scope of the *ISE-SAR Functional Standard* must be done in accordance with other agency legal authorities, policies and procedures, and interagency agreements. This means that reports determined not to be ISE-SARs will be handled in accordance with applicable SLTT and other agencies' authorities, policies, and procedures.

G. Protecting Privacy, Civil Rights, and Civil Liberties

Laws that prohibit or otherwise limit the sharing of PII vary considerably between the Federal SLTT levels. The Privacy Act of 1974 (5 USC §552a), as amended, other statutes such as the E-Government Act of 2002, and many governmentwide or departmental regulations establish a framework and criteria for protecting information privacy in the Federal government. The ISE, including NSI participants, must facilitate the sharing of information in a lawful manner, which, by its nature, must recognize, in addition to Federal statutes and regulations, different SLTT, laws, regulations, or policies that affect privacy. One method for protecting privacy, civil rights, and civil liberties while enabling the broadest possible sharing is to anonymize ISE-SAR reports by excluding data elements that contain PII. Accordingly, NSI participating agencies enter ISE-SARs according to their privacy laws and policies and rules governing the sharing of PII, where appropriate.

SECTION III: INFORMATION EXCHANGE DEVELOPMENT DATA MODEL

This ISE-SAR Functional Standard includes a collection of artifacts that support ISE-SAR information exchanges. The basic ISE-SAR information exchange is documented using five unique artifacts, giving implementers tangible products that can be leveraged for local implementation. A domain model provides a graphical depiction of those data elements required for implementing an exchange and the cardinality between those data elements. Second, a Component Mapping Template is a spreadsheet that associates each required data element with its corresponding XML data element. Third, information exchanges include the schemas that consist of a document, extension, and constraint schema. Fourth, at least one sample XML Instance and associated style-sheet is included to help practitioners validate the model, mapping, and schemas in a more intuitive way. Fifth, a codified data field values listing provides listings, descriptions, and sources as prescribed by the data fields.

SECTION IV: ISE-SAR EXCHANGE DATA MODEL

A. Summary of Elements

This section contains a full inventory of all ISE-SAR information exchange data classes, elements, and definitions. Items and definitions contained in cells with a light purple background are data classes, while items and definition contained in cells with a white background are data elements. A wider representation of data class and element mappings to source (ISE-SAR information exchange) and target is contained in the Component Mapping Template located in the technical artifacts folder.

Cardinality between objects in the model is indicated on the line in the domain model (see Section 5A). Cardinality indicates how many times an entity can occur in the model. For example, Vehicle, Vessel, and Aircraft all have cardinality of 0..n. This means that they are optional but may occur multiple times if multiple suspect vehicles are identified.

Clarification of organizations used in the exchange:

The **source agency/organization** is the agency or entity that originates the SAR report (examples include a local police department, a private security firm handling security for a power plant, and a security force at a military installation). The source organization will not change throughout the life of the SAR.

The **submitting agency/organization** is the organization that actuates the push of the ISE-SAR to the NSI community. The submitting agency/organization and the source agency/organization may be the same.

The **owning agency/organization** is the organization that owns the target¹⁸ associated with the suspicious activity (see page 21).

¹⁸ The target is a technical term for field of interest that is not readily viewed by someone who queries a particular SAR.

Table 2 – ISE-SAR Information Exchange Data Classes, Elements, and Definitions

Privacy Field	Source Class/Element	Source Definition
	Aircraft	
	Aircraft Engine Quantity	The number of engines on an observed aircraft.
	Aircraft Fuselage Color	A code identifying a color of a fuselage of an aircraft.
	Aircraft Wing Color	A code identifying a color of a wing of an aircraft.
X	Aircraft ID	A unique identifier assigned to the aircraft by the observing organization—used for referencing. *If this identifier can be used to identify a specific aircraft, for instance, by using the aircraft tail number, then this element is a privacy field. [free text field]
	Aircraft Make Code	A code identifying a manufacturer of an aircraft.
	Aircraft Model Code	A code identifying a specific design or type of aircraft made by a manufacturer.
	Aircraft Style Code	A code identifying a style of an aircraft.
X	Aircraft Tail Number	An aircraft identification number prominently displayed at various locations on an aircraft, such as on the tail and along the fuselage. [free text field]
	Attachment	
	Attachment Type Text	Describes the type of attachment (e.g., surveillance video, mug shot, evidence). [free text field]
	Binary Image	Binary encoding of the attachment.
	Capture Date	The date that the attachment was created.
	Description Text	Text description of the attachment. [free text field]
	Format Type Text	Format of attachment (e.g., mpeg, jpg, avi). [free text field]
	Attachment URI	Uniform Resource Identifier (URI) for the attachment. Used to match the attachment link to the attachment itself. Standard representation type that can be used for Uniform Resource Locators (URLs) and Uniform Resource Names (URNs).
	Attachment Privacy Field Indicator	Identifies whether the binary attachment contains information that may be used to identify an individual.

Privacy Field	Source Class/Element	Source Definition
	Contact Information	
X	Person First Name	Person to contact at the organization.
X	Person Last Name	Person to contact at the organization.
X	E-Mail Address	An e-mail address of a person or organization. [free text field]
X	Full Telephone Number	A full-length telephone identifier representing the digits to be dialed to reach a specific telephone instrument. [free text field]
	Driver License	
X	Expiration Date	The month, date, and year that the document expires.
	Expiration Year	The year the document expires.
	Issuing Authority Text	Code identifying the organization that issued the driver license assigned to the person. Examples include Department of Motor Vehicles, Department of Public Safety, and Department of Highway Safety and Motor Vehicles. [free text field]
X	Driver License Number	A driver license identifier or driver license permit identifier of the observer or observed person of interest involved with the suspicious activity. [free text field]
	Follow-Up Action	
	Activity Date	Date that the follow-up activity started.
	Activity Time	Time that the follow-up activity started.
	Assigned By Text	Organizational identifier that describes the organization performing a follow-up activity. This is designed to keep all parties interested in a particular ISE-SAR informed of concurrent investigations. [free text field]
	Assigned To Text	Text describing the person or suborganization that will be performing the designated action. [free text field]
	Disposition Text	Description of disposition of suspicious activity investigation. [free text field]
	Status Text	Description of the state of follow-up activity. [free text field]

Privacy Field	Source Class/Element	Source Definition
	Location	
X	Location Description	A description of a location where the suspicious activity occurred. If the location is an address that is not broken into its component parts (e.g., 1234 Main Street), this field may be used to store the compound address. [free text field]
	Location Address	
	Building Description	A complete reference that identifies a building. [free text field]
	County Name	A name of a county, parish, or vicinage. [free text field]
	Country Name	A country name or other identifier. [free text field]
	Cross Street Description	A description of an intersecting street. [free text field]
	Floor Identifier	A reference that identifies an actual level within a building. [free text field]
	ICAO Airfield Code for Departure	An International Civil Aviation Organization (ICAO) airfield code for departure. Indicates aircraft, crew, passengers, and cargo on conveyance location information. [free text field]
	ICAO Airfield Code for Planned Destination	An airfield code for planned destination. Indicates aircraft, crew, passengers, and cargo on conveyance location information. [free text field]
	ICAO for Actual Destination	An airfield code for actual destination. Indicates aircraft, crew, passengers, and cargo on conveyance location information. [free text field]
	ICAO Airfield for Alternate	An airfield code for Alternate. Indicates aircraft, crew, passengers, and cargo on conveyance location information. [free text field]
	Mile Marker Text	Identifies the sequentially numbered marker on a roadside that is closest to the intended location. Also known as milepost, or mile post. [free text field]
	Municipality Name	The name of the city or town. [free text field]
	Postal Code	The ZIP code or postal code. [free text field]
	State Name	Code identifying the state.
	Street Name	A name that identifies a particular street. [free text field]

Privacy Field	Source Class/Element	Source Definition
X	Street Number	A number that identifies a particular unit or location within a street. [free text field]
	Street Post Directional	A direction that appears after a street name. [free text field]
	Street Pre Directional	A direction that appears before a street name. [free text field]
	Street Type	A type of street, e.g., street, boulevard, avenue, highway. [free text field]
X	Unit ID	A particular unit within the location. [free text field]
	Location Coordinates	
	Altitude	Height above or below sea level of a location.
	Coordinate Datum	Coordinate system used for plotting location.
	Latitude Degree	A value that specifies the degree of a latitude. The value comes from a restricted range between -90 (inclusive) and +90 (inclusive).
	Latitude Minute	A value that specifies a minute of a degree. The value comes from a restricted range of 0 (inclusive) to 60 (exclusive).
	Latitude Second	A value that specifies a second of a minute. The value comes from a restricted range of 0 (inclusive) to 60 (exclusive).
	Longitude Degree	A value that specifies the degree of a longitude. The value comes from a restricted range between -180 (inclusive) and +180 (exclusive).
	Longitude Minute	A value that specifies a minute of a degree. The value comes from a restricted range of 0 (inclusive) to 60 (exclusive).
	Longitude Second	A value that specifies a second of a minute. The value comes from a restricted range of 0 (inclusive) to 60 (exclusive).
	Conveyance Track/Intent	A direction by heading and speed or route and/or waypoint of conveyance. [free text field]
	Observer	
	Observer Type Text	Indicates the relative expertise of an observer to the suspicious activity (e.g., professional observer versus layman). Example: a security guard at a utility plant recording the activity, or a citizen driving by viewing suspicious activity. [free text field]

Privacy Field	Source Class/Element	Source Definition
X	Person Employer ID	Number assigned by an employer for a person such as badge number. [free text field]
	Owning Agency/ Organization	
	Organization Item	A name of an organization that owns the target. [free text field]
	Organization Description	A text description of organization that owns the target. The description may indicate the type of organization such as state bureau of investigation, highway patrol, etc. [free text field]
X	Organization ID	A federal tax identifier assigned to an organization. Sometimes referred to as a Federal Employer Identification Number (FEIN), or an Employer Identification Number (EIN). [free text field]
X	Organization Local ID	An identifier assigned on a local level to an organization. [free text field]
	Other Identifier	
X	Person Identification Number (PID)	An identifying number assigned to the person, e.g., military serial numbers. [free text field]
X	PID Effective Date	The month, date, and year that the PID number became active or accurate.
	PID Effective Year	The year that the PID number became active or accurate.
X	PID Expiration Date	The month, date, and year that the PID number expires.
	PID Expiration Year	The year that the PID number expires.
	PID Issuing Authority Text	The issuing authority of the identifier. This may be a State, military organization, etc.
	PID Type Code	Code identifying the type of identifier assigned to the person. [free text field]
	Passport	
X	Passport ID	Document Unique Identifier. [free text field]
X	Expiration Date	The month, date, and year that the document expires.
	Expiration Year	The year the document expires.
	Issuing Country Code	Code identifying the issuing country. [free text field]

Privacy Field	Source Class/Element	Source Definition
	Person	
X	AFIS FBI Number	A number issued by the FBI's Automated Fingerprint Identification System (AFIS) based on submitted fingerprints. [free text field]
	Age	A precise measurement of the age of a person.
	Age Unit Code	Code that identifies the unit of measure of an age of a person (e.g., years, months). [free text field]
X	Date of Birth	The month, date, and year that a person was born.
	Year of Birth	The year a person was born.
	Ethnicity Code	Code that identifies the person's cultural lineage.
	Maximum Age	The maximum age measurement in an estimated range.
	Minimum Age	The minimum age measurement in an estimated range.
X	State Identifier	Number assigned by the State based on biometric identifiers or other matching algorithms. [free text field]
X	Tax Identifier Number	A nine-digit numeric identifier assigned to a living person by the U.S. Social Security Administration. A social security number of the person. [free text field]
	Person Name	
X	First Name	A first name or given name of the person. [free text field]
X	Last Name	A last name or family name of the person. [free text field]
X	Middle Name	A middle name of a person. [free text field]
X	Full Name	Used to designate the compound name of a person that includes all name parts. This field should be used only when the name cannot be broken down into its component parts or if the information is not available in its component parts. [free text field]
X	Moniker	Alternative or gang name for a person. [free text field]
	Name Suffix	A component that is appended after the family name that distinguishes members of a family with the same given, middle, and last name, or otherwise qualifies the name. [free text field]

Privacy Field	Source Class/Element	Source Definition
	Name Type	Text identifying the type of name for the person. For example, maiden name, professional name, nickname.
	Physical Descriptors	
	Build Description	Text describing the physique or shape of a person. [free text field]
	Eye Color Code	Code identifying the color of the person's eyes.
	Eye Color Text	Text describing the color of a person's eyes. [free text field]
	Hair Color Code	Code identifying the color of the person's hair.
	Hair Color Text	Text describing the color of a person's hair. [free text field]
	Person Eyewear Text	A description of glasses or other eyewear a person wears. [free text field]
	Person Facial Hair Text	A kind of facial hair of a person. [free text field]
	Person Height	A measurement of the height of a person.
	Person Height Unit Code	Code that identifies the unit of measure of a height of a person. [free text field]
	Person Maximum Height	The maximum measure value on an estimated range of the height of the person.
	Person Minimum Height	The minimum measure value on an estimated range of the height of the person.
	Person Maximum Weight	The maximum measure value on an estimated range of the weight of the person.
	Person Minimum Weight	The minimum measure value on an estimated range of the weight of the person.
	Person Sex Code	A code identifying the gender or sex of a person (e.g., Male or Female).
	Person Weight	A measurement of the weight of a person.
	Person Weight Unit Code	Code that identifies the unit of measure of a weight of a person. [free text field]
	Race Code	Code that identifies the race of the person.
	Skin Tone Code	Code identifying the color or tone of a person's skin.
	Clothing Description Text	A description of an article of clothing. [free text field]

Privacy Field	Source Class/Element	Source Definition
	Physical Feature	
	Feature Description	A text description of a physical feature of the person. [free text field]
	Feature Type Code	A special kind of physical feature or any distinguishing feature. Examples include scars, marks, tattoos, or a missing ear. [free text field]
	Location Description	A description of a location. If the location is an address that is not broken into its component parts (e.g., 1234 Main Street), this field may be used to store the compound address. [free text field]
	Registration	
	Registration Authority Code	Text describing the organization or entity authorizing the issuance of a registration for the vehicle involved with the suspicious activity. [free text field]
X	Registration Number	The number on a metal plate fixed to/assigned to a vehicle. The purpose of the registration number is to uniquely identify each vehicle within a state. [free text field]
	Registration Type	Code that identifies the type of registration plate or license plate of a vehicle. [free text field]
	Registration Year	A four-digit year as shown on the registration decal issued for the vehicle.
	ISE-SAR Submission	
	Additional Details Indicator	Identifies whether more ISE-SAR details are available at the authoring/submitting agency/organization than what has been provided in the information exchange.
	Data Entry Date	Date the data was entered into the reporting system (e.g., the Records Management System).
	Dissemination Code	Generally established locally, this code describes the authorized recipients of the data. Examples include Law Enforcement Use, Do Not Disseminate, etc.
X	Fusion Center Contact First Name	Identifies the first name of the person to contact at the fusion center. [free text field]
X	Fusion Center Contact Last Name	Identifies the last name of the person to contact at the fusion center. [free text field]
X	Fusion Center Contact E-Mail Address	Identifies the e-mail address of the person to contact at the fusion center. [free text field]

Privacy Field	Source Class/Element	Source Definition
X	Fusion Center Contact Telephone Number	The full phone number of the person at the fusion center who is familiar with the record (e.g., law enforcement officer).
	Message Type Indicator	e.g., Add, Update, Purge.
	Privacy Purge Date	The date by which the privacy information will be purged from the record system; general observation data is retained.
	Privacy Purge Review Date	Date of review to determine the disposition of the privacy fields in a detailed ISE-SAR IEPD record.
	Submitting ISE-SAR Record ID	Identifies the fusion center ISE-SAR record identifier for reports that are possibly related to the current report. [free text field]
	ISE-SAR Submission Date	Date of submission for the ISE-SAR record.
	ISE-SAR Title	Plain language title (e.g., bomb threat at the "X" Hotel). [free text field]
	ISE-SAR Version	Indicates the specific version of the ISE-SAR to which the XML Instance corresponds. [free text field]
	Source Agency Case ID	The case identifier for the agency that originated the SAR. Often, this will be a local law enforcement agency. [free text field]
	Source Agency Record Reference Name	The case identifier that is commonly used by the source agency—may be the same as the system ID. [free text field]
	Source Agency Record Status Code	The current status of the record within the source agency system.
	Privacy Information Exists Indicator	Indicates whether privacy information is available from the source fusion center. This indicator may be used to guide people who only have access to the summary information exchange as to whether they can follow up with the submitting fusion center to obtain more information.
	Sensitive Information Details	
	Classification Label	A classification of information. Includes Confidential, Secret, Top Secret, no markings. [free text field]

Privacy Field	Source Class/Element	Source Definition
	Classification Reason Text	A reason why the classification was made as such. [free text field]
	Sensitivity Level	Local information security categorization level (Controlled Unclassified Information-CUI, including Sensitive But Unclassified or Law Enforcement Sensitive). [free text field]
	Tearlined Indicator	Identifies whether a report is free of classified information.
	Source Agency/ Organization	
	Organization Name	The name used to refer to the agency originating the SAR. [free text field]
	Organization ORI	Originating Agency Identification (ORI) used to refer to the agency.
	System ID	The system that the case identifier (e.g., Records Management System, Computer Aided Dispatch) relates to within or the organization that originated the Suspicious Activity Report. [free text field]
	Fusion Center Submission Date	Date of submission to the fusion center.
X	Source Agency Contact First Name	The first name of the person at the agency that is familiar with the record (e.g., law enforcement officer). [free text field]
X	Source Agency Contact Last Name	The last name of the person at the agency that is familiar with the record (e.g., law enforcement officer). [free text field]
X	Source Agency Contact E-mail Address	The e-mail address of the person at the agency who is familiar with the record (e.g., law enforcement officer). [free text field]
X	Source Agency Contact Phone Number	The full phone number of the person at the agency that is familiar with the record (e.g., law enforcement officer).
	Suspicious Activity Report	
	Community Description	Describes the intended audience of the document. [free text field]
	Community URL	The URL to resolve the ISE-SAR information exchange payload namespace.

Privacy Field	Source Class/Element	Source Definition
	LEXS Version	Identifies the version of Department of Justice LEISP Exchange Specification (LEXS) used to publish this document. ISE-FS-200 has been built using LEXS version 3.1. The schema was developed by starting with the basic LEXS schema and extending that definition by adding those elements not included in LEXS. [free text field]
	Message Date/Time	A timestamp identifying when this message was received.
	Sequence Number	A number that uniquely identifies this message.
	Source Reliability Code	Reliability of the source, in the assessment of the reporting organization: could be one of "reliable," "unreliable," or "unknown."
	Content Validity Code	Validity of the content, in the assessment of the reporting organization: could be one of "confirmed," "doubtful," or "cannot be judged."
	Nature of Source-Code	Nature of the source: could be one of "anonymous tip," "confidential source," "trained interviewer," "written statement—victim, witness, other," "private sector," or "other source."
	Nature of Source-Text	Optional information of "other source" is selected above. [free text field]
	Submitting Agency/ Organization	
	Organization Name	Common Name of the fusion center or NSI participant that submitted the ISE-SAR record to the ISE. [free text field]
	Organization ID	Fusion center or NSI participant's alpha-numeric identifier. [free text field]
	Organization ORI	ORI for the submitting fusion center or NSI participant. [free text field]
	System ID	Identifies the system within the fusion center or NSI participant that is submitting the ISE-SAR. [free text field]
	Suspicious Activity	
	Activity End Date	The end or completion date in Greenwich Mean Time (GMT) of an incident that occurs over a duration of time.

Privacy Field	Source Class/Element	Source Definition
	Activity End Time	The end or completion time in GMT of day of an incident that occurs over a duration of time.
	Activity Start Date	The date in GMT when the incident occurred or the start date if the incident occurs over a period of time.
	Activity Start Time	The time of day in GMT that the incident occurred or started.
	Observation Description Text	Description of the activity including rationale for potential terrorism nexus. [free text field]
	Observation End Date	The end or completion date in GMT of the observation of an activity that occurs over a duration of time.
	Observation End Time	The end or completion time of day in GMT of the observation of an activity that occurred over a period of time.
	Observation Start Date	The date in GMT when the observation of an activity occurred or the start date if the observation of the activity occurred over a period of time.
	Observation Start Time	The time of day in GMT that the observation of an activity occurred or started.
	Threat Type Code	Broad category of threat to which the tip or lead pertains. Includes Financial Incident, Suspicious Activity, and Cyber Crime.
	Threat Type Detail Text	Breakdown of the Tip Type. It indicates the type of threat to which the tip or lead pertains. The subtype is often dependent on the Tip Type. For example, the subtypes for a nuclear/radiological tip class might be Nuclear Explosive or a Radiological Dispersal Device. [free text field]
	Suspicious Activity Code	Indicates the type of threat to which the tip or lead pertains. Examples include a biological or chemical threat.
	Weather Condition Details	The weather at the time of the suspicious activity. The weather may be described using codified lists or text.

Privacy Field	Source Class/Element	Source Definition
	Target	
	Critical Infrastructure Indicator	Critical infrastructure, as defined by 42 USC Sec. 5195c, means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
	Infrastructure Sector Code	The broad categorization of the infrastructure type. These include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government.
	Infrastructure Tier Text	Provides additional detail that enhances the Target Sector Code. For example, if the target sector is Utilities, this field would indicate the type of utility that has been targeted, such as power station or power transmission. [free text field]
	Structure Type Code	National Data Exchange (N-DEx) Code that identifies the type of structure that was involved in the incident.
	Target Type Text	Describes the target type if an appropriate sector code is not available. [free text field]
	Structure Type Text	Text for use when the Structure Type Code does not afford necessary code. [free text field]
	Target Description Text	Text describing the target (e.g., Lincoln Bridge). [free text field]
	Vehicle	
	Color Code	Code that identifies the primary color of a vehicle involved in the suspicious activity.
	Description	Text description of the entity. [free text field]
	Make Name	Code that identifies the manufacturer of the vehicle.
	Model Name	Code that identifies the specific design or type of vehicle made by a manufacturer—sometimes referred to as the series model.
	Style Code	Code that identifies the style of a vehicle. [free text field]

Privacy Field	Source Class/Element	Source Definition
	Vehicle Year	A four-digit year that is assigned to a vehicle by the manufacturer.
X	Vehicle Identification Number	Used to uniquely identify motor vehicles. [free text field]
X	US DOT Number	An assigned number sequence required by Federal Motor Carrier Safety Administration (FMCSA) for all interstate carriers. The identification number (found on the power unit, and assigned by the U.S. Department of Transportation or by a State) is a key element in the FMCSA databases for both carrier safety and regulatory purposes. [free text field]
	Vehicle Description	A text description of a vehicle. Can capture unique identifying information about a vehicle such as damage, custom paint, etc. [free text field]
	Related ISE-SAR	
	Fusion Center ID	Identifies the fusion center that is the source of the ISE-SAR. [free text field]
	Fusion Center ISE-SAR Record ID	Identifies the fusion center ISE-SAR record identifier for reports that are possibly related to the current report.
	Relationship Description Text	Describes how this ISE-SAR is related to another ISE-SAR. [free text field]
	Vessel	
X	VVessel—Official State Registration or Coast Guard Documentation Numbers	An identification issued by either the State or the U.S. Coast Guard. Either number is contained within valid marine documents. State registration numbers should be marked on the forward portion of the hull of the vessel, and documented vessels have a number permanently marked on the vessel's main beam.
X	Vessel ID	A unique identifier assigned to the boat record by the agency—used for referencing. [free text field]
	Vessel ID Issuing Authority	Identifies the organization authorization over the issuance of a vessel identifier. Examples include the State parks department and the U.S. Fish and Wildlife Department. [free text field]
X	Vessel IMO Number Identification	An identification for an International Maritime Organization Number (IMO number) of a vessel. [free text field]
X	Vessel MMSI Identification	An identification for the Maritime Mobile Service Identity (MMSI) or a vessel. [free text field]

Privacy Field	Source Class/Element	Source Definition
	Vessel Make	Code that identifies the manufacturer of the boat.
	Vessel Model	Model name that identifies the specific design or type of boat made by a manufacturer—sometimes referred to as the series model.
	Vessel Model Year	A four-digit year that is assigned to a boat by the manufacturer.
	Vessel Name	Complete boat name and any numerics. [free text field]
	Vessel Hailing Port	The identifying attributes of the hailing port of a vessel. [free text field]
	Vessel National Flag	A data concept for a country under which a vessel sails. [free text field]
	Vessel Overall Length	The length measurement of the boat, bow to stern.
	Vessel Overall Length Measure	Code that identifies the measurement unit used to determine the boat length. [free text field]
X	Vessel Serial Number	The identification number of a boat involved in an incident. [free text field]
	Vessel Type Code	Code that identifies the type of boat.
	Vessel Propulsion Text	Text for use when the Boat Propulsion Code does not afford necessary code. [free text field]

Association Descriptions

This section defines specific data associations contained in the ISE-SAR data model structure. Reference Figure 2 (UML-based model) for the graphical depiction and detailed elements.

Table 3 – ISE-SAR Data Model Structure Associations

Link Between Associated Components	Target Element
Link From Suspicious Activity Report to Attachment	lexs:Digest/lexsdigest:Associations/lexsdigest:EntityAttachmentLinkAssociation
Link From Suspicious Activity Report to Sensitive Information Details	Hierarchical Association
Link From Suspicious Activity Report to ISE-SAR Submission	Hierarchical Association

Link Between Associated Components	Target Element
Link From Suspicious Activity to Vehicle	lexs:Digest/lexsdigest:Associations/lexsdigest:IncidentInvolvedItemAssociation
Link From Vehicle to Registration	Hierarchical Association
Link From Suspicious Activity to Vessel	lexs:Digest/lexsdigest:Associations/lexsdigest:IncidentInvolvedItemAssociation
Link From Suspicious Activity to Aircraft	lexs:Digest/lexsdigest:Associations/lexsdigest:IncidentInvolvedItemAssociation
Link From Suspicious Activity to Location	lexs:Digest/lexsdigest:Associations/lexsdigest:ActivityLocationAssociation
Link From Suspicious Activity to Target	Hierarchical Association
Link From Location to Location Coordinates	Hierarchical Association
Link From Location to Location Address	Hierarchical Association
Link From Suspicious Activity Report to Related ISE-SAR	Hierarchical Association
Link From Person to Location	lexs:Digest/lexsdigest:Associations/lexsdigest:PersonLocationAssociation
Link From Person to Contact Information	lexs:Digest/lexsdigest:Associations/lexsdigest:EntityEmailAssociation or lexs:Digest/lexsdigest:Associations/lexsdigest:EntityTelephoneNumberAssociation
Link From Person to Driver License	Hierarchical Association
Link From Person to Passport	Hierarchical Association
Link From Person to Other Identifier	Hierarchical Association
Link From Person to Physical Descriptors	Hierarchical Association
Link From Person to Physical Feature	Hierarchical Association
Link From Person to Person Name	Hierarchical Association
Link From Suspicious Activity Report to Follow-Up Action	Hierarchical Association

Link Between Associated Components	Target Element
Link From Target to Location	lexs:Digest/lexsdigest:Associations/lexsdigest:ItemLocation Association
Link From Suspicious Activity Report to Organization	Hierarchical Association
Link From Suspicious Activity to Person [Witness]	lexs:Digest/lexsdigest:Associations/lexsdigest:IncidentWitnessAssociation
Link From Suspicious Activity to Person [Person Of Interest]	lexs:Digest/lexsdigest:Associations/lexsdigest:PersonOfInterestAssociation
Link From Organization to Target	ext:SuspiciousActivityReport/nc:OrganizationItemAssociation
Link from ISE-SAR Submission to Submitting Organization	Hierarchical Association
Link From Submitting Organization to Contact Information	Hierarchical Association (Note that the mapping indicates context and we are not reusing Contact Information components)

Extended XML Elements

Additional data elements are also identified as new elements outside of NIEM, Version 2.0. These elements are listed below:

AdditionalDetailsIndicator: Identifies whether more ISE-SAR details are available at the authoring/submitting agency/organization than what has been provided in the information exchange.

AssignedByText: Organizational identifier that describes the organization performing a follow-up activity. This is designed to keep all parties interested in a particular ISE-SAR informed of concurrent investigations.

AssignedToText: Text describing the person or suborganization that will be performing the designated follow-up action.

ClassificationReasonText: A reason why the classification was made as such.

ContentValidityCode: Validity of the content, in the assessment of the reporting organization: could be one of “confirmed,” “doubtful,” or “cannot be judged.”

ConveyanceTrack/Intent: A direction by heading and speed or route and/or waypoint of conveyance.

CriticalInfrastructureIndicator: Critical infrastructure, as defined by 42 USC Sec. 5195c, means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

ICAOAirfieldCodeforDeparture: An International Civil Aviation Organization (ICAO) airfield code for departure. Indicates aircraft, crew, passengers, and cargo on conveyance location information.

ICAOAirfieldCodeforPlannedDestination: An airfield code for planned destination. Indicates aircraft, crew, passengers, and cargo on conveyance location information.

ICAOforActualDestination: An airfield code for actual destination. Indicates aircraft, crew, passengers, and cargo on conveyance location information.

ICAOAirfieldforAlternate: An airfield code for Alternate. Indicates aircraft, crew, passengers, and cargo on conveyance location information.

NatureofSource-Code: Nature of the source: Could be one of “anonymous tip,” “confidential source,” “trained interviewer,” “written statement—victim, witness, other,” “private sector,” or “other source.”

PrivacyFieldIndicator: Data element that may be used to identify an individual and therefore is subject to protection from disclosure under applicable privacy rules. Removal of privacy fields from a detailed report will result in a summary report. This privacy field informs users of the summary information exchange that additional information may be available from the originator of the report.

ReportPurgeDate: The date by which the privacy fields will be purged from the record system; general observation data is retained. Purge policies vary from jurisdiction to jurisdiction and should be indicated as part of the guidelines.

ReportPurgeReviewDate: Date of review to determine the disposition of the privacy fields in a detailed ISE-SAR IEPD record.

SourceReliabilityCode: Reliability of the source, in the assessment of the reporting organization: could be one of “reliable,” “unreliable,” or “unknown.”

VesselHailingPort: The identifying attributes of the hailing port of a vessel.

VesselNationalFlag: A data concept for a country flag under which a vessel sails.

SECTION V: INFORMATION EXCHANGE IMPLEMENTATION ARTIFACTS

A. Domain Model

General Domain Model Overview

The domain model provides a visual representation of the business data requirements and relationships (Figure 2). This Unified Modeling Language (UML)-based Model represents the Exchange Model artifact required in the information exchange development methodology. The model is designed to demonstrate the organization of data elements and illustrate how these elements are grouped together into classes. Further, it describes relationships between these classes. A key consideration in the development of a domain model is that it must be independent of the mechanism intended to implement the model. The domain model is actually a representation of how data is structured from a *business* context. As the technology changes and new Functional Standards emerge, developers can create new standards mapping documents and schema tied to a new standard without having to readdress business process requirements.

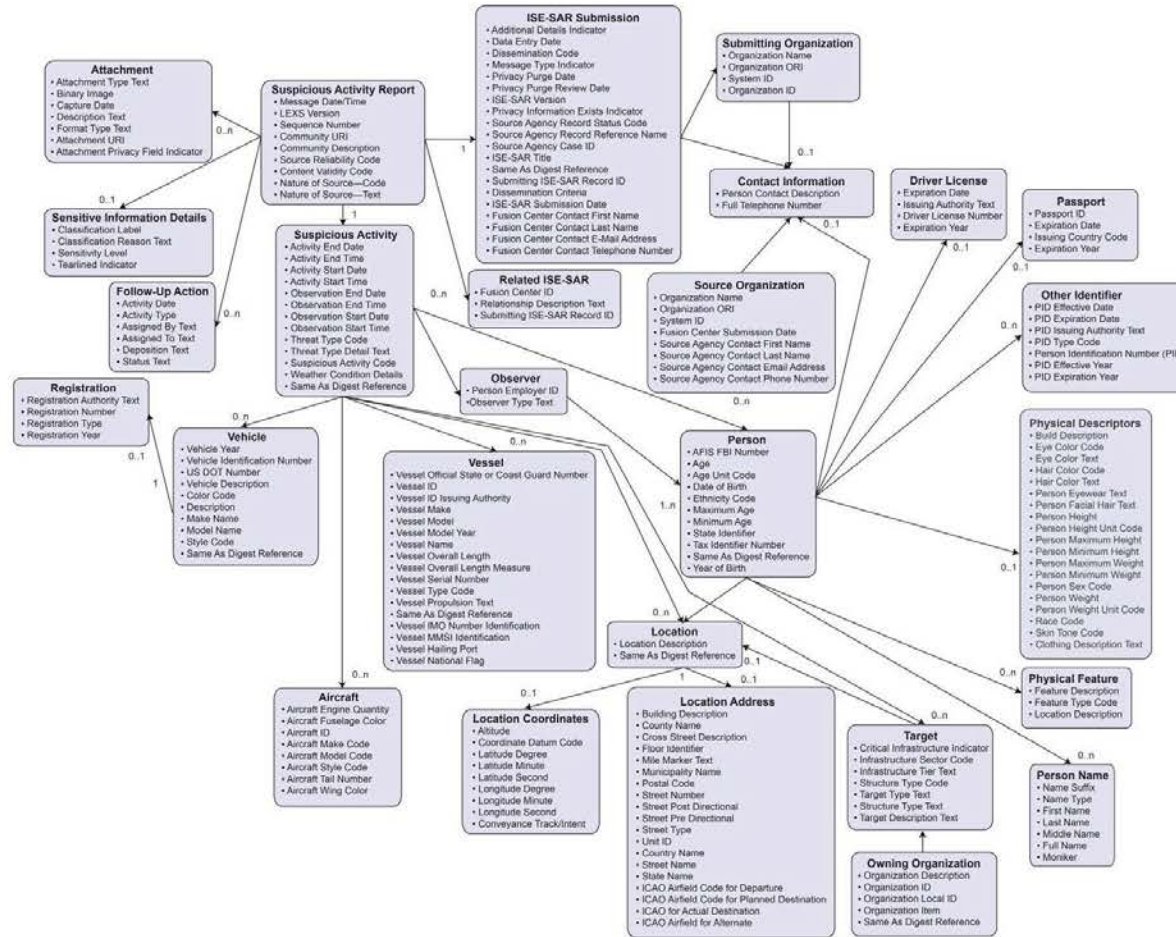


Figure 2 – UML-based Model

B. General Mapping Overview

The detailed component mapping template provides a mechanism to cross-reference the business data requirements documented in the domain model to their corresponding XML Element in the XML Schema. It includes a number of items to help establish equivalency including the business definition and the corresponding XML Element Definition.

C. ISE-SAR Mapping Overview

The Mapping Spreadsheet contains seven unique items for each ISE-SAR data class and element. The Mapping Spreadsheet columns are described in this section.

Table 4 – Mapping Spreadsheet Column Descriptions

Spreadsheet Name and Row	Description
Privacy Field Indicator	This field indicates that the information may be used to identify an individual.
Source Class/ Element	Content in this column is either the data class (grouping of data elements) or the actual data elements. Classes are highlighted and denoted with cells that contain blue background, while elements have a white background. The word “Source” is referring to the ISE-SAR information exchange.
Source Definition	The content in this column is the class or element definition defined for this ISE-SAR information exchange. The word “Source” is referring to the ISE-SAR information exchange definition.
Target Element	The content in this column is the actual namespace path deemed equal to the related ISE-SAR information exchange element.
Target Element Definition	The content in this column provides the definition of the target or NIEM element located at the aforementioned source path. “Target” is referring to the NIEM definition.
Target Element Base	Indicates the data type of the terminal element. Data types of niem-xsd:String or nc:TextType indicate free-form text fields.
Mapping Comments	Provides technical implementation information for developers and implementers of the information exchange.

D. Schemas

The *ISE-SAR Functional Standard* contains the following compliant schemas:

- Subset Schema
- Exchange Schema
- Extension Schema
- Wantlist

E. Examples

The *ISE-SAR Functional Standard* contains two samples that illustrate exchange content as listed below.

XSL Style Sheet

This information exchange artifact provides an implementer and users with a communication tool that captures the look and feel of a familiar form, screen, or like peripheral medium for schema translation testing and user validation of business rules.

XML Instance

This information exchange artifact provides an actual payload of information with data content defined by the schema.

PART B—ISE-SAR CRITERIA GUIDANCE

Part B provides a more thorough explanation of ISE-SAR pre-operational behavioral categories and criteria. This guidance highlights the importance of having a trained analyst or investigator take into account the context, facts, and circumstances in reviewing suspicious behaviors to identify those SARs with a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism). It is important to understand, however, that the behavioral categories and criteria listed below reflect studies of prior terrorism incidents and are not intended to be limited in any way by the descriptive examples.¹⁹ The descriptive examples outlined below in the third column do not represent all possible examples that relate to ISE-SAR submissions. They are provided as a nonexhaustive list of illustrations of pre-operational behaviors that may support the documentation and submission of an ISE-SAR based on the contextual assessment of the reviewing analyst or investigator.

In order to ensure that Part B is responsive to changes in the threat environment, the ISA IPC will establish a formal process for reviewing and updating the behavioral categories in the first column and the behavioral criteria set forth in the second column. (*See the chart below.*) The process will involve coordination and consultation between and among NSI participants and other stakeholders, who will examine the current body of knowledge regarding terrorism and other criminal activity. This process will result in the issuance of an update to the *ISE-SAR Functional Standard* when revisions are made to either or both of the first or second columns.

As needed, the DHS, in conjunction with the FBI, will guide a *separate* process to allow for interim updates to the descriptive examples contained in the third column of Part B. Updates to the third column will be based on field experience (e.g., emerging threats, trip wire reports, and other intelligence) and will be documented in the change management chart²⁰ of the *ISE-SAR Functional Standard*, rather than reissuance of the *ISE-SAR Functional Standard* by the PM-ISE.

The nine behaviors identified below as “Potential Criminal or Non-criminal Activity Requiring Additional Information During Vetting” are not inherently criminal behaviors and may include constitutionally protected activities that must not be documented in an ISE-SAR that contains PII unless there are articulable facts or circumstances that clearly support the determination that the behavior observed is not innocent, but rather reasonably indicative of pre-operational planning associated with terrorism. Race, ethnicity, gender, national origin, religion, sexual orientation, or

¹⁹ In addition to the descriptive examples listed in Part B and in order to further enhance NSI participants’ understanding of the Part B behavioral categories and criteria, the DHS, in conjunction with the FBI, may develop additional examples to be included in implementation materials (e.g., the *Vetting ISE-SAR Data* guidance) or delivered through training. Additionally, relevant federal and SLTT law enforcement agencies may identify and report additional examples of terrorism behavior within the 16 behavioral categories to the DHS or the FBI.

²⁰ This chart is included on page 6 of this *Functional Standard*.

gender identity must not be considered as factors creating suspicion (but attributes may be documented in specific suspect descriptions for identification purposes).²¹ The activities listed as “Potential Criminal or Non-Criminal Activity” are not inherently criminal behaviors and are potentially constitutionally protected; thus, additional facts or circumstances must be articulated in the incident. For example, the trained analyst or investigator should document specific additional facts or circumstances indicating that the behavior is suspicious, such as steps to conceal one’s location and avoid detection while taking pictures.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
DEFINED CRIMINAL ACTIVITY AND POTENTIAL TERRORISM NEXUS ACTIVITY		
Breach/ Attempted Intrusion	Unauthorized personnel attempting to enter or actually entering a restricted area, secured protected site, or nonpublic area. Impersonation of authorized personnel (e.g., police/security officers, janitor, or other personnel).	<ul style="list-style-type: none"> • At 1:30 a.m., an individual breached a security perimeter of a hydroelectric dam complex. Security personnel were alerted by an electronic alarm and observed the subject on CCTV, taking photos of himself in front of a “No Trespassing” sign and of other parts of the complex. The subject departed prior to the arrival of security personnel. • A railroad company reported to police officers that video surveillance had captured images of three individuals illegally entering a train station to gain access to a restricted-access tunnel and taking photos of the tunnel.

²¹ See footnote 9 for additional guidance.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
Misrepresentation	Presenting false information or misusing insignia, documents, and/or identification to misrepresent one's affiliation as a means of concealing possible illegal activity.	<ul style="list-style-type: none"> • A state bureau of motor vehicles employee discovered a fraudulent driver's license in the possession of an individual applying to renew the license. A criminal investigator determined that the individual had also fraudulently acquired a passport in the same name and used it to make several extended trips to countries where terrorist training has been documented. • An individual used a stolen uniform from a private security company to gain access to the video monitoring control room of a shopping mall. Once inside the room, the subject was caught trying to identify the locations of surveillance cameras throughout the entire mall.
Theft/Loss/ Diversion	Stealing or diverting something associated with a facility/infrastructure or secured protected site (e.g., badges, uniforms, identification, emergency vehicles, technology, or documents {classified or unclassified}), which are proprietary to the facility/infrastructure or secured protected site.	<ul style="list-style-type: none"> • A federal aerospace facility reported a vehicle burglary and the theft of an employee's identification credential, a secure ID token, and an encrypted thumb drive. • An explosives ordnance company reported a burglary of a storage trailer. Items stolen included electric initiators, radios, and other items that could be used in connection with explosives.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
Sabotage/ Tampering/ Vandalism	Damaging, manipulating, defacing, or destroying part of a facility/infrastructure or secured protected site.	<ul style="list-style-type: none"> • A light-rail authority reported the discovery of a track switch that had been wrapped in a length of chain in a possible attempt to derail a passenger train car. • A natural gas company reported the deliberate removal of gas meter plugs on the “customer side” in two separate locations approximately a quarter of a mile apart. One location was a government facility. The discovery was made as the government facility’s sensor detected the threat of an explosion.
Cyberattack	Compromising or attempting to compromise or disrupt an organization’s information technology infrastructure.	<ul style="list-style-type: none"> • A federal credit union reported it was taken down for two and a half hours through a cyberattack, and the attacker was self-identified as a member of a terrorist organization. • A state’s chief information officer reported the attempted intrusion of the state’s computer network by a group that has claimed responsibility for a series of hacks and distributed denial-of-service attacks on government and corporate targets.
Expressed or Implied Threat	Communicating a spoken or written threat to commit a crime that will result in death or bodily injury to another person or persons or to damage or compromise a facility/infrastructure or secured protected site.	<ul style="list-style-type: none"> • A customer-experience feedback agency received a call from a watchlisted individual stating, “Wait till they see what we do to the ATF, IRS, NSA.” • A military museum received a threatening letter containing a white powder. The letter claimed a full-scale anthrax attack had been launched in retaliation for crimes committed by the U.S. Armed Forces.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
Aviation Activity	Learning to operate, or operating an aircraft, or interfering with the operation of an aircraft in a manner that poses a threat of harm to people or property and that would arouse suspicion of terrorism or other criminality in a reasonable person. Such activity may or may not be a violation of Federal Aviation Regulations.	<ul style="list-style-type: none">• Federal air traffic control personnel reported two separate laser beam cockpit illumination incidents involving different commercial airliners occurring at night and during the take-off phase of flight. The reports revealed that the laser beam in both incidents originated from the same general geographic area, near a major airport on the East Coast. These findings indicate the likelihood of purposeful acts by the same individual.• A chemical facility representative reported an unauthorized helicopter hovering within 50 feet of a chemical tank located in a posted restricted area. An FAA registry search of the tail number was negative, indicating use of an unregistered number, which suggests an attempt to conceal the identity of the plane's owner and/or its place of origin.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
POTENTIAL CRIMINAL OR NON-CRIMINAL ACTIVITY REQUIRING ADDITIONAL INFORMATION DURING VETTING		
Eliciting Information	Questioning individuals or otherwise soliciting information at a level beyond mere curiosity about a public or private event or particular facets of a facility's or building's purpose, operations, security procedures, etc., in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.	<ul style="list-style-type: none"> • A tour bus company servicing one of the nation's national monuments reported that a male subject asked a driver many unusual and probing questions about fuel capacity, fueling locations, and fueling frequency such that the driver became very concerned about the intent of the questioning. The male subject was not a passenger. • A guest services employee at a shopping center was questioned by an individual about how much security was on the property. The employee contacted security personnel, who confronted the individual. When questioned by security personnel, the individual quickly changed his questions to renting a wheelchair and then left without being identified. Security personnel reported that the individual seemed very nervous and that his explanations were not credible.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
Testing or Probing of Security	Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel, or cybersecurity capabilities in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.	<ul style="list-style-type: none"> • An individual who refused to identify himself to facility personnel at a shipping port reported that he was representing the governor's office and wanted to access the secure area of a steel manufacturer's space. He was inquiring about the presence of foreign military personnel. The individual fled when he realized that personnel were contacting the security office about his activities. He ran through the lobby and departed in a vehicle with an out-of-state license plate and containing two other individuals. • An individual discharged a fire extinguisher in a stairwell of a hotel and set off the building's fire alarm. This individual was observed entering the hotel approximately two minutes before the alarm sounded, was observed exiting from the stairwell at about the same time as the alarm, and then was observed in the lobby area before leaving the hotel.
Recruiting/Financing	Providing direct financial support to operations teams and contacts or building operations teams and contacts; compiling personnel data, banking data, or travel data in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.	<ul style="list-style-type: none"> • A prison inmate reported an effort to radicalize inmates nearing release toward violence. According to the plan, released inmates would go to a particular location for the purpose of obtaining information about attending an overseas terrorist training camp. • An individual reported that a former friend and business associate (a chemist) had recently asked him to participate in a terrorist-cell operation by providing funding to purchase needed equipment. The funding for the operation was reportedly linked to the illegal production of drugs.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
Photography	Taking pictures or video of persons, facilities, buildings, or infrastructure in an unusual or surreptitious manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include taking pictures or video of infrequently used access points, the superstructure of a bridge, personnel performing security functions (e.g., patrols, badge/vehicle checking), security-related equipment (e.g., perimeter fencing, security cameras), etc.	<ul style="list-style-type: none">• A citizen reported to local police that she saw an unknown male crouched down in the back of an SUV with the hatchback open half-way. The subject was videotaping a National Guard readiness center. The vehicle was parked on the side of the road but sped away when the citizen began to approach the vehicle. The citizen could not provide a license tag number.• A citizen observed a female subject taking photographs of a collection of chemical storage containers in the vicinity of the port. The subject was hiding in some bushes while taking photographs of the storage tanks. The citizen reported this information to the city's port police. When the port police officer arrived and approached the subject, she ran to a nearby vehicle and sped off.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
Observation/ Surveillance	Demonstrating unusual or prolonged interest in facilities, buildings, or infrastructure beyond mere casual (e.g., tourists) or professional (e.g., engineers) interest and in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include observation through binoculars, taking notes, attempting to mark off or measure distances, etc.	<ul style="list-style-type: none"> • A mall security officer observed a person walking through the mall, filming at waist level, and stopping at least twice to film his complete surroundings, floor to ceiling. The subject became nervous when he detected security personnel observing his behavior. Once detained, the subject explained that he came to the mall to walk around and was simply videotaping the mall for his brother. The camera contained 15 minutes of mall coverage and footage of a public train system, along with zoomed photos of a bus. • Military pilots reported that occupants of multiple vehicles were observing and photographing in the area of residences of the military pilots. The pilots are responsible for the transport of special forces units. The report was made once the pilots realized that they had been individually surveyed by occupants of multiple vehicles during the same time period.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
Materials Acquisition/Storage	Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, radio control toy servos or controllers; fuel, chemicals, or toxic materials; and timers or other triggering devices, in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.	<ul style="list-style-type: none"> • A garden center owner reported an individual in his twenties seeking to purchase 40 pounds of urea and 30 pounds of ammonium sulfate. The owner does not carry these items and became suspicious when the individual said he was purchasing the items for his mother and then abruptly departed the business. • A female reported that a man wanted to borrow her car to purchase fertilizer to add to the 3,000 pounds he had already acquired. When asked why he was acquiring fertilizer, he responded that he was going to “make something go boom.” The subject lives in a storage unit and utilizes several other storage units at the location.
Acquisition of Expertise	Attempts to obtain or conduct training or otherwise obtain knowledge or skills in security concepts, military weapons or tactics, or other unusual capabilities in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.	<ul style="list-style-type: none"> • A fusion center received information on a watch-listed individual who was making repeated attempts to gain a hazardous materials endorsement for his commercial driver’s license even though his immigration status made him ineligible. • A complaint was received from a gun shop about an individual under the age of 21 who had brought multiple groups of students into the gun shop to rent weapons to shoot. They desired to shoot assault rifles and handguns and asked questions about how to get around state and federal laws on weapon possession and transport.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
Weapons Collection/Discovery	Collection or discovery of unusual amounts or types of weapons, including explosives, chemicals, and other destructive materials, or evidence, detonations or other residue, wounds, or chemical burns, that would arouse suspicion of terrorism or other criminality in a reasonable person.	<ul style="list-style-type: none"> • A city employee discovered a backpack near a park bench along the route of a planned Martin Luther King Day march in the city. The backpack contained an improvised explosive device. • A suspicious person call resulted in the discovery of three individuals possessing hand-held radios, a military-grade periscope, a 7mm Magnum scoped rifle, an AK-74 assault rifle, a pistol-gripped shotgun, a semi-automatic handgun, a bandolier of shotgun ammunition, dozens of loaded handgun magazines, dozens of AK-74 magazines, Ghillie suits, several homemade explosive devices constructed of pill bottles, blast simulators, and military clothing.
Sector-Specific Incident	Actions associated with a characteristic of unique concern to specific sectors (e.g., the public health sector), with regard to their personnel, facilities, systems, or functions in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.	<ul style="list-style-type: none"> • A water company reported that it had security footage of an unknown person breaking into the premises. At 5 a.m., the individual cut through a fence and used a tool to breach a door. Once inside the building, the person took photos of the chlorination system, including the chlorine tank. A pump failure occurred, but it was not certain that this was related to the break-in. • A vehicle containing two individuals was discovered in a secure area of a loading dock at a facility that stores officially designated sensitive chemicals. The vehicle sped off upon discovery by security personnel. Surveillance footage revealed that the individuals gained entry by manually lifting a security gate to the compound.

PART C—ISE-SAR INFORMATION FLOW DESCRIPTION

Step	Activity	Process	Notes
1	Observation	The information flow begins when a person observes behavior that, based on the circumstances, would appear suspicious to a reasonable person. Such activities could include, but are not limited to, expressed or implied threats, probing of security responses, site breach or physical intrusion, cyberattacks, indications of unusual public health-sector activity, unauthorized attempts to obtain precursor chemical/agents or toxic materials, or other unusual behavior or sector-specific incidents. ²² Race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity must not be considered as factors creating suspicion (but attributes may be documented in specific suspect descriptions for identification purposes). ²³	The observer may be a private citizen, a government official, or a law enforcement officer.

²² A SAR is official documentation of observed behavior that is reasonably indicative of pre-operational planning associated with terrorism or other criminal activity. ISE-SARs are a subset of all SARs that have been determined by an appropriate authority to have a potential nexus to terrorism. An ISE-SAR is a SAR (as defined below in 5.t) that has been determined, pursuant to a two-part process, to have a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism). ISE-SAR business rules and privacy and civil liberties requirements will serve as a unified process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.

²³ See footnote 9 for additional guidance.

Step	Activity	Process	Notes
2	Initial Response and Investigation	<p>An official of a Federal, State, local, tribal, or territorial agency with jurisdiction responds to the reported observation.²⁴ This official gathers additional facts through personal observations, interviews, and other investigative activities. At the discretion of the official, further observation or engaging the subject in conversation may be required. Additional information acquired from such limited investigative activity may then be used to determine whether to dismiss the activity as innocent or escalate to the next step of the process, which may include reporting it to the FBI's JTTF. In the context of priority information requirements, as provided by State and major urban area fusion centers, the officer/agent may use a number of information systems to continue the investigation. These systems provide the officer/agent with a more complete picture of the activity being investigated. Some examples of such systems and the information they may provide include the following:</p> <ul style="list-style-type: none"> • The Department of Motor Vehicles provides driver's license and vehicle registration information. • The National Crime Information Center provides wants and warrants information; criminal history information; and access to the Terrorist Screening Center, the terrorist watch list, and Regional Information Sharing Systems (RISS). • Other Federal and SLTT systems can provide criminal checks within the immediate and surrounding jurisdictions. <p>When the initial investigation is complete, the official documents the event. The report becomes the initial record for the law enforcement or Federal agency's records management system (RMS).</p>	<p>The event may be documented using a variety of reporting mechanisms and processes, including, but not limited to, reports of investigation, event histories, field interviews, citations, incident reports, and arrest reports.</p> <p>The record may be hard and/or soft copy and does not yet constitute an ISE-SAR.</p>

Step	Activity	Process	Notes
3	Local/Regional Processing	<p>The agency processes and stores the information in the RMS, following agency policies and procedures. The flow will vary depending on whether the reporting organization is an SLTT agency or a field element of a Federal agency.</p> <p><u>SLTT</u>: Based on specific criteria or the nature of the activity observed, the SLTT law enforcement components forward the information to the State or major urban area fusion center and/or FBI's JTTF for further analysis.</p> <p><u>Federal</u>: Federal field components collecting suspicious activity forward their reports to the appropriate resident, district, or division office. This information is reported to field intelligence groups or headquarters elements through processes that vary from agency to agency.</p> <p>In addition to providing the information to its headquarters office, the Federal field component provides an information copy to the State or major urban area fusion center in its geographic region. This information contributes to the assessment of all suspicious activity in the State or major urban area fusion center's area of responsibility.</p>	<p>The State or major urban area fusion center should have access to all suspicious activity reporting in its geographic region, whether collected by SLTT entities or Federal field components.</p>

²⁴ If a suspicious activity has a direct connection to terrorist activity, the flow moves along an operational path. The information must move immediately into law enforcement operations so as to lead to action against the identified terrorist activity. In this case, the suspicious activity would travel from the initial law enforcement contact directly to the FBI's JTTF.

Step	Activity	Process	Notes
4	Creation of an ISE-SAR	<p>The determination of an ISE-SAR is a two-part process. First, at the State or major urban area fusion center or Federal agency, an analyst or law enforcement officer reviews the newly reported information for suspicious behavior based on his or her training and expertise and against ISE-SAR behavior criteria. Second, based on the context, facts, and circumstances, the analyst or investigator determines whether the information meeting the criteria has a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism).</p> <p>Once this determination is made, the information becomes an ISE-SAR and is formatted in accordance with the <i>ISE-SAR Functional Standard</i>. The ISE-SAR is then shared with the FBI's JTTF and appropriate law enforcement and homeland security personnel in the State or major urban area fusion center's area of responsibility.</p>	<p>Some of this information may be used to develop criminal intelligence information or intelligence products that identify trends and other terrorism-related information and are derived from Federal agencies such as NCTC, DHS, and the FBI. For SLTT law enforcement, the ISE-SAR information may or may not meet the reasonable suspicion standard for criminal intelligence information. If it does, the information may <u>also</u> be submitted to a criminal intelligence information database and handled in accordance with 28 CFR Part 23.</p>
5	ISE-SAR Sharing and Dissemination	<p>In a State or major urban area fusion center, the ISE-SAR is shared with the appropriate FBI field components and the DHS representative and made accessible to other law enforcement agencies in the NSI SDR.</p> <p>The FBI field component enters the ISE-SAR information into the FBI system and sends the information to FBI Headquarters.</p> <p>The DHS representative enters the ISE-SAR information into the DHS system and sends the information to DHS, Office of Intelligence Analysis. The ISE-SAR is also made available to the FBI for investigation.</p>	

Step	Activity	Process	Notes
6	Federal Headquarters (HQ) Processing	<p>At the Federal headquarters level, ISE-SAR information is combined with information from other State or major urban area fusion centers and Federal field components and incorporated into an agency-specific national threat assessment that is shared with NSI participants and other ISE members.</p> <p>The ISE-SAR information may be provided to NCTC in the form of an agency-specific strategic threat assessment (e.g., strategic intelligence product).</p>	
7	NCTC Analysis	<p>When product(s) containing the ISE-SAR information are made available to NCTC, they are processed, collated, and analyzed with terrorism information from across the five communities—intelligence, defense, law enforcement, homeland security, and foreign affairs—and open sources.</p> <p>NCTC has the primary responsibility within the Federal government for analysis of terrorism information. NCTC produces federally coordinated analytic products that are shared through NCTC Online, the NCTC secure Web site.</p> <p>The Joint Counterterrorism Assessment Team (JCAT), formerly the Interagency Threat Assessment and Coordinating Group (ITACG), housed at NCTC, facilitates the production of coordinated terrorism-related products that are focused on issues and needs of SLTT entities and, when appropriate, private-sector entities. JCAT is the mechanism that facilitates the sharing of counterterrorism information with SLTT entities.</p>	

Step	Activity	Process	Notes
8	NCTC Alerts, Warnings, Notifications	NCTC products, ²⁵ informed by the JCAT as appropriate, are shared with all appropriate Federal departments and agencies and with SLTT entities through the State or major urban area fusion centers. The sharing with SLTT entities and the private sector occurs through the Federal departments or agencies that have been assigned the responsibility and have connectivity with the State or major urban area fusion centers. Some State or major urban area fusion centers, with secure connectivity and an NCTC Online account, can access NCTC products directly. State or major urban area fusion centers will use NCTC and JCAT informed products to help develop geographic-specific risk assessments (GSRAs) to facilitate regional counterterrorism efforts. The GSRAs are shared with SLTT entities and the private sector as appropriate. The recipient of a GSRA may use the GSRA to develop information gathering priorities or requirements.	NCTC products form the foundation of informational needs and guide collection of additional information. NCTC products should be responsive to informational needs of SLTT entities.
9	Focused Collection	The information has come full circle and the process begins again, informed by another Federal organization's product and the identified information needs of SLTT entities and Federal field components.	

²⁵ NCTC products include: Alerts, warnings, and notifications—identifying time sensitive or strategic threats; situational awareness reports; and strategic and foundational assessments of terrorist risks and threats to the United States and related intelligence information.

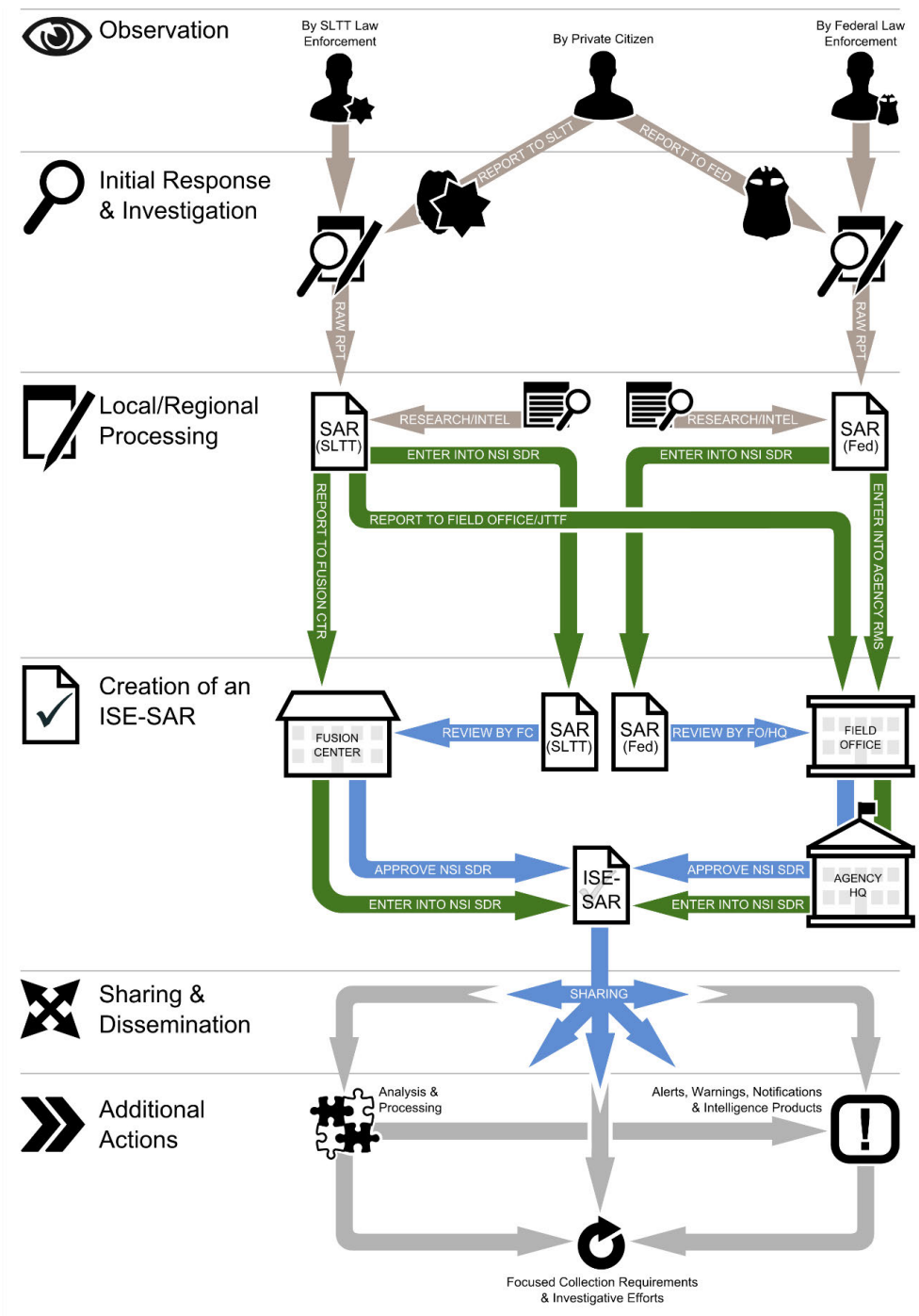


Figure 3—SAR Information Flow Diagram

PART D—ACRONYMS

CTISS	Common Terrorism Information Sharing Standards
CONOPS	Concept of Operations
DHS	Department of Homeland Security
DOJ	Department of Justice
EE	Evaluation Environment
FBI	Federal Bureau of Investigation
FIGs	Field Intelligence Groups
GRSA	Geographic-Specific Risk Assessment
IEPD	Information Exchange Package Document
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISA IPC	Information Sharing and Access Interagency Policy Committee
ISE	Information Sharing Environment
ISE-SAR	Information Sharing Environment-Suspicious Activity Report
JCAT	Joint Counterterrorism Assessment Team
JTTF	Joint Terrorism Task Force
NCTC	National Counterterrorism Center
NIEM	National Information Exchange Model
NSI	Nationwide SAR Initiative
P/CRCL	privacy, civil rights, and civil liberties
P/CL	privacy and civil liberties

PII	personally identifiable information
PM-ISE	Program Manager for the Information Sharing Environment
SAR	Suspicious Activity Report
SDR	Shared Data Repository
SLTT	State, local, tribal, and territorial

1 BENJAMIN C. MIZER
Acting Assistant Attorney General

2 ANTHONY J. COPPOLINO
Deputy Branch Director

3 PAUL G. FREEBORNE
Senior Trial Counsel
Virginia State Bar No. 33024

4 KIERAN G. GOSTIN
Trial Attorney

5 Civil Division, Federal Programs Branch
U.S. Department of Justice
P.O. Box 883
Washington, D.C. 20044
Telephone: (202) 353-0543
Facsimile: (202) 616-8460
E-mail: paul.freeborne@usdoj.gov

6 *Attorneys for Federal Defendants*

7
8
9
10
11
12
13
14 **UNITED STATES DISTRICT COURT**
15 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**

16 WILEY GILL; JAMES PRIGOFF; TARIQ
17 RAZAK; KHALID IBRAHIM; and AARON
CONKLIN,

18 Plaintiffs,

19 v.

20 DEPARTMENT OF JUSTICE, *et al.*,

21 Defendants.
22
23

No. 3:14-cv-03120 (RS)

**DEFENDANTS' ANSWER TO
COMPLAINT**

1 interviewed Plaintiff Prigoff by telephone on August 23, 2004 on a telephone number associated
2 with Prigoff's residence in Sacramento, California. Fifth Sentence: Defendants are without
3 knowledge or information sufficient to admit or deny the allegations in this sentence, except to
4 admit that information relating to an incident involving Plaintiff Prigoff was submitted to the
5 FBI. Defendants further aver that no information referencing Plaintiff Prigoff was uploaded into,
6 or resides in, eGuardian.

7 7. First Sentence: Defendants are without knowledge or information sufficient to
8 admit or deny the allegations in this sentence. Second Sentence: Defendants are without
9 knowledge or information sufficient to admit or deny the allegations in this sentence. Third
10 Sentence: Defendants are without knowledge or information sufficient to admit or deny the
11 allegations in this sentence. Fourth Sentence: Defendants did not generate the document
12 attached as Appendix B to the Complaint, and are without knowledge or information sufficient to
13 admit or deny the allegations in this sentence. Fifth Sentence: To the extent this sentence refers
14 to the document attached as Appendix B to the Complaint, Defendants admit that the document
15 contains the language quoted in this sentence but are otherwise without knowledge or
16 information sufficient to admit or deny the allegations in this sentence. Sixth Sentence:
17 Defendants are without knowledge or information sufficient to admit or deny the allegations in
18 this sentence. Seventh Sentence: To the extent this sentence refers to the document attached as
19 Appendix B to the Complaint, Defendants are without knowledge or information sufficient to
20 admit or deny the allegations in this sentence because Appendix B was not created by
21 Defendants, is redacted and bears no title. Defendants aver, nonetheless, that Appendix B
22 appears to contain information that is similar to that contained in two incident reports relating to
23 a 2011 incident involving Plaintiff Ibrahim that were uploaded to eGuardian. One of these
24 referenced incident reports was subsequently deleted from eGuardian pursuant to the applicable
25 retention policy, making it inaccessible (other than to the FBI) to federal, state, local, tribal, and
26 territorial law enforcement agencies through any NSI database. The other incident report will be
27 deleted from eGuardian pursuant to the applicable retention policy. Eighth Sentence:
28 Defendants admit the allegations in this sentence.

1 94. First Sentence: Defendants deny the allegations in this sentence, except admit
2 that the PM-ISE issued a Functional Standard identifying “[a]ttempts to obtain or conduct
3 training in security concepts; military weapons or tactics; or other unusual capabilities that would
4 arouse suspicion in a reasonable person” as a behavior that may be reasonably indicative of pre-
5 operational planning related to terrorism. With regard to the allegations made regarding the
6 Department of Justice, while the exhibits attached to the Complaint appear to contain similar
7 language to that referenced in such allegations, Defendants can neither confirm nor deny the
8 authenticity of the documents, or the information attributed therein, and reserve the right to assert
9 privilege, as necessary. Second Sentence: Defendants are without knowledge or information
10 sufficient to admit or deny the allegations in this sentence.

11 95. First Sentence: Defendants deny the allegations contained in this sentence.
12 Second Sentence: Defendants are without knowledge or information sufficient to admit or deny
13 the allegations in this sentence.

14 96. First Sentence: Defendants deny the allegations in this sentence, except admit
15 that referenced document contains the language quoted in this sentence. Second Sentence:
16 Defendants are without knowledge or information sufficient to admit or deny the allegations in
17 this sentence.

18 97. To the extent this paragraph refers to the actions of any non-Defendant,
19 Defendants are without knowledge or information sufficient to admit or deny the allegations in
20 this paragraph. To the extent the allegations in this paragraph refer to the actions of Defendants,
21 Defendants admit, as disclosed above, that an incident report relating to a 2010 incident
22 involving Plaintiff Gill has been uploaded to eGuardian and an incident report relating to a 2012
23 incident involving Plaintiff Gill has been uploaded to eGuardian. Whether or not any additional
24 investigative actions have been undertaken by Defendants regarding Plaintiff Gill, and any
25 information related to the nature, reasons or manner of undertaking any such investigation (if
26 any), is law enforcement sensitive and otherwise privileged information, the disclosure of which
27 is not required in response to the Complaint.
28

1 117. Defendants are without knowledge or information sufficient to admit or deny the
2 allegations in this paragraph.

3 118. Defendants are without knowledge or information sufficient to admit or deny the
4 allegations in this paragraph.

5 119. Defendants are without knowledge or information sufficient to admit or deny the
6 allegations in this paragraph.

7 120. Defendants are without knowledge or information sufficient to admit or deny the
8 information in this paragraph.

9 121. First Sentence: To the extent this sentence refers to the document attached as
10 Appendix B to the Complaint, Defendants admit that the document lists November 14, 2011 as
11 the “date created” and contains the language quoted in this sentence but are otherwise without
12 knowledge or information sufficient to admit or deny the allegations in this sentence. Second
13 Sentence: To the extent this sentence refers to the document attached as Appendix B to the
14 Complaint, Defendants are without knowledge or information sufficient to admit or deny the
15 allegations in this sentence because Appendix B is redacted and bears no title. Defendants aver,
16 nonetheless, that Appendix B appears to contain information that is similar to that contained in
17 two incident reports relating to a 2011 incident involving Plaintiff Ibrahim that were uploaded to
18 eGuardian. One of these referenced incident reports was subsequently deleted from eGuardian
19 pursuant to the applicable retention policy, making it inaccessible (other than to the FBI) to
20 federal, state, local, tribal, and territorial law enforcement agencies through any NSI database.
21 The other incident report will be deleted from eGuardian pursuant to the applicable retention
22 policy. Third Sentence: Defendants are without knowledge or information sufficient to admit
23 or deny the allegations in this sentence.

24 122. Defendants are without knowledge or information sufficient to admit or deny this
25 sentence, except to admit that PM-ISE issued a Functional Standard identifying the “[a]quisition
26 and/or storage of unusual quantities of materials such as cell phones, pagers, fuel, chemicals,
27 toxic materials, and timers such that a reasonable person would suspect possible criminal
28 activity” as a behavior that may be reasonably indicative of pre-operational planning related to

1 regarding the Department of Justice set forth in these sentences, while the exhibits attached to the
2 Complaint appear to contain similar language to that referenced in such allegations, Defendants
3 can neither confirm nor deny the authenticity of the documents, or the information attributed
4 therein, and reserve the right to assert privilege, as necessary. Fourth Sentence: To the extent
5 this sentence refers to the document attached as Appendix C to the Complaint, Defendants are
6 without information or knowledge sufficient to admit or deny the allegations in this sentence
7 because Appendix C is redacted and bears no title. Defendants aver, nonetheless, that Appendix
8 C appears to contain information that is similar to that contained in an incident report that was
9 uploaded to eGuardian. The incident report was manually deleted by the originating agency that
10 submitted the incident report.

11 134. To the extent this paragraph refers to the actions of any non-Defendant,
12 Defendants are without knowledge or information sufficient to admit or deny the allegations in
13 this paragraph. To the extent the allegations in this paragraph refer to the actions of Defendants,
14 Defendants admit that an incident report relating to 2011 incident involving Plaintiff Razak was
15 uploaded to eGuardian. Whether or not any additional investigative actions have been
16 undertaken by Defendants regarding Plaintiff Razik, and any information related to the nature,
17 reasons or manner of undertaking any such investigation (if any), is law enforcement sensitive
18 and otherwise privileged information, the disclosure of which is not required in response to the
19 Complaint.

20 135. Defendants are without knowledge or information sufficient to admit or deny the
21 allegations in this paragraph.

22 136. To the extent this sentence refers to the document attached as Appendix C to the
23 Complaint, Defendants are without information or knowledge sufficient to admit or deny the
24 allegations in this sentence because Appendix C is redacted and bears no title. Defendants aver,
25 nonetheless, that Appendix C appears to contain information that is similar to that contained in
26 an incident report relating to a 2011 incident involving Plaintiff Razak that was uploaded to
27 eGuardian. The incident report was manually deleted from eGuardian by the originating agency
28 that submitted the incident report.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

)	
)	No. 3:14-cv-03120-RS
)	
WILEY GILL; JAMES PRIGOFF; TARIQ)	JOINT CASE MANAGEMENT
RAZAK; KHALED IBRAHIM; and AARON)	STATEMENT & [PROPOSED] ORDER
CONKLIN,)	
Plaintiffs,)	
)	
v.)	
)	
DEPARTMENT OF JUSTICE; ERIC H.)	
HOLDER, Jr., in his official capacity as the)	
Attorney General of the United States;)	
PROGRAM MANAGER - INFORMATION)	
SHARING ENVIRONMENT;)	
KSHEMENDRA PAUL, in his official)	
capacity as the Program Manager of the)	
Information Sharing Environment,)	
Defendants.)	

The Parties to the above-entitled action, Plaintiffs Wiley Gill, James Prigoff, Tariq Razak, Khaled Ibrahim, and Aaron Conklin (collectively “Plaintiffs”), by and through their attorneys of record, and Defendants Department of Justice (“DOJ”), Eric. H. Holder, Jr. (“Holder”), Program Manager – Information Sharing Environment (“PM-ISE”), and Kshemendra Paul (“Paul”), jointly submit this JOINT CASE MANAGEMENT STATEMENT & PROPOSED ORDER pursuant to the Standing Order for All Judges of the Northern District of California dated July 1, 2011 and Civil Local Rule 16-9.¹

¹ Counsel for the parties met and conferred by telephone on February 27, 2015. Stephen Scotch-Marmo, Julia Harumi Mass, Nasrina Bargzie, Michael Ableson, and Nicole Sadler participated

1 5. Amendment of Pleadings

2 Plaintiffs do not anticipate amending the pleadings at this time. Defendants reserve the
3 right to oppose any amendment.

4
5 6. Evidence Preservation

6 The Parties certify that they have reviewed the Guidelines Relating to the Discovery of
7 Electronically Stored Information and confirm that the Parties have met and conferred pursuant
8 to Federal Rule of Civil Procedure 26(f) regarding reasonable and proportionate steps taken to
9 preserve evidence relevant to the issues reasonably evident in this action.

10
11 7. Disclosures

12 Defendants contend that these proceedings are exempt from initial disclosures under
13 Federal Rule of Civil Procedure 26(a)(1)(B)(i) because Plaintiffs solely bring claims under the
14 APA. Plaintiffs dispute that these proceedings are exempt from initial disclosures. For the
15 reasons set forth in Paragraph 8(b) below, Plaintiffs contend that review in this case is not
16 limited to the “administrative record.” Fed. R. Civ. P. 26(a)(1)(B)(i).

17 To the extent the Court determines that these proceedings are not exempt from initial
18 disclosures, the Parties hereby stipulate that they will exchange initial disclosures on April 27,
19 2015. Defendants note, however, that the identification of Plaintiff-specific documents may not
20 be possible in light of privilege.

21
22 8. Discovery

23 Defendants’ Position on Proper the Scope of Discovery:

- 24 a. Defendants contend that Plaintiffs’ claims should be resolved on an administrative record
25 because Plaintiffs seek relief solely under the APA. *Fla. Power & Light Co. v. Lorion*,
26 470 U.S. 729, 743–44 (1985). Accordingly, Plaintiffs should only be permitted to seek

1 discovery on the merits in this action if they are able to satisfy their burden of
2 demonstrating that they are entitled to discovery under one of the narrow exceptions to
3 the well-recognized rule that discovery is not permitted in APA actions. *See Bark v.*
4 *Northrop*, 2 F. Supp. 3d 1147, 1152 (D. Or. 2014) (holding that it is the burden of the
5 party seeking discovery to establish that an exception to general bar on discovery in APA
6 cases applies); *McCrary v. Gutierrez*, 495 F. Supp. 2d 1038, 1041 (N.D. Cal. 2007)
7 (Seeborg, J.) (“Because a court’s review of an agency decision is limited to the
8 administrative record, discovery is generally not permitted in APA cases.”). While, as
9 Plaintiffs contend below, evidence outside of the administrative record can be considered
10 on the question of standing, that is permitted so that Plaintiffs’ can “satisfy a prerequisite
11 to this [C]ourt’s jurisdiction,” *Nw. Entl. Def. Ctr. v. Bonneville Power Admin.*, 117 F.3d
12 1520, 1528 (9th Cir. 1997). It does not permit Plaintiffs to seek discovery on the merits.
13 Contrary to Plaintiffs’ contention below, therefore, merits discovery should not be
14 permitted until Plaintiffs carry their burden of demonstrating an exception to the general
15 bar to discovery in APA actions. Because that cannot occur until Defendants have the
16 opportunity to present the administrative record, Plaintiffs’ proposal is not in accordance
17 with the law governing APA review. Plaintiffs fail, moreover, to provide any authority
18 for the assertion that final agency action is a subject of discovery in an APA action.
19 Finally, Plaintiffs seek to manufacture a need for discovery based upon the argument that
20 the FBI has issued a different standard for suspicious activity reporting than is set forth
21 by the PM-ISE in the Functional Standard. But they have never pled facts establishing
22 that a separate DOJ standard exists, nor, as the Court recognized in its Order, have they
23 articulated “any significance to the dispute over whether there is one set of protocols or
24 two” in briefing regarding the motion to dismiss, Dkt. 38 at 2. There is thus no basis to
25 adopt Plaintiffs’ proposed schedule, nor any basis to impose upon Defendants the
26 unwarranted burden of moving for a protective order regarding facially improper
27 discovery. Plaintiffs have pled this action as an APA action and review should be
28 conducted in a manner consistent with all other APA challenges.

United States District Court
Northern District of California

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

WILEY GILL, et al.,
Plaintiffs,
v.
DEPARTMENT OF JUSTICE, et al.,
Defendants.

Case No. [14-cv-03120-RS](#)

**ORDER DENYING MOTION TO
DISMISS**

I. INTRODUCTION

In this action brought under the Administrative Procedures Act (“APA”), plaintiffs challenge certain aspects of the National Suspicious Activity Reporting Initiative (“NSI”), a nationwide program that collects, vets, and disseminates intelligence with a possible nexus to terrorism. Plaintiffs contend that defendants Department of Justice (“DOJ”) and the Program Manager-Information Sharing Environment (“PM-ISE”) have issued protocols utilizing an overly broad standard to define the types of activities that should be deemed as having a potential nexus to terrorism. As a result, plaintiffs allege, state and local law enforcement authorities submit “Suspicious Activity Reports” (“SARs”) to the federal government even if unsupported by reasonable suspicion of criminal activity, and innocent Americans are “wrongly branded as potential terrorists.”

Plaintiffs contend that the protocols they are challenging conflict with a duly promulgated DOJ regulation, 28 C.F.R. Part 23, which they assert was adopted to protect

United States District Court
Northern District of California

1 constitutional and privacy rights by prohibiting the collection of criminal intelligence unless
2 supported by reasonable suspicion. In their four-count complaint, plaintiffs assert that each of the
3 two challenged protocols, (1) violates the APA’s requirement that the public be provided a notice
4 and comment period prior to adoption of “legislative rules,” and/or, (2) is invalid as “arbitrary and
5 capricious,” in light of the alleged conflict with 28 C.F.R. Part 23.

6 Defendants move to dismiss, contending plaintiffs lack standing, and have not stated viable
7 APA claims in any event. Alternatively, defendants challenge venue. The motion will be denied,
8 for reasons explained below.

9
10 II. BACKGROUND

11 As plaintiffs describe it, the NSI was created to facilitate the nationwide sharing of
12 information potentially related to terrorism. It is premised on the notion that while state, local, and
13 tribal law enforcement agents – so called “front line” personnel – are well situated to gather that
14 type of information, their reports should be vetted under uniform standards. DOJ and PM-ISE
15 have each issued protocols relating to SAR reporting designed to provide such standards for
16 evaluating information collected by front line personnel before it is disseminated nationally.

17 DOJ’s protocols, which plaintiffs refer to as the “DOJ SAR Standard,” appear in several
18 documents, including one entitled “eGuardian 2008 Privacy Impact Assessment.” The
19 PM-ISE protocols appear in a document entitled “Information Sharing Environment (ISE) –
20 Functional Standard (FS) – Suspicious Activity Reporting (SAR) Version 1.5.”
21 (hereinafter “Functional Standard 1.5”). Defendants contend there is only one standard—
22 Functional Standard 1.5—and that the DOJ protocols conform thereto and do not represent a set of
23 rules that could be separately challenged. Plaintiffs object that defendants’ position contradicts
24 the allegations of the complaint and certain evidence. For purposes of the present motion,
25 however, neither party contends there is any significance to the dispute over whether there is one
26 set of protocols or two. For convenience, the challenged protocols will hereinafter be referred to
27 as “Defendants’ Standards” without any determination as to whether the so-called DOJ SAR

United States District Court
Northern District of California

1 Standard is separate from Functional Standard 1.5 or not.

2 According to the allegations of the complaint, the SAR process proceeds in three stages:
3 collection by front line personnel, vetting by trained analysts at “fusion centers,” and
4 dissemination to law enforcement nationwide. Front line personnel are allegedly trained in
5 Defendants’ Standards, collect information about people engaged in activities that purportedly
6 have a potential nexus to terrorism, and submit the information in the form of SARs, either
7 directly to the Federal Bureau of Investigation or to a fusion center.

8 Fusion centers, which are federally funded, gather, receive, store, analyze, and share
9 intelligence, including SARs, related to terrorism and other threats. Although the local collecting
10 agencies perform some vetting, the primary responsibility for doing so rests with fusion centers,
11 whose staff are trained in Defendants’ Standards and review SARs for compliance with those
12 Standards.

13 SARs that meet Defendants’ Standards are then disseminated both regionally through the
14 fusion center’s database, and nationally through a data base known as “eGuardian” and/or another
15 national database.¹ The FBI oversees eGuardian, which allows law enforcement personnel across
16 the country to access the SARs that have been uploaded to it. Plaintiffs expressly allege that the
17 federal government maintains SARs sent to eGuardian for 30 years, even when the FBI has
18 determined that a particular SAR has no nexus to terrorism.²

19 Each of the four plaintiffs knows or believes that he is the subject of an SAR, or in the case
20 of one plaintiff, a report similar to an SAR. Plaintiff Wiley Gill, a U.S. citizen and graduate of
21

22 _____
23 ¹ Defendants contend that eGuardian is presently the *only* such database system in use, and
24 request judicial notice of materials found on certain government websites to establish that fact.
25 While judicial notice would not be an appropriate mechanism to resolve this factual issue at the
26 pleading stage or otherwise, the dispute is not material to the issues presented, as the result would
27 be the same regardless of the number of databases presently in use.

28 ² From materials attached as exhibits to the complaint, however, it appears that where no nexus to
potential terrorism can be validated, the SAR will not be made accessible through the ISE. Also,
the protocols appear to include some measures to address removing unfounded information. See
Complaint Exh. D, pp. 61. 63; Exh. E, p. 93.

United States District Court
Northern District of California

1 California State University, Chico, converted to Islam after learning about the religion in a class.
 2 In 2012, the Chico Police Department conducted a warrantless search of his home for reasons
 3 allegedly later acknowledged to be unfounded. The police reported the encounter and two earlier
 4 interactions with Gill in an SAR. The SAR notes that Gill “is unemployed” and states that he had
 5 “potential access to flight simulators via the internet,” because his computer displayed a webpage
 6 titled something “similar to ‘Games that fly under the radar.’” The complaint asserts that Gill, a
 7 video game enthusiast, was likely viewing a website about video games. The SAR concludes by
 8 describing as “worthy of note” Gill’s “full conversion to Islam as a young WMA [white, male
 9 adult]” and his “pious demeanor.”

10 Plaintiff Khaled Ibrahim, a U.S. citizen of Egyptian descent who works in accounting, is
 11 the subject of an SAR describing his attempt to purchase “a large amount of computers.” At the
 12 time, Ibrahim, worked as a purchasing agent, and was seeking to make a bulk purchase of
 13 computers for his employer.

14 Plaintiff Aaron Conklin, believes he is the subject of an SAR. Conklin is a graphic design
 15 student and amateur photographer with an interest in industrial architecture. He has twice been
 16 prevented from photographing oil refineries. In one incident at the Shell refinery in Martinez,
 17 California, he was questioned by private security, and then detained and searched by Contra Costa
 18 Sheriff’s deputies, who told him he had to be placed on an “NSA watch list.”

19 Finally, James Prigoff is a U.S. citizen and renowned photographer of public art, who
 20 believes he is the subject of an “SAR or SAR-like report.” While attempting to photograph a
 21 famous piece of public art on a natural gas storage tank near Boston, he allegedly was harassed by
 22 private guards, who prevented him from photographing the tank from his preferred location.
 23 Although he provided the guards no identifying information, the FBI purportedly then tracked him
 24 cross-country, visited his home in Sacramento, and questioned a neighbor about him.³

25 _____
 26 ³ Because the incident involving Prigoff predated adoption of Defendants’ Standards, they contend
 27 those standards cannot have caused his alleged injury, and, in a footnote, contend his claims are
 28 time-barred in any event. Even assuming the timing issues could ultimately undermine Prigoff’s
 claims, defendants have not shown that his separate dismissal from the action is warranted at this

United States District Court
Northern District of California

III. LEGAL STANDARD

A complaint must contain “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2). While “detailed factual allegations are not required,” a complaint must have sufficient factual allegations to “state a claim to relief that is plausible on its face.” *Ashcroft v. Iqbal*, 566 U.S. 652, 678 (2009) (citing *Bell Atlantic v. Twombly*, 550 U.S. 544, 570 (2007)). A claim is facially plausible “when the pleaded factual content allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Id.* This standard asks for “more than a sheer possibility that a defendant acted unlawfully.” *Id.* The determination is a context-specific task requiring the court “to draw in its judicial experience and common sense.” *Id.* at 1950.

A motion to dismiss a complaint under Rule 12(b)(6) of the Federal Rules of Civil Procedure tests the legal sufficiency of the claims alleged in the complaint. *See Parks Sch. of Bus., Inc. v. Symington*, 51 F.3d 1480, 1484 (9th Cir. 1995). Dismissal under Rule 12(b)(6) may be based on either the “lack of a cognizable legal theory” or on “the absence of sufficient facts alleged under a cognizable legal theory.” *Balistreri v. Pacifica Police Dep’t*, 901 F.2d 696, 699 (9th Cir. 1990).

Defendants also invoke Rule 12(b)(1), arguing that plaintiffs’ purported lack of standing deprives the Court of subject matter jurisdiction. A motion to dismiss for lack of subject matter jurisdiction may be made on the grounds that the lack of jurisdiction appears from the “face of the complaint,” or may be based on extrinsic evidence apart from the pleadings. *Warren v. Fox Family Worldwide, Inc.*, 328 F.3d 1136, 1139 (9th Cir. 2003); *McMorgan & Co. v. First Cal. Mortgage Co.*, 916 F. Supp. 966, 973 (N.D. Cal. 1995). Where the jurisdictional issue is whether the plaintiff has standing, dismissal is also appropriate under Rule 12(b)(6) absent sufficient factual allegations in the complaint, which, if proven, would confer standing. *Sacks v. Office of Foreign Assets Control*, 466 F.3d 764, 771 (9th Cir. 2006).

junction.

United States District Court
Northern District of California

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Defendants’ venue challenge is brought under Rule 12(b)(3), which states that a party may move to dismiss a case for “improper venue.” The question of whether venue is “wrong” or “improper” is generally governed by 28 U.S.C. § 1391. That provision states that “[e]xcept as otherwise provided by law . . . this section shall govern the venue of all civil actions brought in district courts of the United States.” § 1391(a)(1). It further provides that “[a] civil action may be brought in—(1) a judicial district in which any defendant resides, if all defendants are residents of the State in which the district is located; (2) a judicial district in which a substantial part of the events or omissions giving rise to the claim occurred, or a substantial part of property that is the subject of the action is situated; or (3) if there is no district in which an action may otherwise be brought as provided in this section, any judicial district in which any defendant is subject to the court’s personal jurisdiction with respect to such action.” § 1391(b). When venue is challenged, the court must determine whether the case falls within one of the three categories set out in § 1391(b). If it does, venue is proper; if it does not, venue is improper, and the case must be dismissed or transferred under § 1406(a).

III. DISCUSSION

A. Standing

“To satisfy Article III’s standing requirements, a plaintiff must show (1) she has suffered an ‘injury in fact’ that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.” *Bernhardt v. Cnty. of Los Angeles*, 279 F.3d 862, 868–69 (9th Cir. 2002) (quoting *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180–81 (2000)).

Defendants primarily frame their challenge to plaintiffs’ standing as a purported failure to allege facts showing causation and redressability. Defendants’ argument characterizes plaintiffs’ supposed injuries as arising, if at all, primarily from the actions of the “front line” state and local

United States District Court
Northern District of California

1 law enforcement authorities. Defendants contend plaintiffs have not alleged, and credibly cannot,
2 that the scrutiny they purportedly received from state and local police, or even from private
3 security personnel, was the result of the challenged protocols or other conduct of defendants.

4 The allegations of the complaint, however, show that the gravamen of the alleged injuries
5 lie not in actions of “front line” authorities standing alone, but in the fact that those authorities,
6 pursuant to the guidance and training provided by defendants, submit SAR reports under criteria
7 and circumstances that are allegedly inconsistent with legal principles and policies embodied in
8 other law. Plaintiffs’ cognizable challenge is not to the conduct of law enforcement or private
9 security officers during the alleged encounters *per se*, although there is at least some implication
10 that plaintiffs believe Defendants’ Standards lead front line personnel to overreach even at the
11 point of making initial observations. Plaintiffs are claiming injury from what occurs *after* the
12 encounters, pursuant to the Standards.

13 As such, defendants’ contentions as to causality and redressability both fail. The harms
14 plaintiffs seek to remedy arise directly from the existence of Defendants’ Standards. If plaintiffs
15 can show those standards violate the APA, they will be declared invalid.

16 While invoking causality and redressability as the main purported shortcomings of
17 plaintiffs’ standing, defendants also imply that merely being the subject of an SAR, in the national
18 database, should not be deemed a cognizable injury. In light of the privacy and reputational
19 interests involved, however, this argument is not tenable. *See Meese v. Keene*, 481 U.S. 465, 474-
20 75 (1987) (plaintiff had standing to challenge statute labeling films he exhibited as “political
21 propaganda” because of “risk of injury to his reputation”); *Joint Anti-Fascist Refugee Comm. v.*
22 *McGrath*, 341 U.S. 123, 131, 140-41 (1951) (organizations had “clear” standing to challenge
23 loyalty oath based on injury, inter alia, to “reputation”).⁴ Accordingly, the motion to dismiss for
24 lack of standing must be denied.

25 _____
26 ⁴ Defendants suggest that because SARs are not disseminated to the general public, plaintiffs
27 suffer no reputational injury. In light of the alleged wide distribution and availability of the
information, however, this argument is not persuasive.

United States District Court
Northern District of California

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

B. Alternative remedies

Defendants further argue that Plaintiffs’ APA claims are barred because Plaintiffs have adequate alternative remedies, in that they theoretically could sue the individual local agencies or private guards that collected SARs about them. This argument similarly misconstrues the nature of plaintiffs’ claims. The challenge is to the system itself, not to the acts of the “front line” personnel. While plaintiffs may indeed believe that those officials and private actors overstepped their bounds in at least some of the instances (*e.g.*, Conklin contends the security guards had no right to interfere with his taking photographs on public property), the primary issue is the collection and dissemination of SARs through national databases under standards that plaintiffs contend are not appropriate. A suit against local agencies or security guards cannot change Defendants’ Standards. Indeed, local and private defendants likely would have a defense against any claim that their preparation and transmission of SARs is wrongful, when undertaken pursuant to those standards. Accordingly, the APA claims are not subject to dismissal on grounds that plaintiffs have adequate remedies elsewhere.

C. Finality of agency action

Claims under the APA lie only against “final” agency actions. In *Bennett v. Spear*, 520 U.S. 154 (1997), the Supreme Court set out the legal standard for agency action to be considered final:

First, the action must mark the “consummation” of the agency’s decisionmaking process—it must not be of a merely tentative or interlocutory nature. And second, the action must be one by which “rights or obligations have been determined,” or from which “legal consequences will flow.”

Id. at 177-78 (citations omitted). Defendants concede the first prong, but challenge the second, asserting that Functional Standard 1.5 does not impose a “binding legal norm,” but merely provides “functional guidance for the operation of the NSI” and that NSI participants are not “require[d]” to follow this guidance.

United States District Court
Northern District of California

1 It may be that Defendants’ Standards do not mandate any state or local law
2 enforcement agency participate in the NSI and share SARs meeting those standards. There is no
3 dispute, however, that if a state or local law enforcement agency does participate in the NSI and
4 submits SARs, it is to do so consistent with the Defendants’ Standards. As such, those standards
5 “alter the legal regime” and have “direct and appreciable legal consequences,” such that the
6 second prong of the finality requirement is satisfied. *Bennett*, 520 U.S. at 178.

7
8 D. Arbitrary and Capricious

9 Plaintiffs’ first and second claims for relief seek to set aside the DOJ SAR Standard and
10 Functional Standard 1.5, respectively, as “arbitrary, capricious, an abuse of discretion, otherwise
11 not in accordance with law.” Plaintiffs’ theory is that because Defendants’ Standards do not
12 require SARs to be based on a “reasonable suspicion” standard, they conflict with 28 C.F.R. Part
13 23’s requirement that criminal intelligence not be collected or maintained unless supported by
14 “reasonable suspicion.”

15 The rules in that section proceed from an “[o]perating principle[.]” that a “project shall
16 collect and maintain criminal intelligence information concerning an individual only if there is
17 reasonable suspicion that the individual is involved in criminal conduct or activity and the
18 information is relevant to that criminal conduct or activity.” 28 C.F.R. § 23.20(a). There is no
19 dispute that Defendants’ Standards allow for collection and dissemination of SARs not meeting
20 that test.

21 Defendants insist there is no conflict between the Standards and Part 23 because, they
22 contend, the NSI is not a system for collecting “criminal intelligence.” They argue that the
23 Functional Standard and 28 C.F.R. Part 23 were issued pursuant to distinct statutory authorities for
24 application to different information gathering programs. Compare 42 U.S.C. § 3789g(c)
25 (authorizing OJP to issue policy standards for criminal intelligence systems funded under the
26 Omnibus Act) with 6 U.S.C. § 485(f)(2)(A)(iii) (authorizing the Program Manager to issue
27 functional standards for the ISE). They note that the operating principles of 28 C.F.R. Part 23 are

United States District Court
Northern District of California

1 expressly linked to federal funding of criminal intelligence systems under the Omnibus Act. See
2 42 U.S.C. § 3789g(c); 28 C.F.R. § 23.1; 28 C.F.R. § 23.3; 28 C.F.R. § 23.30; 28 C.F.R. § 23.40.

3 As plaintiffs point out, however, whether or not ISE is appropriately characterized as a
4 criminal intelligence system within the scope of Part 23 may depend on factual issues not
5 appropriately resolved at the motion to dismiss stage. It may be that the question of whether
6 Defendants’ Standards are subject to being set aside as “arbitrary, capricious, an abuse of
7 discretion, otherwise not in accordance with law” will ultimately turn primarily on legal issues.
8 The question is certainly the heart of this case. At this juncture, however, defendants have not
9 shown the declaratory relief claims should be dismissed, as opposed to adjudicated on the merits.

10
11 E. Notice and comment

12 Plaintiffs’ third and fourth claims for relief seek determinations that the DOJ SAR
13 Standard and Functional Standard 1.5, respectively, are invalid because they were adopted without
14 notice and comment. An agency can issue a legislative rule only by using the notice and comment
15 procedure described in the APA, unless it publishes a specific finding of good cause documenting
16 why such procedures “are impracticable, unnecessary, or contrary to the public interest.” 5 U.S.C.
17 § 553(b), (b)(B). In contrast, an agency need not follow the notice and comment procedure to
18 issue an interpretive rule. § 553(b)(A). See *Hemp Indus. Ass’n v. Drug Enforcement Admin.*, 333
19 F.3d 1082, 1087 (9th Cir. 2003). There is no dispute that the Standards were adopted without
20 notice and comment, or a specific finding of good cause that none was appropriate.

21
22 Courts have struggled with identifying the difference between
23 legislative rules and interpretive rules. In general terms, interpretive
24 rules merely explain, but do not add to, the substantive law that
25 already exists in the form of a statute or legislative rule. *Yesler
Terrace Community Council v. Cisneros*, 37 F.3d 442, 449 (9th
26 Cir.1994). Legislative rules, on the other hand, create rights, impose
27 obligations, or effect a change in existing law pursuant to authority
28 delegated by Congress. *Id.*

Hemp Indus., 333 F.3d at 1087.

United States District Court
Northern District of California

1 Plaintiffs contend Defendants’ Standards are “legislative” because no statute sets forth “a
 2 self-executing substantive standard governing the type of information that can be collected,
 3 maintained, or disseminated.” Plaintiffs contend the statutes instead delegate the authority to
 4 promulgate such standards to defendants, and that they have done so in Functional Standard 1.5.
 5 Defendants, in turn, point to the voluntary nature of the system as a whole to argue the standards
 6 are not legislative in nature.

7 This issue also goes to the heart of plaintiffs’ case for declaratory relief. The proper
 8 characterization of Defendants’ Standards as legislative or interpretative likely will involve few
 9 disputed factual issues, and perhaps can be resolved on cross-motions for summary judgment. At
 10 this juncture, however, plaintiffs have sufficiently identified potential grounds for treating the
 11 standards as legislative to avoid dismissal. Whether those arguments will prevail on a more
 12 fulsome record remains to be seen.

13
14 F. Venue

15 Finally, defendants contend that at a minimum, the claims of all plaintiffs other than
 16 Ibrahim should be severed and dismissed because they arose outside this district.⁵ This argument
 17 relies on the same mischaracterization of the claims discussed above. Plaintiffs are not
 18 challenging the circumstances of their individual encounters with authorities *per se*, but the
 19 underlying federal scheme.

20 Parties may be permissively joined where their claims arise “out of the same transaction,
 21 occurrence, or series of transactions or occurrences,” and there is a common “question of law or
 22 fact.” Fed. R. Civ. P. 20(a)(1). This rule “is to be construed liberally in order to promote trial
 23 convenience and to expedite the final determination of disputes, thereby preventing multiple
 24 lawsuits.” *League to Save Lake Tahoe v. Tahoe Reg’l Planning Agency*, 558 F.2d 914, 917 (9th
 25

26 ⁵ It is unclear why defendants believe Conklin’s claims arose outside this district given that in
 27 one of the alleged events underlying those claims he was photographing a refinery in Contra Costa
 28 County.

1 Cir. 1977). Challenges to a governmental policy or system generally satisfy the same transaction
 2 or occurrence requirement. See *United States v. Mississippi*, 380 U.S. 128, 142-43 (1965); see also
 3 *Turner v. LaFond*, No. C 09-00683 MHP, 2009 WL 3400987, at *3 (N.D. Cal Oct. 20, 2009)
 4 (“Typically this requirement will be met where plaintiffs collectively challenge a widely-held
 5 practice or policy.”) Accordingly, the venue objection is not tenable.

6
7 V. CONCLUSION

8
9 The motion to dismiss is denied. The parties shall appear for a further case management
 10 conference on March 12, 2015, with an updated joint case management conference statement to be
 11 filed one week in advance.

12
13 **IT IS SO ORDERED.**

14
15 Dated: February 20, 2015

16 

17 RICHARD SEEBORG
18 United States District Judge

United States District Court
Northern District of California

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

)	
)	No. 3:14-cv-03120-RS
)	
WILEY GILL; JAMES PRIGOFF;TARIQ)	JOINT CASE MANAGEMENT
RAZAK; KHALED IBRAHIM; and AARON)	STATEMENT & [PROPOSED] ORDER
CONKLIN,)	
Plaintiffs,)	
)	
v.)	
)	
DEPARTMENT OF JUSTICE; ERIC H.)	
HOLDER, Jr., in his official capacity as the)	
Attorney General of the United States;)	
PROGRAM MANAGER - INFORMATION)	
SHARING ENVIRONMENT;)	
KSHEMENDRA PAUL, in his official)	
capacity as the Program Manager of the)	
Information Sharing Environment,)	
Defendants.)	

The Parties to the above-entitled action, Plaintiffs Wiley Gill, James Prigoff, Tariq Razak, Khaled Ibrahim, and Aaron Conklin (collectively “Plaintiffs”), by and through their attorneys of record, and Defendants Department of Justice (“DOJ”), Eric. H. Holder, Jr. (“Holder”), Program Manager – Information Sharing Environment (“PM-ISE”), and Kshemendra Paul (“Paul”), jointly submit this JOINT CASE MANAGEMENT STATEMENT &

1 of establishing standing, *see e.g., Chandler v. State Farm Mut. Auto Ins. Co.*, 598 F.3d
2 1115, 1122 (9th Cir. 2010) (recognizing obligation of party asserting jurisdiction to come
3 forward with evidence of standing in response to Rule 12(b)(1) motion to satisfy burden
4 of demonstrating jurisdiction), which they failed to do. And while Plaintiffs claim that
5 they are entitled to discovery on the merits, they seek to invoke exceptions to the well-
6 recognized rule that discovery is not permitted in an APA action. Plaintiffs bear the
7 burden of demonstrating that these narrow exceptions apply, *Bark v. Northrop*, 2 F. Supp.
8 3d 1147, 1152 (D. Or. 2014)(D. Or. 2014), which they have not done. Accordingly, no
9 discovery is appropriate in this APA action. To the extent the Court determines that
10 discovery should be permitted in this action, however, Defendants request that any such
11 discovery be postponed until the Court rules on Defendants' dispositive motion because
12 that motion raises issues relating to this Court's subject-matter jurisdiction.

- b. Plaintiffs contend that this case cannot be resolved on the pleadings and that Defendants' motion to dismiss should be denied.

13 Defendants assert that discovery is inappropriate in this APA action. As a threshold
14 matter, Plaintiffs contend that this is not a question that can be properly litigated and
15 resolved via a case management statement. If Defendants oppose discovery, then the
16 proper course of action is for Defendants to move for a protective order, which is what
17 happened in *Bark v. Northrop*, 2 F. Supp. 3d 1147 (D. Or. 2014). However, because
18 Defendants have raised this issue, Plaintiffs will explain why discovery is appropriate.
19 *Fla. Power & Light Co. v. Lorion*, 470 U.S. 729 (1985), has no bearing on this action. It
20 involved a challenge to a licensing decision of the Nuclear Regulatory Commission, an
21 agency action over which Congress vested initial judicial review in the court of appeals.
22 *Id.* at 746. *McCrary v. Gutierrez*, 495 F. Supp. 2d 1038 (N.D. Cal. 2007), stands for the
23 proposition that judicial review of an agency's decision is generally limited to the
24 "administrative record" that the agency compiles and submits to the Court. *Id.* at 1041.
25 This rule only limits what the Court may consider when reviewing the merits of the
26 agency decision. It does not limit the evidence the Court may consider when deciding
27 other issues, such as whether plaintiffs have standing to sue. *See e.g., Cent. Sierra Envtl.*

1 *Res. Ctr. v. U.S. Forest Serv.*, 916 F. Supp. 2d 1078, 1086 (E.D. Cal. 2013) (“In an action
2 under the APA, the court . . . may consider extra-record evidence that allows plaintiffs to
3 establish standing.”) (citation omitted); *accord Nw. Env'tl. Def. Ctr. v. Bonneville Power*
4 *Admin.*, 117 F.3d 1520, 1527-28 (9th Cir. 1997).² And even when the Court is reviewing
5 the merits of the agency’s decision, *McCrary* itself recognizes that there are exceptions
6 where “[j]udicial review may be expanded and discovery allowed.” *McCrary*, 495 F.
7 *Supp. 2d at 1041*; see also *Common Sense Salmon Recovery v. Evans*, 217 F. Supp. 2d
8 17, 20 (D.D.C. 2002) (administrative record may be supplemented “when discovery
9 provides ‘the only possibility for effective judicial review and when there have been no
10 contemporaneous administrative findings.’”) (citation omitted) (cited in *McCrary*).
11 Furthermore, the APA specifically requires the Court to review the “whole record,” and
12 “[t]he whole record is not just what the agency submitted as the administrative record but
13 also includes ‘all documents and materials directly or indirectly considered by agency
14 decision-makers and includes evidence contrary to the agency’s position.’” *Oregon*
15 *Natural Desert Ass'n v. Cain*, 17 F. Supp. 3d 1037, 1048 (D. Or. 2014) (emphasis in
16 original) (citing *Thompson v. U.S. Dep't of Labor*, 885 F.2d 551, 555 (9th Cir.1989)).
17 Therefore, there are multiple grounds for why discovery is appropriate in the present
18 case.

19 Nevertheless, with respect to Defendants’ request in the alternative for a stay of
20 discovery, Plaintiffs do not oppose a stay of all other discovery pending the Court’s
21 ruling on Defendants’ motion to dismiss, if Defendants produce a modest subset of
22 documents relevant to Plaintiffs’ standing, in particular, all documents in their possession

23 ² Contrary to Defendants’ assertion, Plaintiffs are not required to come forward with “evidence”
24 in response to a 12(b)(1) motion. *Chandler v. State Farm Mut. Auto. Ins.*, 598 F.3d 1115, 1121
25 (9th Cir. 2010), recognizes the well-established rule that “[o]n a motion to dismiss for lack of
26 standing, a district court must accept as true all material allegations in the complaint, and must
27 construe the complaint in the nonmovant’s favor.” See also *Lujan v. Defenders of Wildlife*, 504
28 U.S. 555, 561 (1992) (plaintiff must support standing “with the manner and degree of evidence
required at the successive stages of the litigation” such that “general allegations of injury . . . may
suffice” at the motion to dismiss stage but evidence is required “[i]n response to a summary
judgment motion”).

(including all documents contained in databases operated or maintained by Defendant DOJ's component the FBI) referencing any of the Plaintiffs by January 30, 2014.

Defendants have already indicated that as to some documents, Defendants may not be able to confirm or deny the existence of any such documents. Plaintiffs contend that Defendants must produce documents that are reasonably calculated to lead to the discovery of admissible evidence and that Defendants must explain the basis for any asserted privilege. Plaintiffs are amenable to entering a protective order if necessary.

c. Plaintiffs anticipate seeking discovery in this action, including third-party discovery, that focuses on, among other things, matters:

- (i) how Defendants PM-ISE and Kshemendra Paul implement NSI, including how they train fusion centers, state and local law enforcement, and private entities participating in the NSI and how they describe their standard for suspicious activity reporting;
- (ii) how Defendants DOJ (including its components) and Holder implement the NSI, including how they train fusion centers, state and local law enforcement, and private entities participating in the NSI and how they describe their standard for suspicious activity reporting;
- (iii) the standard for suspicious activity reporting used by Defendant DOJ's component the FBI;
- (iv) how fusion centers, state and local law enforcement, and private entities implement the NSI;
- (v) how fusion centers, state and local law enforcement, and private entities interpret Defendants' suspicious activity reporting standards.
- (vi) the purposes for which SARs are used and the consequences of being the subject of a SAR;
- (vii) the databases used to collect and maintain SARs and the funding that supports any such databases;

1 JOYCE R. BRANDA
 2 Acting Assistant Attorney General
 3 MELINDA L. HAAG
 4 United States Attorney
 5 ANTHONY J. COPPOLINO
 6 Deputy Branch Director
 7 PAUL G. FREEBORNE
 8 Senior Trial Counsel
 9 Va. Bar No. 33024
 10 KIERAN G. GOSTIN
 11 Trial Attorney
 12 D.C. Bar. No. 1019779
 13 Civil Division, Federal Programs Branch
 14 U.S. Department of Justice
 15 P.O. Box 883
 16 Washington, D.C. 20044
 17 Telephone: (202) 353-0543
 18 Facsimile: (202) 616-8460
 19 E-mail: paul.freeborne@usdoj.gov
 20 *Attorneys for the Defendants*

21 **UNITED STATES DISTRICT COURT**
 22 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**

23 WILEY GILL; JAMES PRIGOFF; TARIQ
 24 RAZAK; KHALID IBRAHIM; and AARON
 25 CONKLIN,

26 Plaintiffs,

27 v.

28 DEPARTMENT OF JUSTICE, *et al.*,

Defendants.

No. 3:14-cv-03120 (RS)

**NOTICE OF MOTION AND
 MEMORANDUM OF LAW IN SUPPORT
 OF DEFENDANTS' MOTION TO
 DISMISS**

Hearing Date: January 8, 2015
 Time: 1:30 p.m.
 Ctrm: 3, 17th Floor
 Judge: Hon. Richard G. Seeborg

TABLE OF CONTENTS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

	PAGE
INTRODUCTION	1
BACKGROUND	4
I. STATUTORY AND REGULATORY BACKGROUND.....	4
A. The Information Sharing Environment.....	4
B. The Nationwide Suspicious Activity Reporting Initiative.....	5
C. Functional Standard for Suspicious Activity Reporting Version 1.5	6
D. The eGuardian Privacy Impact Assessment	9
E. 28 C.F.R. Part 23.....	11
II. PLAINTIFFS’ INDIVIDUAL ALLEGATIONS	13
ARGUMENT	16
I. PLAINTIFFS HAVE FAILED TO ALLEGE THE NECESSARY ELEMENTS OF STANDING	17
II. PLAINTIFFS HAVE AN ADEQUATE ALTERNATIVE REMEDY THAT PRECLUDES APA JURISDICTION.....	22
III. PLAINTIFFS’ FAILURE TO ALLEGE A FINAL AGENCY ACTION ALSO PRECLUDES APA JURISDICTION	23
IV. PLAINTIFFS’ APA CLAIMS ARE LEGALLY DEFICIENT.....	25
A. Notice-and-Comment Rulemaking Is Not Required.....	26
B. Defendants are Acting in Accordance with Law	27
V. PLAINTIFFS’ CLAIMS SHOULD BE SEVERED AND ALL BUT IBRAHIM’S CLAIMS DISMISSED FOR LACK OF VENUE	30
A. Plaintiffs Do Not Satisfy the Requirements of Rule 20(a)	30
B. The Claims of Plaintiffs Gill, Prigoff, Razak, and Conklin Should Be Dismissed Pursuant to 28 U.S.C. §1391(e).....	31
CONCLUSION.....	34

Pages ER 588-94 intentionally omitted.

1 enforcement and private security companies as a result of guidance and training provided
2 by Defendants in connection with the NSI. But they have not adequately alleged a
3 sufficient nexus between those alleged injuries and the guidance and training provided by
4 Defendant to satisfy Article III's causation or redressability requirements. Plaintiffs also
5 allege that SARs relating to them have been purportedly uploaded to a federally
6 maintained database and that these SARs are accessible to NSI participants. But
7 assuming that allegation is true, Plaintiffs' alleged injuries as a result of the availability of
8 these SARs (*e.g.*, law enforcement questioning) do not constitute legally cognizable
9 injuries-in-fact, another necessary element of Article III standing. Moreover, because
10 Plaintiffs seek prospective relief against the Federal Defendants, they must allege facts
11 sufficient to establish clearly impending or imminent future harm. Their allegations of
12 future law enforcement scrutiny are too speculative and conjectural to satisfy that
13 requirement.

14 Assuming, *arguendo*, that they can establish their standing to sue, Plaintiffs have
15 no viable legal claim under the APA, for several distinct reasons. As a threshold matter,
16 Plaintiffs fail to establish subject-matter jurisdiction under the APA. *See infra* Argument
17 Part II. The APA can only supply a basis for federal subject-matter jurisdiction where
18 there are no adequate alternative remedies. Here, Plaintiffs assert that they have been
19 injured as a result of actions undertaken by state and local law enforcement agencies and
20 private security companies, and an action against those entities is not only an adequate
21 alternative remedy, it is the more appropriate remedy if any exists.

22 Even if Defendants were the appropriate target of Plaintiffs' APA claims, the
23 guidance provided by Defendants in connection with the NSI does not create the sort of
24 binding, legal obligations that are remediable under the APA. The APA was enacted, in
25 part, to regulate the way in which federal agencies wield the legislative authority
26 delegated to them by Congress. This is reflected in at least two aspects of that statute.
27 First, the APA only grants courts subject-matter jurisdiction over final agency actions
28 that determine legal rights and obligations. Second, the APA only requires notice-and-

Pages ER 597-617 intentionally omitted.

1 *Id.* at 177–88 (citations omitted); *see also Mamigonian v. Biggs*, 710 F.3d 936, 942 (9th
2 Cir. 2013).

3 Plaintiffs cannot satisfy the second condition. Under this prong of the finality
4 test, “[t]he general rule is that administrative orders are not final and reviewable unless
5 and until they impose an obligation, deny a right, or fix some legal relationship as a
6 consummation of the administrative process.” *Ukiah Valley Med. Ctr. v. F.T.C.*, 911
7 F.2d 261, 264 (9th Cir. 1990); *see also Oregon Natural Desert Ass’n v. U.S. Forest Serv.*,
8 465 F.3d 977, 986 (9th Cir. 2006). Relevant factors in determining whether an action is
9 final include “whether the order [or rule] has the status of law or comparable legal force,”
10 “whether immediate compliance with its terms is expected,” and whether the agency
11 action has a “direct and immediate effect on the day-to-day business of the subject party.”
12 *Ukiah*, 911 F.2d at 264 (quotation marks and citations omitted); *see also Oregon Natural*,
13 465 F.3d at 986. Because the Functional Standard and Privacy Impact Assessment only
14 provide functional guidance for the operation of the NSI, and do not create any legal
15 rights or obligations, they do not constitute reviewable actions.

16 On their face, neither the Functional Standard nor the Privacy Impact Assessment
17 requires NSI participants to apply the definition of suspicious activity (*i.e.*, “behavior
18 reasonably indicative of pre-operational planning related to terrorism or other criminal
19 activity”) or the “Criteria Guidance” (*i.e.*, the categories of behavior that may be
20 indicative of pre-operational planning related to terrorism) they provide. The Functional
21 Standard, as explained, is descriptive in nature. It explains the NSI process, standardizes
22 terminology, and discusses the type of incident reports that NSI participants should
23 consider sharing. In fact, it expressly provides that analysts and law enforcement officers
24 should exercise their professional judgment in deciding whether to share information in
25 connection with the NSI. And the Privacy Impact Assessment simply repeats the
26 guidance provided in a prior version the Functional Standard. These documents do not
27 impose any legal obligation on NSI participants to share, or refrain from sharing,
28 information relating to suspicious incidents or behaviors.

Pages ER 619-31 intentionally omitted.

U.S. District Court
California Northern District (San Francisco)
CIVIL DOCKET FOR CASE #: 3:14-cv-03120-RS

Gill et al v. Department of Justice et al
Assigned to: Hon. Richard Seeborg
Referred to: Magistrate Judge Kandis A. Westmore
Case in other court: 17-16107
Cause: 05:702 Administrative Procedure Act

Date Filed: 07/10/2014
Date Terminated: 03/29/2017
Jury Demand: None
Nature of Suit: 899 Other Statutes:
Administrative Procedures Act/Review or
Appeal of Agency Decision
Jurisdiction: U.S. Government Defendant

Plaintiff

Wiley Gill

represented by **Jeffrey Scott Raskin**
Morgan Lewis and Bockius
One Market, Spear Street Tower
San Francisco, CA 94105
415-442-1000
Fax: 415-442-1001
Email: jraskin@morganlewis.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Jonathan Alan Loeb
Blank Rome LLP
2029 Century Park East
6th Floor
Santa Monica, CA 90067
424-239-3422
Fax: 424-239-3443
Email: jloeb@blankrome.com
TERMINATED: 10/27/2015
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Christina Sinha
Asian Americans Advancing Justice - Asian
Law Caucus
55 Columbus Avenue
San Francisco, CA 94111
415-896-1701
Fax: 415-896-1702
Email: christinas@advancingjustice-alc.org
ATTORNEY TO BE NOTICED

Edward A Andrews
Bingham McCutchen LLP
The Water Garden, Suite 2050 North
1601 Cloverfield Boulevard
1620 26th St 4th Fl

Santa Monica, CA 90404-4082
310-907-1000
Fax: (310) 907-2000
ATTORNEY TO BE NOTICED

Hina Shamsi

American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
212-549-2500
Fax: (212) 549-2654
Email: hshamsi@aclu.org
ATTORNEY TO BE NOTICED

Hugh Handeyside

American Civil Liberties Union Foundation
125 Broad Street
New York, NY 10004
212-549-2500
Fax: (212) 549-2654
Email: hhandeyside@aclu.org
ATTORNEY TO BE NOTICED

Jeffrey Rosenfeld

Blank Rome
2029 Century Park East
6th Floor
Los Angeles, CA 90067
424-239-3417
Fax: 424-239-3807
Email: jrosenfeld@blankrome.com
TERMINATED: 10/27/2015
ATTORNEY TO BE NOTICED

John David Loy

ACLU of San Diego
P.O. Box 87131
San Diego, CA 92138-7131
(619) 232-2121 x230
Email: davidloy@aclusandiego.org
ATTORNEY TO BE NOTICED

Julia Harumi Mass, Esq.

ACLU Foundation of Northern California
39 Drumm Street
San Francisco, CA 94111
415-621-2493
Fax: 415-255-8437
Email: jmass@aclunc.org
ATTORNEY TO BE NOTICED

Linda Lye

ACLU Foundation of Northern California
39 Drumm Street

San Francisco, CA 94111
(415) 621-2493
Fax: (415) 255-8437
Email: llye@aclunc.org
ATTORNEY TO BE NOTICED

Michael James Ableson
Morgan, Lewis & Bockius LLP
101 Park Avenue
New York, NY 10178
(212) 309-6113
Fax: (212) 309-6001
Email: michael.ableson@morganlewis.com
ATTORNEY TO BE NOTICED

Mitra Ebadolahi
ACLU Foundation of San Diego and
Imperial Counties
P.O. Box 87131
San Diego, CA 92138
619-232-2121
Fax: 619-232-0036
Email: mebadolahi@aclusandiego.org
ATTORNEY TO BE NOTICED

Nasrina Bargzie
Asian Americans Advancing Justice - Asian
Law Caucus
55 Columbus Ave
San Francisco, CA 94111
925-330-1163
Email: nbargzie@bsflp.com
TERMINATED: 05/26/2016
ATTORNEY TO BE NOTICED

Nicole Robins Sadler
Morgan Lewis Bockius LLP
One Market
Spear Street Tower
San Francisco, CA 94105
415-442-1373
Fax: 415-442-1001
Email: nsadler@morganlewis.com
TERMINATED: 04/27/2016

Peter Bibring
ACLU Foundation of Southern California
1313 West 8th Street
Los Angeles, CA 90017
213-977-9500
Fax: 213-977-5299
Email: pbibring@aclusocal.org
ATTORNEY TO BE NOTICED

Phillip Jared Wiese
Morgan, Lewis and Bockius LLP
One Market, Spear Street Tower
San Francisco, CA 94105
(415) 442-1483
Fax: (415) 442-1001
Email: pwiese@morganlewis.com
ATTORNEY TO BE NOTICED

Stephen Scotch-Marmo
Morgan, Lewis & Bockius LLP
101 Park Avenue
New York, NY 10178
(212) 309-6167
Fax: (212) 309-6001
Email: stephen.scotch-
marmo@morganlewis.com
ATTORNEY TO BE NOTICED

Winifred Virginia Kao
Asian Law Caucus
55 Columbus Avenue
San Francisco, CA 94111
415-896-1701
Fax: 415-896-1702
Email: winifredk@advancingjustice-alc.org
ATTORNEY TO BE NOTICED

Yaman Salahi
Asian American Advancing Justice-Asian
Law Caucus
55 Columbus Avenue
San Francisco, CA 94610
415-848-7711
Fax: (415) 896-1702
Email: yamans@advancingjustice-alc.org
TERMINATED: 01/20/2016

Plaintiff

James Prigoff

represented by **Jeffrey Scott Raskin**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Jonathan Alan Loeb
(See above for address)
TERMINATED: 10/27/2015
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Edward A Andrews
(See above for address)
ATTORNEY TO BE NOTICED

Hina Shamsi

(See above for address)

*ATTORNEY TO BE NOTICED***Hugh Handeyside**

(See above for address)

*ATTORNEY TO BE NOTICED***Jeffrey Rosenfeld**

(See above for address)

*TERMINATED: 10/27/2015**ATTORNEY TO BE NOTICED***John David Loy**

(See above for address)

*ATTORNEY TO BE NOTICED***Julia Harumi Mass , Esq.**

(See above for address)

*ATTORNEY TO BE NOTICED***Linda Lye**

(See above for address)

*ATTORNEY TO BE NOTICED***Michael James Ableson**

(See above for address)

*ATTORNEY TO BE NOTICED***Mitra Ebadolahi**

(See above for address)

*ATTORNEY TO BE NOTICED***Nasrina Bargzie**

(See above for address)

*TERMINATED: 05/26/2016**ATTORNEY TO BE NOTICED***Nicole Robins Sadler**

(See above for address)

*TERMINATED: 04/27/2016***Peter Bibring**

(See above for address)

*ATTORNEY TO BE NOTICED***Phillip Jared Wiese**

(See above for address)

*ATTORNEY TO BE NOTICED***Stephen Scotch-Marmo**

(See above for address)

ATTORNEY TO BE NOTICED

Winifred Virginia Kao
(See above for address)
ATTORNEY TO BE NOTICED

Yaman Salahi
(See above for address)
TERMINATED: 01/20/2016

Plaintiff

Tariq Razak

represented by **Jeffrey Scott Raskin**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Jonathan Alan Loeb
(See above for address)
TERMINATED: 10/27/2015
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Edward A Andrews
(See above for address)
ATTORNEY TO BE NOTICED

Hina Shamsi
(See above for address)
ATTORNEY TO BE NOTICED

Hugh Handeyside
(See above for address)
ATTORNEY TO BE NOTICED

Jeffrey Rosenfeld
(See above for address)
TERMINATED: 10/27/2015
ATTORNEY TO BE NOTICED

John David Loy
(See above for address)
ATTORNEY TO BE NOTICED

Julia Harumi Mass , Esq.
(See above for address)
ATTORNEY TO BE NOTICED

Linda Lye
(See above for address)
ATTORNEY TO BE NOTICED

Michael James Ableson
(See above for address)
ATTORNEY TO BE NOTICED

Mitra Ebadolahi

(See above for address)
ATTORNEY TO BE NOTICED

Nasrina Bargzie
(See above for address)
TERMINATED: 05/26/2016
ATTORNEY TO BE NOTICED

Nicole Robins Sadler
(See above for address)
TERMINATED: 04/27/2016

Peter Bibring
(See above for address)
ATTORNEY TO BE NOTICED

Phillip Jared Wiese
(See above for address)
ATTORNEY TO BE NOTICED

Stephen Scotch-Marmo
(See above for address)
ATTORNEY TO BE NOTICED

Winifred Virginia Kao
(See above for address)
ATTORNEY TO BE NOTICED

Yaman Salahi
(See above for address)
TERMINATED: 01/20/2016

Plaintiff

Khaled Ibrahim

represented by **Jeffrey Scott Raskin**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Jonathan Alan Loeb
(See above for address)
TERMINATED: 10/27/2015
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Edward A Andrews
(See above for address)
ATTORNEY TO BE NOTICED

Hina Shamsi
(See above for address)
ATTORNEY TO BE NOTICED

Hugh Handeyside
(See above for address)

ATTORNEY TO BE NOTICED

Jeffrey Rosenfeld

(See above for address)

TERMINATED: 10/27/2015

ATTORNEY TO BE NOTICED

John David Loy

(See above for address)

ATTORNEY TO BE NOTICED

Julia Harumi Mass , Esq.

(See above for address)

ATTORNEY TO BE NOTICED

Linda Lye

(See above for address)

ATTORNEY TO BE NOTICED

Michael James Ableson

(See above for address)

ATTORNEY TO BE NOTICED

Mitra Ebadolahi

(See above for address)

ATTORNEY TO BE NOTICED

Nasrina Bargzie

(See above for address)

TERMINATED: 05/26/2016

ATTORNEY TO BE NOTICED

Nicole Robins Sadler

(See above for address)

TERMINATED: 04/27/2016

Peter Bibring

(See above for address)

ATTORNEY TO BE NOTICED

Phillip Jared Wiese

(See above for address)

ATTORNEY TO BE NOTICED

Stephen Scotch-Marmo

(See above for address)

ATTORNEY TO BE NOTICED

Winifred Virginia Kao

(See above for address)

ATTORNEY TO BE NOTICED

Yaman Salahi

(See above for address)

TERMINATED: 01/20/2016

Plaintiff

Aaron Conklin

represented by **Jeffrey Scott Raskin**

(See above for address)

LEAD ATTORNEY

ATTORNEY TO BE NOTICED

Jonathan Alan Loeb

(See above for address)

TERMINATED: 10/27/2015

LEAD ATTORNEY

ATTORNEY TO BE NOTICED

Edward A Andrews

(See above for address)

ATTORNEY TO BE NOTICED

Hina Shamsi

(See above for address)

ATTORNEY TO BE NOTICED

Hugh Handeyside

(See above for address)

ATTORNEY TO BE NOTICED

Jeffrey Rosenfeld

(See above for address)

TERMINATED: 10/27/2015

ATTORNEY TO BE NOTICED

John David Loy

(See above for address)

ATTORNEY TO BE NOTICED

Julia Harumi Mass , Esq.

(See above for address)

ATTORNEY TO BE NOTICED

Linda Lye

(See above for address)

ATTORNEY TO BE NOTICED

Michael James Ableson

(See above for address)

ATTORNEY TO BE NOTICED

Mitra Ebadolahi

(See above for address)

ATTORNEY TO BE NOTICED

Nasrina Bargzie

(See above for address)

TERMINATED: 05/26/2016

ATTORNEY TO BE NOTICED

Nicole Robins Sadler

(See above for address)

TERMINATED: 04/27/2016

Peter Bibring

(See above for address)

ATTORNEY TO BE NOTICED

Phillip Jared Wiese

(See above for address)

ATTORNEY TO BE NOTICED

Stephen Scotch-Marmo

(See above for address)

ATTORNEY TO BE NOTICED

Winifred Virginia Kao

(See above for address)

ATTORNEY TO BE NOTICED

Yaman Salahi

(See above for address)

TERMINATED: 01/20/2016

V.

Defendant

Department of Justice

represented by **Paul Gerald Freeborne**
U.S. Department of Justice
Civil Division
20 Massachusetts Avenue
N.W., Room 6108
Washington, DC 20001
(202) 353-0543
Fax: (202) 616-8460
Email: paul.freeborne@usdoj.gov
TERMINATED: 03/07/2016
LEAD ATTORNEY

Steven Andrew Myers

United States Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave. NW
Washington, DC 20530
(202) 305-8648
Fax: (202) 616-8460
Email: steven.a.myers@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kieran Gavin Gostin
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, N.W.
Washington, DC 20037
202-353-4556
Fax: 202-616-8460
Email: kieran.g.gostin@usdoj.gov
TERMINATED: 08/25/2016
ATTORNEY TO BE NOTICED

Defendant

Eric H. Holder, Jr.
*in his official capacity as Attorney General
of the United States*
TERMINATED: 09/08/2015

represented by **Paul Gerald Freeborne**
(See above for address)
TERMINATED: 03/07/2016
LEAD ATTORNEY

Steven Andrew Myers
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kieran Gavin Gostin
(See above for address)
TERMINATED: 08/25/2016
ATTORNEY TO BE NOTICED

Defendant

**Program Manager - Information Sharing
Environment**

represented by **Paul Gerald Freeborne**
(See above for address)
TERMINATED: 03/07/2016
LEAD ATTORNEY

Steven Andrew Myers
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kieran Gavin Gostin
(See above for address)
TERMINATED: 08/25/2016
ATTORNEY TO BE NOTICED

Defendant

Kshemendra Paul
*in his official capacity as Program Manager
of the Information Sharing Environment*

represented by **Paul Gerald Freeborne**
(See above for address)
TERMINATED: 03/07/2016
LEAD ATTORNEY

Steven Andrew Myers
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kieran Gavin Gostin
 (See above for address)
TERMINATED: 08/25/2016
ATTORNEY TO BE NOTICED

Defendant**Attorney General Loretta Lynch**

represented by **Paul Gerald Freeborne**
 (See above for address)
TERMINATED: 03/07/2016
LEAD ATTORNEY

Steven Andrew Myers
 (See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kieran Gavin Gostin
 U.S. Department of Justice
 Civil Division, Federal Programs Branch
 20 Massachusetts Avenue, N.W.
 Washington, DC 20037
 (202) 353-4556
 Fax: (202) 616-8460
 Email: kieran.g.gostin@usdoj.gov
TERMINATED: 08/25/2016
ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
07/10/2014	1	COMPLAINT for Declaratory and Injunctive Relief against Department of Justice, Eric H. Holder, Jr, Kshemendra Paul, Program Manager - Information Sharing Environment (Filing fee \$ 400.00, receipt number 0971-8757477.). Filed by James Prigoff, Wiley Gill, Khaled Ibrahim, Aaron Conklin. (Attachments: # 1 Civil Cover Sheet)(Loeb, Jonathan) (Filed on 7/10/2014) Modified on 7/10/2014 (gbaS, COURT STAFF). (Entered: 07/10/2014)
07/10/2014	2	Proposed Summons. (Loeb, Jonathan) (Filed on 7/10/2014) (Entered: 07/10/2014)
07/10/2014	3	CONSENT/DECLINATION to Proceed Before a US Magistrate Judge by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak.. (Loeb, Jonathan) (Filed on 7/10/2014) (Entered: 07/10/2014)
07/10/2014	4	Case assigned to Hon. Richard Seeborg. Counsel for plaintiff or the removing party is responsible for serving the Complaint or Notice of Removal, Summons and the assigned judge's standing orders and all other new case documents upon the opposing parties. For information, visit <i>E-Filing A New Civil Case</i> at http://cand.uscourts.gov/ecf/caseopening . Standing orders can be downloaded from the court's web page at www.cand.uscourts.gov/judges . Upon receipt, the summons will be issued and returned electronically. Counsel is required to send chambers a copy of the initiating documents pursuant to L.R. 5-1(e)(7). A scheduling order will be sent by Notice of Electronic Filing

		(NEF) within two business days. (svS, COURT STAFF) (Filed on 7/10/2014) (Entered: 07/10/2014)
07/10/2014	5	Initial Case Management Scheduling Order with ADR Deadlines: Case Management Statement due by 10/2/2014. Case Management Conference set for 10/9/2014 10:00 AM in Courtroom 3, 17th Floor, San Francisco. (Attachments: # 1 Standing Order) (gbaS, COURT STAFF) (Filed on 7/10/2014) (Entered: 07/10/2014)
07/10/2014	6	Summons Issued as to Department of Justice, Eric H. Holder, Jr, Kshemendra Paul, Program Manager - Information Sharing Environment. (gbaS, COURT STAFF) (Filed on 7/10/2014) (Entered: 07/10/2014)
07/11/2014	7	MOTION for leave to appear in Pro Hac Vice <i>Hugh Handeyside</i> (Filing fee \$ 305, receipt number 0971-8760932.) filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Attachments: # 1 Certificate of Good Standing)(Lye, Linda) (Filed on 7/11/2014) (Entered: 07/11/2014)
07/11/2014	8	MOTION for leave to appear in Pro Hac Vice <i>Hina Shamsi</i> (Filing fee \$ 305, receipt number 0971-8761004.) filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Attachments: # 1 Certificate of Good Standing)(Lye, Linda) (Filed on 7/11/2014) (Entered: 07/11/2014)
07/11/2014	9	ORDER GRANTING APPLICATION FOR ADMISSION OF ATTORNEY HUGH HANDEYSIDE PRO HAC VICE. by Judge Richard Seeborg (cl, COURT STAFF) (Filed on 7/11/2014) (Entered: 07/11/2014)
07/11/2014	10	ORDER GRANTING APPLICATION FOR ADMISSION OF ATTORNEY HINA SHAMSI PRO HAC VICE. by Judge Richard Seeborg (cl, COURT STAFF) (Filed on 7/11/2014) (Entered: 07/11/2014)
07/14/2014	11	MOTION for leave to appear in Pro Hac Vice <i>by Stephen Scotch-Marmo</i> (Filing fee \$ 305, receipt number 0971-8764691.) filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Scotch-Marmo, Stephen) (Filed on 7/14/2014) (Entered: 07/14/2014)
07/14/2014	12	ORDER GRANTING APPLICATION FOR ADMISSION OF ATTORNEY STEPHEN SCOTCH-MARMO PRO HAC VICE. by Judge Richard Seeborg (cl, COURT STAFF) (Filed on 7/14/2014) (Entered: 07/14/2014)
07/16/2014	13	MOTION for leave to appear in Pro Hac Vice <i>of Attorney Michael Ableson</i> (Filing fee \$ 305, receipt number 25GMJS9U.) Filing fee previously paid on 07/16/2014 filed by Wiley Gill. (Ableson, Michael) (Filed on 7/16/2014) (Entered: 07/16/2014)
07/16/2014	14	ORDER GRANTING APPLICATION FOR ADMISSION OF ATTORNEY MICHAEL ABLESON PRO HAC VICE. by Judge Richard Seeborg (cl, COURT STAFF) (Filed on 7/16/2014) (Entered: 07/16/2014)
07/22/2014	15	NOTICE of Appearance by Paul Gerald Freeborne <i>on Behalf of the Federal Defendants</i> (Freeborne, Paul) (Filed on 7/22/2014) (Entered: 07/22/2014)
08/06/2014	16	NOTICE of Appearance by Kieran Gavin Gostin (Gostin, Kieran) (Filed on 8/6/2014) (Entered: 08/06/2014)
08/21/2014	17	STIPULATION WITH PROPOSED ORDER filed by Department of Justice, Eric H. Holder, Jr, Kshemendra Paul, Program Manager - Information Sharing Environment. (Attachments: # 1 Proposed Order)(Gostin, Kieran) (Filed on 8/21/2014) (Entered: 08/21/2014)
08/28/2014	18	CLERK'S NOTICE CONTINUING CASE MANAGEMENT CONFERENCE. Case

		Management Statement due by 1/2/2015. Case Management Conference previously set for 10/9/14 has been CONTINUED TO 1/8/2015 10:00 AM in Courtroom 3, 17th Floor, San Francisco. This is a text only entry. There is no document associated with this notice. (cl, COURT STAFF) (Filed on 8/28/2014) (Entered: 08/28/2014)
10/14/2014	19	MOTION for Leave to File Excess Pages filed by Department of Justice, Eric H. Holder, Jr, Kshemendra Paul, Program Manager - Information Sharing Environment. (Attachments: # 1 Proposed Order)(Gostin, Kieran) (Filed on 10/14/2014) (Entered: 10/14/2014)
10/16/2014	20	ORDER by Judge Richard Seeborg granting 19 Motion for Leave to File Excess Pages. (cl, COURT STAFF) (Filed on 10/16/2014) (Entered: 10/16/2014)
10/16/2014	21	MOTION to Dismiss filed by Department of Justice, Eric H. Holder, Jr, Kshemendra Paul, Program Manager - Information Sharing Environment. Motion Hearing set for 1/8/2014 01:30 PM in Courtroom 3, 17th Floor, San Francisco before Hon. Richard Seeborg. Responses due by 11/20/2014. Replies due by 12/11/2014. (Attachments: # 1 Proposed Order)(Gostin, Kieran) (Filed on 10/16/2014) (Entered: 10/16/2014)
10/24/2014	22	NOTICE of Appearance by John David Loy (Loy, John) (Filed on 10/24/2014) (Entered: 10/24/2014)
11/06/2014		Reset Hearing re 21 MOTION to Dismiss Motion Hearing set for 1/8/2015 01:30 PM in Courtroom 3, 17th Floor, San Francisco before Hon. Richard Seeborg. (cl, COURT STAFF) (Filed on 11/6/2014) (Entered: 11/06/2014)
11/06/2014	23	CLERK'S NOTICE RESETTING THE TIME ON CASE MANAGEMENT CONFERENCE. Case Management Conference RESET TO 01:30 PM on January 8, 2015 in Courtroom 3, 17th Floor, San Francisco. This is a text only entry. There is no document associated with this notice. (cl, COURT STAFF) (Filed on 11/6/2014) (Entered: 11/06/2014)
11/13/2014	24	STIPULATION WITH PROPOSED ORDER <i>re page limits</i> filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Lye, Linda) (Filed on 11/13/2014) (Entered: 11/13/2014)
11/14/2014	25	STIPULATION AND ORDER REGARDING PAGE LIMITS. Signed by Judge Richard Seeborg on 11/14/14. (cl, COURT STAFF) (Filed on 11/14/2014) (Entered: 11/14/2014)
11/20/2014	26	RESPONSE (re 21 MOTION to Dismiss) filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Lye, Linda) (Filed on 11/20/2014) (Entered: 11/20/2014)
12/08/2014	27	SUMMONS Returned Executed by Tariq Razak, James Prigoff, Wiley Gill, Khaled Ibrahim, Aaron Conklin. All Defendants. (Lye, Linda) (Filed on 12/8/2014) (Entered: 12/08/2014)
12/11/2014	28	REPLY (re 21 MOTION to Dismiss) filed by Department of Justice, Eric H. Holder, Jr, Kshemendra Paul, Program Manager - Information Sharing Environment. (Gostin, Kieran) (Filed on 12/11/2014) (Entered: 12/11/2014)
12/18/2014	29	ADR Certification (ADR L.R. 3-5 b) of discussion of ADR options <i>Filed by Defendants</i> (Freeborne, Paul) (Filed on 12/18/2014) (Entered: 12/18/2014)
12/18/2014	30	Certificate of Interested Entities by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak (Lye, Linda) (Filed on 12/18/2014) (Entered: 12/18/2014)
12/18/2014	31	ADR Certification (ADR L.R. 3-5 b) of discussion of ADR options <i>by Plaintiffs</i> (Lye,

		Linda) (Filed on 12/18/2014) (Entered: 12/18/2014)
12/18/2014	32	NOTICE of need for ADR Phone Conference (ADR L.R. 3-5 d) (Lye, Linda) (Filed on 12/18/2014) (Entered: 12/18/2014)
12/22/2014	33	NOTICE of Change In Counsel by Michael James Ableson <i>and Stephen Scotch-Marmo</i> (Ableson, Michael) (Filed on 12/22/2014) (Entered: 12/22/2014)
12/22/2014	34	ADR Clerk's Notice Setting ADR Phone Conference on January 6, 2015 at 2:30 PM Pacific time. Please note that you must be logged into an ECF account of counsel of record in order to view this document. (cmf, COURT STAFF) (Filed on 12/22/2014) (Entered: 12/22/2014)
12/31/2014	35	NOTICE of Appearance by Jeffrey Scott Raskin <i>Notice of Appearance of Jeffrey S. Raskin and Nicole R. Sadler</i> (Raskin, Jeffrey) (Filed on 12/31/2014) (Entered: 12/31/2014)
12/31/2014	36	CASE MANAGEMENT STATEMENT (<i>JOINT</i>) filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Lye, Linda) (Filed on 12/31/2014) (Entered: 12/31/2014)
01/06/2015		ADR Remark: ADR Phone Conference held 1/6/2015 with Daniel Bowling, ADR Program Staff Attorney. (cmf, COURT STAFF) (Filed on 1/6/2015) (Entered: 01/06/2015)
01/08/2015	37	Minute Entry for proceedings held before Hon. Richard Seeborg: Further Case Management Conference held on 1/8/2015. Motion Hearing held on 1/8/2015 re 21 MOTION to Dismiss Court Reporter Name: James Pence. (cl, COURT STAFF) (Date Filed: 1/8/2015) (Entered: 01/08/2015)
02/20/2015	38	ORDER by Judge Richard Seeborg denying 21 Motion to Dismiss. (cl, COURT STAFF) (Filed on 2/20/2015) (Entered: 02/20/2015)
02/26/2015	39	STIPULATION filed by Department of Justice, Eric H. Holder, Jr, Kshemendra Paul, Program Manager - Information Sharing Environment. (Gostin, Kieran) (Filed on 2/26/2015) (Entered: 02/26/2015)
03/05/2015	40	CASE MANAGEMENT STATEMENT (<i>JOINT</i>) filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Scotch-Marmo, Stephen) (Filed on 3/5/2015) (Entered: 03/05/2015)
03/12/2015	41	Minute Entry for proceedings held before Hon. Richard Seeborg: Further Case Management Conference held on 3/12/2015. Further Case Management Conference set for 7/9/2015 10:00 AM in Courtroom 3, 17th Floor, San Francisco.Court Reporter: Not Reported. (cl, COURT STAFF) (Date Filed: 3/12/2015) (Entered: 03/12/2015)
03/20/2015	42	STIPULATION <i>To Extend Time For Defendants to Answer Plaintiffs' Complaint</i> filed by Department of Justice, Eric H. Holder, Jr, Program Manager - Information Sharing Environment. (Freeborne, Paul) (Filed on 3/20/2015) (Entered: 03/20/2015)
04/01/2015	43	Consent Administrative Motion to File Under Seal <i>Defendants' Answer</i> filed by Department of Justice, Eric H. Holder, Jr, Kshemendra Paul, Program Manager - Information Sharing Environment. (Attachments: # 1 Declaration, # 2 Proposed Order) (Freeborne, Paul) (Filed on 4/1/2015) (Entered: 04/01/2015)
04/01/2015	44	ORDER by Judge Richard Seeborg granting 43 Administrative Motion to File Under Seal. (cl, COURT STAFF) (Filed on 4/1/2015) (Entered: 04/01/2015)
04/03/2015	45	DOCUMENT E-FILED UNDER SEAL re 44 Order on Administrative Motion to File

		Under Seal <i>Defendants' Answer to Complaint</i> by Department of Justice, Eric H. Holder, Jr, Kshemendra Paul, Program Manager - Information Sharing Environment. (Freeborne, Paul) (Filed on 4/3/2015) (Entered: 04/03/2015)
04/24/2015	46	STIPULATION <i>re: Filing of Unredacted Answer</i> filed by Department of Justice, Eric H. Holder, Jr, Kshemendra Paul, Program Manager - Information Sharing Environment. (Attachments: # 1 Answer)(Gostin, Kieran) (Filed on 4/24/2015) (Entered: 04/24/2015)
05/05/2015	47	NOTICE of Change of Address by Nicole Robins Sadler (Sadler, Nicole) (Filed on 5/5/2015) (Entered: 05/05/2015)
06/04/2015	48	STIPULATION WITH PROPOSED ORDER <i>Setting Hearing Date and Briefing Schedule for Plaintiffs Special Motion to Establish Right to Discovery on the Department of Justices Standard for Suspicious Activity Reporting and Submission of Administrative Record Regarding Functional Standard</i> filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Sadler, Nicole) (Filed on 6/4/2015) (Entered: 06/04/2015)
06/04/2015	49	ORDER by Judge Richard Seeborg granting [#48] Stipulation Setting Hearing Date and Briefing Schedule for Plaintiffs Special Motion to Establish Right to Discovery on the Department of Justices Standard for Suspicious Activity Reporting and Submission of Administrative Record Regarding Functional Standard. (cl, COURT STAFF) (Filed on 6/4/2015) (Entered: 06/04/2015)
06/04/2015	50	MOTION for Discovery <i>Notice of Motion and Memorandum of Law In Support of Plaintiffs Special Motion to Establish Right to Discovery on the Department of Justices Standard for Suspicious Activity Reporting</i> filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. Motion Hearing set for 8/20/2015 01:30 PM in Courtroom 3, 17th Floor, San Francisco before Hon. Richard Seeborg. Responses due by 7/10/2015. Replies due by 7/30/2015. (Attachments: # 1 Proposed Order)(Sadler, Nicole) (Filed on 6/4/2015) (Entered: 06/04/2015)
06/04/2015	51	Declaration of Hugh Handeyside in Support of 50 MOTION for Discovery <i>Notice of Motion and Memorandum of Law In Support of Plaintiffs Special Motion to Establish Right to Discovery on the Department of Justices Standard for Suspicious Activity Reporting</i> filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Exhibit C, # 4 Exhibit D, # 5 Exhibit E, # 6 Exhibit F, # 7 Exhibit G, # 8 Exhibit H, # 9 Exhibit I, # 10 Exhibit J, # 11 Exhibit K, # 12 Exhibit L, # 13 Exhibit M, # 14 Exhibit N, # 15 Exhibit O, # 16 Exhibit P, # 17 Exhibit Q)(Related document(s) 50) (Sadler, Nicole) (Filed on 6/4/2015) (Entered: 06/04/2015)
06/16/2015	52	NOTICE by Department of Justice, Eric H. Holder, Jr, Kshemendra Paul, Program Manager - Information Sharing Environment re 49 Order on Stipulation, 41 Case Management Conference - Further,, Set Hearings, <i>of Filing of Administrative Record</i> (Attachments: # 1 Certification of Administrative Record, # 2 Exhibit A - Index of Administrative Record)(Freeborne, Paul) (Filed on 6/16/2015) (Entered: 06/16/2015)
06/17/2015	53	ADMINISTRATIVE RECORD by Department of Justice, Eric H. Holder, Jr, Kshemendra Paul, Program Manager - Information Sharing Environment. Amendment to 52 Notice (Other), <i>Supplement to Notice of Filing of Administrative Record-Administrative Record</i> . (Attachments: # 1 Supplement AR-Part 2, # 2 Supplement AR-Part 3, # 3 Supplement AR-Part 4, # 4 Supplement AR-Part 5, # 5 Supplement AR-Part 6, # 6 Supplement AR-Part 7, # 7 Supplement AR-Part 8, # 8 Supplement AR-Part 9, # 9 Supplement AR-Part 10, # 10 Supplement AR-Part 11, # 11 Supplement AR-Part 12, # 12 Supplement AR-Part 13, # 13 Supplement AR-Part 14, # 14 Supplement AR-Part 15, # 15 Supplement AR-Part 16, # 16 Supplement AR-Part 17, # 17 Supplement AR-Part

		18)(Freeborne, Paul) (Filed on 6/17/2015) Modified on 6/17/2015 (gbaS, COURT STAFF). (Entered: 06/17/2015)
06/30/2015	54	STIPULATION WITH PROPOSED ORDER re 41 Case Management Conference - Further,, Set Hearings, filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Lye, Linda) (Filed on 6/30/2015) (Entered: 06/30/2015)
06/30/2015	55	CLERK'S NOTICE The Case Management Conference previously set for 7/9/2015 is continued to 8/20/2015 at 1:30 PM in Courtroom 3, 17th Floor, San Francisco. This is a text only entry. There is no document associated with this notice.(rslc2, COURT STAFF) (Filed on 6/30/2015) (Entered: 06/30/2015)
07/10/2015	56	RESPONSE (re 50 MOTION for Discovery <i>Notice of Motion and Memorandum of Law In Support of Plaintiffs Special Motion to Establish Right to Discovery on the Department of Justices Standard for Suspicious Activity Reporting</i>) filed by Department of Justice, Eric H. Holder, Jr, Kshemendra Paul, Program Manager - Information Sharing Environment. (Gostin, Kieran) (Filed on 7/10/2015) (Entered: 07/10/2015)
07/29/2015	57	NOTICE of Appearance by Nicole Robins Sadler (Sadler, Nicole) (Filed on 7/29/2015) (Entered: 07/29/2015)
07/30/2015	58	REPLY (re 50 MOTION for Discovery <i>Notice of Motion and Memorandum of Law In Support of Plaintiffs Special Motion to Establish Right to Discovery on the Department of Justices Standard for Suspicious Activity Reporting</i>) <i>Reply in Support of Plaintiffs Special Motion to Establish Right to Discovery on the Department of Justices Standard for Suspicious Activity Reporting</i> filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Sadler, Nicole) (Filed on 7/30/2015) (Entered: 07/30/2015)
08/12/2015	59	JOINT CASE MANAGEMENT STATEMENT & <i>Proposed Order</i> filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Sadler, Nicole) (Filed on 8/12/2015) (Entered: 08/12/2015)
08/14/2015	60	ORDER by Judge Richard Seeborg denying 50 Motion for Discovery. (cl, COURT STAFF) (Filed on 8/14/2015) (Entered: 08/14/2015)
08/17/2015		Reset Hearing: Further Case Management Conference previously set for 8/20/2015 Continued to 8/27/2015 at 10:00 AM in Courtroom 3, 17th Floor, San Francisco. (cl, COURT STAFF) (Filed on 8/17/2015) (Entered: 08/17/2015)
08/21/2015	61	JOINT CASE MANAGEMENT STATEMENT <i>Supplemental Joint Case Management Statement</i> filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Lye, Linda) (Filed on 8/21/2015) (Entered: 08/21/2015)
08/25/2015	62	ORDER CONTINUING CASE MANAGEMENT CONFERENCE AND DIRECTING SUPPLEMENTAL FILING. Further Case Management Conference previously set for 8/27/2015 Continued to 9/3/2015 at 10:00 AM in Courtroom 3, 17th Floor, San Francisco. Signed by Judge Richard Seeborg on 8/25/15. (cl, COURT STAFF) (Filed on 8/25/2015) (Entered: 08/25/2015)
08/26/2015	63	STIPULATION WITH PROPOSED ORDER re 62 Order,, Set Hearings, <i>Regarding Continuation of Initial Case Management Conference</i> filed by Department of Justice, Eric H. Holder, Jr, Kshemendra Paul, Program Manager - Information Sharing Environment. (Attachments: # 1 Proposed Order)(Freeborne, Paul) (Filed on 8/26/2015) (Entered: 08/26/2015)
08/26/2015	64	STIPULATION AND ORDER RE 63 CONTINUING FURTHER CASE MANAGEMENT CONFERENCE. Further Case Management Conference previously set for 9/3/2015 Continued to 9/10/2015 at 10:00 AM in Courtroom 3,

		17th Floor, San Francisco. Signed by Judge Richard Seeborg on 8/26/15. (cl, COURT STAFF) (Filed on 8/26/2015) (Entered: 08/26/2015)
08/28/2015	65	Statement <i>re Notice re Pltfs' Mot for Leave to File Suppl Complaint</i> by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Lye, Linda) (Filed on 8/28/2015) (Entered: 08/28/2015)
09/01/2015	66	MOTION for Leave to File <i>Notice of Motion and Motion for Leave to File Supplemental Complaint; and Memorandum of Points and Authorities in Support</i> filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Lye, Linda) (Filed on 9/1/2015) (Entered: 09/01/2015)
09/01/2015	67	Declaration of Linda Lye in Support of 66 MOTION for Leave to File <i>Notice of Motion and Motion for Leave to File Supplemental Complaint; and Memorandum of Points and Authorities in Support</i> filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Attachments: # 1 Exhibit Exhibit 1, # 2 Exhibit Exhibit 2 Pages 1 to 16, # 3 Exhibit Exhibit 2 Pages 17 to 33, # 4 Exhibit Exhhibit 2 Pages 34 to 50, # 5 Exhibit Exhibit 2 Pages 51 to 58, # 6 Exhibit Exhibit 2 Pages 59 to 65, # 7 Exhibit Exhibit 2 Pages 66 to 131, # 8 Exhibit Exhibit 2 Pages 132 to 194)(Related document(s) 66) (Lye, Linda) (Filed on 9/1/2015) (Entered: 09/01/2015)
09/01/2015	68	Proposed Order re 66 MOTION for Leave to File <i>Notice of Motion and Motion for Leave to File Supplemental Complaint; and Memorandum of Points and Authorities in Support</i> , 67 Declaration in Support,, [<i>Proposed</i>] <i>Order Granting Plaintiffs' Motion for Leave to File Supplemental Complaint</i> by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Lye, Linda) (Filed on 9/1/2015) (Entered: 09/01/2015)
09/02/2015	69	ORDER by Judge Richard Seeborg granting 66 Motion for Leave to File. (cl, COURT STAFF) (Filed on 9/2/2015) (Entered: 09/02/2015)
09/03/2015	70	FIRST AMENDED COMPLAINT for Declaratory and Injunctive Relief against All Defendants. Filed by Tariq Razak, James Prigoff, Wiley Gill, Khaled Ibrahim, Aaron Conklin. (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Exhibit C, # 4 Exhibit D Part 1a, # 5 Exhibit D Part 1b, # 6 Exhibit D Part 2, # 7 Exhibit E, # 8 Exhibit F, # 9 Exhibit G, # 10 Exhibit H, # 11 Exhibit I, # 12 Exhibit J, # 13 Exhibit K)(Lye, Linda) (Filed on 9/3/2015) Modified on 9/4/2015 (gbaS, COURT STAFF). (Entered: 09/03/2015)
09/04/2015	71	JOINT CASE MANAGEMENT STATEMENT <i>Further Supplemental Joint Case Management Statement</i> filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Lye, Linda) (Filed on 9/4/2015) (Entered: 09/04/2015)
09/08/2015	72	ORDER REFERRING ISSUES TO MAGISTRATE JUDGE AND CONTINUING FURTHER CASE MANAGEMENT CONFERENCE. Order Referring Case to Magistrate Judge. Further Case Management Conference set for 11/19/2015 at 10:00 AM in Courtroom 3, 17th Floor, San Francisco. Signed by Judge Richard Seeborg on 9/8/15. (cl, COURT STAFF) (Filed on 9/8/2015) (Entered: 09/08/2015)
09/08/2015		CASE REFERRED to Magistrate Judge Kandis A. Westmore for Discovery (ahm, COURT STAFF) (Filed on 9/8/2015) (Entered: 09/08/2015)
10/01/2015	73	MOTION Complete the Administrative Record <i>Plaintiffs Notice of Motion and Motion to Complete the Administrative Record; Memorandum of Points and Authorities in Support Thereof</i> filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. Motion Hearing set for 11/5/2015 11:00 AM before Magistrate Judge Kandis A. Westmore. Responses due by 10/15/2015. Replies due by 10/22/2015. (Sadler, Nicole) (Filed on 10/1/2015) (Entered: 10/01/2015)
10/01/2015	74	Statement re 73 MOTION Complete the Administrative Record <i>Plaintiffs Notice of</i>

		<i>Motion and Motion to Complete the Administrative Record; Memorandum of Points and Authorities in Support Thereof Plaintiffs Statement re: Filing of Noticed Motion to Complete the Administrative Record</i> by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Sadler, Nicole) (Filed on 10/1/2015) (Entered: 10/01/2015)
10/01/2015	75	Declaration of Linda Lye in Support of 73 MOTION Complete the Administrative Record <i>Plaintiffs Notice of Motion and Motion to Complete the Administrative Record; Memorandum of Points and Authorities in Support Thereof</i> filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Attachments: # 1 Exhibit 1, # 2 Exhibit 2, # 3 Exhibit 3, # 4 Exhibit 4, # 5 Exhibit 5, # 6 Exhibit 6, # 7 Exhibit 7, # 8 Exhibit 8, # 9 Exhibit 9)(Related document(s) 73) (Sadler, Nicole) (Filed on 10/1/2015) (Entered: 10/01/2015)
10/01/2015	76	Proposed Order re 73 MOTION Complete the Administrative Record <i>Plaintiffs Notice of Motion and Motion to Complete the Administrative Record; Memorandum of Points and Authorities in Support Thereof [Proposed] Order Granting Plaintiffs Motion to Complete the Administrative Record</i> by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Sadler, Nicole) (Filed on 10/1/2015) (Entered: 10/01/2015)
10/08/2015	77	STIPULATION WITH PROPOSED ORDER filed by Department of Justice, Eric H. Holder, Jr, Loretta Lynch, Kshemendra Paul, Program Manager - Information Sharing Environment. (Attachments: # 1 Proposed Order)(Gostin, Kieran) (Filed on 10/8/2015) (Entered: 10/08/2015)
10/09/2015	78	ORDER GRANTING 77 STIPULATION WITH PROPOSED ORDER (AS MODIFIED BY THE COURT); CONTINUING HEARING ON 73 MOTION TO COMPLETE THE ADMINISTRATIVE RECORD TO DECEMBER 3, 2015 AT 11:00 AM. Signed by Judge Kandis A. Westmore on 10/09/2015. (kawlc2S, COURT STAFF) (Filed on 10/9/2015) (Entered: 10/09/2015)
10/22/2015	79	RESPONSE (re 73 MOTION Complete the Administrative Record <i>Plaintiffs Notice of Motion and Motion to Complete the Administrative Record; Memorandum of Points and Authorities in Support Thereof</i>) filed by Department of Justice, Eric H. Holder, Jr, Loretta Lynch, Kshemendra Paul, Program Manager - Information Sharing Environment. (Attachments: # 1 Exhibit 1, # 2 Exhibit 2)(Gostin, Kieran) (Filed on 10/22/2015) (Entered: 10/22/2015)
10/27/2015	80	NOTICE by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak of <i>Withdrawal of Counsel</i> (Attachments: # 1 Proposed Order)(Scotch-Marmo, Stephen) (Filed on 10/27/2015) (Entered: 10/27/2015)
10/28/2015	81	ORDER withdrawing counsel. Signed by Judge Richard Seeborg on 10/28/15. (cl, COURT STAFF) (Filed on 10/28/2015) (Entered: 10/28/2015)
11/05/2015	82	REPLY (re 73 MOTION Complete the Administrative Record <i>Plaintiffs Notice of Motion and Motion to Complete the Administrative Record; Memorandum of Points and Authorities in Support Thereof</i>) filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff. (Sadler, Nicole) (Filed on 11/5/2015) (Entered: 11/05/2015)
11/09/2015	83	STIPULATION WITH PROPOSED ORDER re 72 Order,, Order Referring Case to Magistrate Judge,, Set Hearings, <i>Regarding Continuation of November 19, 2015 Case Management Conference</i> filed by Department of Justice, Eric H. Holder, Jr, Loretta Lynch, Kshemendra Paul, Program Manager - Information Sharing Environment. (Attachments: # 1 Proposed Order)(Freeborne, Paul) (Filed on 11/9/2015) (Entered: 11/09/2015)
11/09/2015	84	CLERK'S NOTICE CONTINUING FURTHER CASE MANAGEMENT CONFERENCE. Case Management Statement due by 1/21/2016. Further Case Management Conference

		previously set for 11/19/2015 Continued to 1/28/2016 at 10:00 AM in Courtroom 3, 17th Floor, San Francisco. <i>(This is a text-only entry generated by the court. There is no document associated with this entry.)</i> (cl, COURT STAFF) (Filed on 11/9/2015) (Entered: 11/09/2015)
12/02/2015	85	CLERK'S NOTICE Continuing Motion Hearing as to 73 MOTION Complete the Administrative Record <i>Plaintiffs Notice of Motion and Motion to Complete the Administrative Record; Memorandum of Points and Authorities in Support Thereof.</i> Motion Hearing continued to 12/17/2015 11:00 AM before Magistrate Judge Kandis A. Westmore. <i>(This is a text-only entry generated by the court. There is no document associated with this entry.)</i> (kawlc1, COURT STAFF) (Filed on 12/2/2015) (Entered: 12/02/2015)
12/02/2015	86	CLERK'S NOTICE Advancing Motion Hearing on 73 MOTION Complete the Administrative Record to Thursday, 12/3/2015 11:00 AM in Courtroom 2, 4th Floor, Oakland before Magistrate Judge Kandis A. Westmore. <i>(This is a text-only entry generated by the court. There is no document associated with this entry.)</i> (kawlc1, COURT STAFF) (Filed on 12/2/2015) (Entered: 12/02/2015)
12/03/2015	87	Minute Entry for proceedings held before Magistrate Judge Kandis A. Westmore: Arguments heard, matter submitted. Court to issue order.Motion Hearing held on 12/3/2015. re 73 MOTION Complete the Administrative Record <i>Plaintiffs Notice of Motion and Motion to Complete the Administrative Record; Memorandum of Points and Authorities in Support Thereof</i> filed by James Prigoff, Aaron Conklin, Khaled Ibrahim, Wiley Gill, Tariq Razak Court Reporter Name Diane Skillman. (sisS, COURT STAFF) (Date Filed: 12/3/2015) (Entered: 12/03/2015)
12/18/2015	88	Order by Magistrate Judge Kandis A. Westmore granting in part and denying in part 73 motion to complete administrative record.(kawlc2S, COURT STAFF) (Filed on 12/18/2015) (Entered: 12/18/2015)
12/22/2015	89	STIPULATION WITH PROPOSED ORDER filed by Department of Justice, Eric H. Holder, Jr, Loretta Lynch, Kshemendra Paul, Program Manager - Information Sharing Environment. (Attachments: # 1 Proposed Order)(Gostin, Kieran) (Filed on 12/22/2015) (Entered: 12/22/2015)
12/22/2015	90	STIPULATION AND ORDER REGARDING EXTENSION TO SEEK RELIEF FROM MAGISTRATE JUDGE'S NONDISPOSITIVE ORDER. Signed by Judge Richard Seeborg on 12/22/15. (cl, COURT STAFF) (Filed on 12/22/2015) (Entered: 12/22/2015)
01/11/2016	91	NOTICE of Substitution of Counsel by Winifred Virginia Kao (Kao, Winifred) (Filed on 1/11/2016) (Entered: 01/11/2016)
01/13/2016	92	First MOTION for Leave to File Excess Pages <i>Unopposed Administrative Motion to Exceed Page Limits For Motion Filed Under L.R. 72-2</i> filed by Department of Justice, Eric H. Holder, Jr, Loretta Lynch, Kshemendra Paul, Program Manager - Information Sharing Environment. (Attachments: # 1 Affidavit, # 2 Proposed Order)(Freeborne, Paul) (Filed on 1/13/2016) (Entered: 01/13/2016)
01/13/2016	93	ORDER by Judge Richard Seeborg granting 92 Motion for Leave to File Excess Pages. (cl, COURT STAFF) (Filed on 1/13/2016) (Entered: 01/13/2016)
01/15/2016	94	MOTION Relief from Nondispositive Pretrial Order of Magistrate Judge re 88 Order on Motion for Miscellaneous Relief <i>Pursuant to L.R. 72-2</i> filed by Department of Justice, Eric H. Holder, Jr, Loretta Lynch, Kshemendra Paul, Program Manager - Information Sharing Environment. Responses due by 1/29/2016. Replies due by 2/5/2016.

		(Attachments: # 1 Proposed Order)(Freeborne, Paul) (Filed on 1/15/2016) (Entered: 01/15/2016)
01/15/2016	95	ORDER SETTING BRIEFING SCHEDULE. Signed by Judge Richard Seeborg on 1/15/16. (cl, COURT STAFF) (Filed on 1/15/2016) (Entered: 01/15/2016)
01/20/2016	96	STIPULATION WITH PROPOSED ORDER <i>Regarding Continuation of January 28, 2016 Case Management Conference</i> filed by Department of Justice, Eric H. Holder, Jr, Loretta Lynch, Kshemendra Paul, Program Manager - Information Sharing Environment. (Attachments: # 1 Proposed Order)(Freeborne, Paul) (Filed on 1/20/2016) (Entered: 01/20/2016)
01/20/2016	97	TRANSCRIPT ORDER by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak for Court Reporter Diane Skillman. (Lye, Linda) (Filed on 1/20/2016) (Entered: 01/20/2016)
01/21/2016	98	CLERK'S NOTICE CONTINUING FURTHER CASE MANAGEMENT CONFERENCE. Case Management Statement due by 2/11/2016. Further Case Management Conference previously set for 1/28/2016 Continued to 2/18/2016 at 10:00 AM in Courtroom 3, 17th Floor, San Francisco. <i>(This is a text-only entry generated by the court. There is no document associated with this entry.)</i> (cl, COURT STAFF) (Filed on 1/21/2016) (Entered: 01/21/2016)
01/29/2016	99	Transcript of Proceedings held on December 3, 2015, before Judge Kandis A. Westmore. Court Reporter Diane E. Skillman, telephone number 510-451-2930, Diane_Skillman@cand.uscourts.gov. Per General Order No. 59 and Judicial Conference policy, this transcript may be viewed only at the Clerk's Office public terminal or may be purchased through the Court Reporter until the deadline for the Release of Transcript Restriction. After that date it may be obtained through PACER. Any Notice of Intent to Request Redaction, if required, is due no later than 5 business days from date of this filing. (Re 97 Transcript Order) Release of Transcript Restriction set for 4/28/2016. (Related documents(s) 97) (Skillman, Diane) (Filed on 1/29/2016) (Entered: 01/29/2016)
01/29/2016	100	RESPONSE (re 94 MOTION Relief from Nondispositive Pretrial Order of Magistrate Judge re 88 Order on Motion for Miscellaneous Relief Pursuant to L.R. 72-2) <i>Plaintiffs Response to Defendants Motion for Relief from Non-Dispositive Pretrial Order of Magistrate Judge</i> filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Sadler, Nicole) (Filed on 1/29/2016) (Entered: 01/29/2016)
02/11/2016	101	CASE MANAGEMENT STATEMENT (<i>Joint</i>) filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Lye, Linda) (Filed on 2/11/2016) (Entered: 02/11/2016)
02/12/2016	102	ORDER RE DEFENDANTS' MOTION FOR RELIEF FROM NON-DISPOSITIVE PRETRIAL ORDER OF MAGISTRATE JUDGE. Further Case Management Conference set for 8/4/2016 at 10:00 AM in Courtroom 3, 17th Floor, San Francisco.Signed by Judge Richard Seeborg on 2/16/16. (cl, COURT STAFF) (Filed on 2/12/2016) (Entered: 02/12/2016)
03/04/2016	103	NOTICE by Department of Justice, Eric H. Holder, Jr, Loretta Lynch, Kshemendra Paul, Program Manager - Information Sharing Environment <i>Notice of Withdrawal of Counsel</i> (Freeborne, Paul) (Filed on 3/4/2016) (Entered: 03/04/2016)
04/08/2016	104	STIPULATION WITH PROPOSED ORDER filed by Department of Justice, Eric H. Holder, Jr, Loretta Lynch, Kshemendra Paul, Program Manager - Information Sharing Environment. (Attachments: # 1 Proposed Order)(Gostin, Kieran) (Filed on 4/8/2016) (Entered: 04/08/2016)

04/08/2016	105	ORDER by Judge Richard Seeborg granting 104 Stipulation regarding extension of deadline to comply with Magistrate Judge's Order.(cl, COURT STAFF) (Filed on 4/8/2016) (Entered: 04/08/2016)
04/15/2016	106	NOTICE by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak <i>Notice of Withdrawal of Nicole R. Sadler as Counsel for Plaintiffs</i> (Wiese, Phillip) (Filed on 4/15/2016) (Entered: 04/15/2016)
05/10/2016	107	NOTICE by Department of Justice, Eric H. Holder, Jr, Loretta Lynch, Kshemendra Paul, Program Manager - Information Sharing Environment <i>Filing of Supplemental Administrative Record</i> (Attachments: # 1 Certification, # 2 Supplemental Administrative Record - Part 1, # 3 Supplemental Administrative Record - Part 2)(Gostin, Kieran) (Filed on 5/10/2016) (Entered: 05/10/2016)
05/25/2016	108	NOTICE of Substitution of Counsel by Christina Sinha (Sinha, Christina) (Filed on 5/25/2016) (Entered: 05/25/2016)
06/10/2016	109	NOTICE of Appearance by Phillip Jared Wiese (Wiese, Phillip) (Filed on 6/10/2016) (Entered: 06/10/2016)
06/21/2016	110	JOINT CASE MANAGEMENT STATEMENT filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Lye, Linda) (Filed on 6/21/2016) (Entered: 06/21/2016)
07/22/2016	111	CLERK'S NOTICE The Case Management Conference previously set for August 4, 2016, is continued to January 26, 2017, at 10:00 AM in Courtroom 3, 17th Floor, San Francisco. This is a text only entry. There is no document associated with this notice. (rslc2S, COURT STAFF) (Filed on 7/22/2016) (Entered: 07/22/2016)
07/25/2016	112	CASE MANAGEMENT SCHEDULING ORDER: Motion Hearing for cross MSJ set for 12/8/2016 01:30 PM in Courtroom 3, 17th Floor, San Francisco before Hon. Richard Seeborg. Signed by Judge Richard Seeborg on 7/25/16. (bpf, COURT STAFF) (Filed on 7/25/2016) (Entered: 07/25/2016)
08/18/2016	113	MOTION for Summary Judgment <i>and Memorandum in Support</i> filed by Department of Justice, Eric H. Holder, Jr, Loretta Lynch, Kshemendra Paul, Program Manager - Information Sharing Environment. Motion Hearing set for 12/8/2016 01:30 PM in Courtroom 3, 17th Floor, San Francisco before Hon. Richard Seeborg. Responses due by 9/22/2016. Replies due by 10/20/2016. (Attachments: # 1 Exhibit A, # 2 Exhibit B) (Gostin, Kieran) (Filed on 8/18/2016) (Entered: 08/18/2016)
08/22/2016	114	NOTICE of Substitution of Counsel by Steven Andrew Myers (Myers, Steven) (Filed on 8/22/2016) (Entered: 08/22/2016)
09/22/2016	115	RESPONSE (re 113 MOTION for Summary Judgment <i>and Memorandum in Support</i>) <i>Plaintiffs' Opposition to Defendants' Motion for Summary Judgment and Cross-Motion for Summary Judgment; Memorandum of Points and Authorities in Support</i> filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Wiese, Phillip) (Filed on 9/22/2016) (Entered: 09/22/2016)
09/22/2016	116	Declaration of Linda Lye in Support of 115 Opposition/Response to Motion, <i>Motion for Summary Judgment and Cross-Motion for Summary Judgment</i> filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Related document(s) 115) (Wiese, Phillip) (Filed on 9/22/2016) (Entered: 09/22/2016)
09/22/2016	117	Declaration of James Prigoff in Support of 115 Opposition/Response to Motion, <i>Motion for Summary Judgment and Plaintiffs' Opposition to Defendants' Motion for Summary Judgment</i> filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq

		Razak. (Related document(s) 115) (Wiese, Phillip) (Filed on 9/22/2016) (Entered: 09/22/2016)
09/22/2016	118	Declaration of Tariq Razak in Support of 115 Opposition/Response to Motion, <i>Motion for Summary Judgment</i> filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Related document(s) 115) (Wiese, Phillip) (Filed on 9/22/2016) (Entered: 09/22/2016)
09/22/2016	119	Declaration of Khaled Ibrahim in Support of 115 Opposition/Response to Motion, <i>Motion for Summary Judgment</i> filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Related document(s) 115) (Wiese, Phillip) (Filed on 9/22/2016) (Entered: 09/22/2016)
09/22/2016	120	Declaration of Aaron Conklin in Support of 115 Opposition/Response to Motion, <i>Motion for Summary Judgment and Plaintiffs' Opposition to Defendants' Motion for Summary Judgment</i> filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Related document(s) 115) (Wiese, Phillip) (Filed on 9/22/2016) (Entered: 09/22/2016)
09/22/2016	121	First MOTION to Strike 113 MOTION for Summary Judgment <i>and Memorandum in Support Plaintiffs Motion to Strike Defendants Declarations and to Supplement the Record with Plaintiffs Declarations; Memorandum of Points and Authorities in Support</i> filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. Motion Hearing set for 12/8/2016 01:30 PM in Courtroom 3, 17th Floor, San Francisco before Hon. Richard Seeborg. Responses due by 10/20/2016. Replies due by 11/17/2016. (Attachments: # 1 Proposed Order [Proposed] Order Denying Defendants' Motion for Summary Judgment, Granting Plaintiffs' Motions to Strike and Supplement, and Granting Plaintiffs' Motion for Summary Judgment)(Wiese, Phillip) (Filed on 9/22/2016) (Entered: 09/22/2016)
09/29/2016	122	STIPULATION WITH PROPOSED ORDER re 121 First MOTION to Strike 113 MOTION for Summary Judgment <i>and Memorandum in Support Plaintiffs Motion to Strike Defendants Declarations and to Supplement the Record with Plaintiffs Declarations; Memorandum of Points and Authorities in Su</i> filed by Department of Justice, Eric H. Holder, Jr, Loretta Lynch, Kshemendra Paul, Program Manager - Information Sharing Environment. (Myers, Steven) (Filed on 9/29/2016) (Entered: 09/29/2016)
09/30/2016	123	STIPULATION AND ORDER RE 122 SETTING BRIEFING SCHEDULE ON PLAINTIFFS' MOTION TO STRIKE DEFENDANTS' DECLARATIONS AND TO SUPPLEMENT THE RECORD WITH PLAINTIFFS' DECLARATIONS. Signed by Judge Richard Seeborg on 9/30/16. (cl, COURT STAFF) (Filed on 9/30/2016) (Entered: 09/30/2016)
10/20/2016	124	REPLY (re 113 MOTION for Summary Judgment <i>and Memorandum in Support</i>) ; <i>Opposition to Plaintiffs' Motion for Summary Judgment 115 ; and Opposition to Plaintiffs' Motion to Strike Defendants' Declarations and Supplement the Record with Plaintiffs' Declarations 121</i> filed by Department of Justice, Eric H. Holder, Jr, Loretta Lynch, Kshemendra Paul, Program Manager - Information Sharing Environment. (Myers, Steven) (Filed on 10/20/2016) (Entered: 10/20/2016)
11/01/2016	125	ADMINISTRATIVE MOTION File Declaration <i>Unopposed Administrative Motion to File Declaration in Support of Summary Judgment</i> filed by Wiley Gill. Responses due by 11/7/2016. (Attachments: # 1 Declaration Declaration of Linda Lye in Support of Unopposed Administrative Motion to File Declaration in Support of Summary Judgment, # 2 Proposed Order [Proposed] Order)(Lye, Linda) (Filed on 11/1/2016) (Entered: 11/01/2016)

11/03/2016	126	ORDER by Judge Richard Seeborg granting 125 Administrative Motion. (cl, COURT STAFF) (Filed on 11/3/2016) (Entered: 11/03/2016)
11/03/2016	127	Declaration of Wiley Gill in Support of 115 Opposition/Response to Motion, <i>Motion for Summary Judgment</i> filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Related document(s) 115) (Wiese, Phillip) (Filed on 11/3/2016) (Entered: 11/03/2016)
11/17/2016	128	REPLY (re 113 MOTION for Summary Judgment <i>and Memorandum in Support</i>) <i>Plaintiffs Reply in Support of Motion for Summary Judgment and Motion to Strike And Supplement</i> filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Wiese, Phillip) (Filed on 11/17/2016) (Entered: 11/17/2016)
12/08/2016	129	Minute Entry for proceedings held before Hon. Richard Seeborg: Motion Hearing held on 12/8/2016. Matters taken under submission. Court to issue an order re 121 First MOTION to Strike 113 MOTION for Summary Judgment Total Time in Court 30 minutes. Court Reporter: Pam Batalo. Plaintiff Attorney: Lynda Lye, Julia Harumi Mass, Christina Sinha, Ellie Chapman, Phillip Wiese. Defendant Attorney: Steven Meyers. This is a text only Minute Entry (cl, COURT STAFF) (Date Filed: 12/8/2016) (Entered: 12/08/2016)
01/18/2017	130	JOINT CASE MANAGEMENT STATEMENT <i>Further Joint Case Management Statement and [Proposed] Order</i> filed by Wiley Gill. (Lye, Linda) (Filed on 1/18/2017) (Entered: 01/18/2017)
01/18/2017	131	CLERK'S NOTICE CONTINUING CASE MANAGEMENT CONFERENCE. Case Management Statement due by 3/16/2017. Initial Case Management Conference previously set for 1/26/2017 Continued to 3/23/2017 at 10:00 AM in Courtroom 3, 17th Floor, San Francisco. (cl, COURT STAFF) (Filed on 1/18/2017) (Entered: 01/18/2017)
03/13/2017	132	JOINT CASE MANAGEMENT STATEMENT <i>Further Joint Case Management Statement and [Proposed] Order</i> filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. (Lye, Linda) (Filed on 3/13/2017) (Entered: 03/13/2017)
03/14/2017	133	CLERK'S NOTICE RESCHEDULING FURTHER CASE MANAGEMENT CONFERENCE. Case Management Statement due by 4/20/2017. Further Case Management Conference previously set for 3/23/2017 Continued to 4/27/2017 at 10:00 AM in Courtroom 3, 17th Floor, San Francisco. <i>(This is a text-only entry generated by the court. There is no document associated with this entry.)</i> (cl, COURT STAFF) (Filed on 3/14/2017) (Entered: 03/14/2017)
03/27/2017	134	ORDER ON CROSS MOTIONS FOR SUMMARY JUDGMENT. Signed by Judge Richard Seeborg on 3/27/17. (cl, COURT STAFF) (Filed on 3/27/2017) (Entered: 03/27/2017)
03/29/2017	135	JUDGMENT. Signed by Judge Richard Seeborg on 3/29/17. (cl, COURT STAFF) (Filed on 3/29/2017) (Entered: 03/29/2017)
05/28/2017	136	NOTICE OF APPEAL to the 9th Circuit Court of Appeals filed by Aaron Conklin, Wiley Gill, Khaled Ibrahim, James Prigoff, Tariq Razak. Appeal of Order, Terminate Motions 134 , Judgment, Terminated Case 135 (Appeal fee FEE NOT PAID.) ***17-16107*** (Lye, Linda) (Filed on 5/28/2017) Modified on 6/8/2017 (gbaS, COURT STAFF). (Entered: 05/28/2017)

05/30/2017	137	USCA Appeal Fees received \$ 505.00 receipt number 0971-11430023 re 136 Notice of Appeal, filed by James Prigoff, Aaron Conklin, Khaled Ibrahim, Wiley Gill, Tariq Razak. (gbaS, COURT STAFF) (Filed on 5/30/2017) (Entered: 06/07/2017)
06/08/2017	138	USCA Case Number 17-16107 for 136 Notice of Appeal, filed by James Prigoff, Aaron Conklin, Khaled Ibrahim, Wiley Gill, Tariq Razak. (gbaS, COURT STAFF) (Filed on 6/8/2017) (Entered: 06/08/2017)

9th Circuit Case Number(s) 17-16107

NOTE: To secure your input, you should print the filled-in form to PDF (File > Print > PDF Printer/Creator).

CERTIFICATE OF SERVICE

When All Case Participants are Registered for the Appellate CM/ECF System

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system

on (date) Nov 3, 2017 .

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Signature (use "s/" format) s/ Linda Lye

CERTIFICATE OF SERVICE

When Not All Case Participants are Registered for the Appellate CM/ECF System

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system

on (date) .

Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

I further certify that some of the participants in the case are not registered CM/ECF users. I have mailed the foregoing document by First-Class Mail, postage prepaid, or have dispatched it to a third party commercial carrier for delivery within 3 calendar days to the following non-CM/ECF participants:

[Empty box for listing non-CM/ECF participants]

Signature (use "s/" format)

[Empty box for signature]