

No. 17-16107

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

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

Plaintiffs-Appellants,

v.

U.S. DEPARTMENT OF JUSTICE; JEFFERSON B. SESSIONS III, in his official
capacity as Attorney General; PROGRAM MANAGER—INFORMATION
SHARING ENVIRONMENT; and THE OFFICE OF PROGRAM MANAGER
FOR THE INFORMATION SHARING ENVIRONMENT,

Defendants-Appellees.

On Appeal from the United States District Court for the
Northern District of California, Case No. 3:14-cv-03120-RS

SUPPLEMENTAL EXCERPTS OF RECORD — VOLUME 2 OF 2
(Pages 298-499)

CHAD A. READLER
Acting Assistant Attorney General

ALEX G. TSE
Acting United States Attorney

H. THOMAS BYRON III
(202) 616-5367

DANIEL AGUILAR
(202) 514-5432
Attorneys, Appellate Staff
Civil Division, Room 7266
Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530-0001

TABLE OF CONTENTS

Volume 1

Dkt. 115, Plaintiff's Opposition to Defendants' Motion for Summary Judgment and Cross-motion for Summary Judgment (excerpts) (Sept. 22, 2016)	1
Dkt. 113-1, Declaration of Basil N. Harris (excerpts) (Aug. 17, 2016)	7
Dkt. 107, Supplemental Administrative Record (May 10, 2016).....	9
Doc. 3, National Strategy for Information Sharing (Oct. 2007).....	11
Doc. 7, ISE SAR Evaluation Environment Implementation Guide, Version 1.0 (Jan. 9, 2009).....	59
Doc. 8, Final Report: Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Evaluation Environment (Jan. 2010)	89
Doc. 9, Review of Advocate Websites for Concerns and Issues on ISE-Related Activities (2012)	252
Dkt. 70, First Supplemental Complaint for Declaratory and Injunctive Relief (Sept. 3, 2015)	259

Volume 2

Dkt. 52-2, Administrative Record Index (June 16, 2015).....	298
Dkt. 53, Administrative Record (June 16, 2015)	
Doc. 12, Agenda for a September 2008 Dialogue on Privacy and Civil Liberties outreach meeting agenda hosted by the PM-ISE (Aug. 27, 2008)	304
Doc. 13, September 2008 PM-ISE hosted Dialogue on Privacy and Civil Liberties outreach meeting attendee list (Aug. 27, 2008).....	306

Doc. 14, September 2008 PM-ISE hosted Dialogue on Privacy and Civil Liberties outreach meeting description of meeting purpose and ground rules (Aug. 28, 2008)	310
Doc. 15, Information Sharing Environment – Suspicious Activity Reporting Functional Standard And Evaluation Environment Initial Privacy and Civil Liberties Analysis September 2008—Version 1 (Sept. 2008)	311
Doc. 17, Email from Michael German (ACLU) providing suspicious activity examples, with attachment (Jan. 16, 2009)	343
Doc. 18, Email from Michael German regarding possible amendments to the ISE-SAR Functional Standard ver. 1.0 (Jan. 23, 2009)	346
Doc. 19, Tips and Leads Issue Paper email, with attachment Tips and Leads Issue Paper 10 07.pdf (Feb. 10, 2009)	349
Doc. 20, Feedback Session with Privacy and Civil Liberties Advocates: Suspicious Activity Reporting (SAR) Line-Officer Training and the ISE-SAR Functional Standard --Agenda (Feb. 13, 2009)	363
Doc. 21, Feedback Session with Privacy and Civil Liberties Advocates: Suspicious Activity Reporting (SAR) Line-Officer Training and the ISE-SAR Functional Standard --Attendee List (Feb. 18, 2009)	364
Doc. 23, Email from Mohamed Elibiary regarding feedback (Feb. 26, 2009)	366
Doc. 24, Suggestions from Michael German for revision to functional standard email (Mar. 30, 2009)	369
Doc. 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)	371

Doc. 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)	409
Doc. 31, Email regarding meeting between Mike German and the Program Manager on July 18, 2012 and meeting invitation (July 9, 2012).....	446
Doc. 34, Email regarding meeting between Greg Nojeim (Center for Democracy and Technology) and the Program Manager on October 22, 2012 and meeting invitation (Oct. 1, 2012)	450
Doc. 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).....	456
Doc. 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, including attachments (May 24, 2013).....	457
Dkt. 1, Complaint for Declaratory and Injunctive Relief.....	461

ADMINISTRATIVE RECORD INDEX

	<u>DOCUMENT INFORMATION</u>	<u>BATES NUMBER</u>	<u>REDACTION¹</u>
1	2	3	4
3	4	5	6
4	5	6	7
5	6	7	8
6	7	8	9
7	8	9	10
8	9	10	11
9	10	11	12
10	11	12	13
11	12	13	14
12	13	14	15
13	14	15	16
14	15	16	17
15	16	17	18
16	17	18	19
17	18	19	20
18	19	20	21
19	20	21	22
20	21	22	23
21	22	23	24
22	23	24	25
23	24	25	26
24	25	26	27
25	26	27	28
26	27	28	
27	28		
28			

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	158-160	01 & 03
3	amendments to the ISE-SAR Functional Standard ver.		
4	1.0 (January 23, 2009) (Comments on Functional		
5	Standard.msg)		
6	19 Tips and Leads Issue Paper email, with attachment	161-174	01 & 03
7	Tips and Leads Issue Paper 10 07.pdf (February 10,		
8	2009) (Tips and Leads Issue Paper.msg)		
9	20 Feedback Session with Privacy and Civil Liberties	175	01
10	Advocates: Suspicious Activity Reporting (SAR)		
11	Line-Officer Training and the ISE-SAR Functional		
12	Standard --Agenda (February 13, 2009) (Agenda		
13	February 18, 2009 - SAR Feedback Session.doc)		
14	21 Feedback Session with Privacy and Civil Liberties	176-177	01 & 03
15	Advocates: Suspicious Activity Reporting (SAR)		
16	Line-Officer Training and the ISE-SAR Functional		
17	Standard --Attendee List (February 18, 2009)		
18	(Attendee List v3 Feb2009 roundtable.xls)		
19	22 ISE- SAR Steering Committee March meeting email,	178-179	01 & 02
20	with attachment ISE-SAR SC Agenda_2009-03-		
21	05_v2.doc (February 25, 2009) (FW ISE-SAR		
22	Steering Committee Meeting March 5 2009.msg)		
23	23 Email from Mohamed Elibiary regarding feedback	180-182	01 & 03
24	(February 26, 2009) (Re follow-up and some heart-		
25	felt feedback.msg)		
26	24 Suggestions from Michael German for revision to	183-184	01, 03 & 04
27	functional standard email (March 30, 2009) (Re		
28	Thanks.msg)		
29	25 ISE- SAR Steering Committee April meeting email,	185-186	01 & 02
30	with attachment ISE-SAR SC_Agenda_2009-04-		
31	07.doc (April 1, 2009) (FW ISE-SAR Steering		
32	Committee Meeting April 7 2009.msg)		
33	26 Memorandum for Release of the Information Sharing	187-188	None
34	Environment (ISE) Functional Standard for		
35	Suspicious Activity Reporting, Version 1.5 (May 21,		
36	2009) (ISE-SAR Functional Standard V1.5 Cover		

	Letter.pdf)		
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
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
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
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
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
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
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

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
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
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
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
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
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

	Final DRAFT Clean 112114.doc)		
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
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
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






DIALOGUE ON PRIVACY AND CIVIL LIBERTIES

SEPTEMBER 3, 2008
WASHINGTON, DC

**International Square Center
1875 I Street, NW
Fifth Floor, Capitol Conference Room
Washington, DC**

9:00 a.m. – 9:15 a.m.	Welcome and Introductions	<p>██████████ Deputy Program Manager, Information Sharing Environment (PM-ISE), Office of the Director of National Intelligence (ODNI)</p> <p>Mr. Michael German Policy Counsel, Washington Office, American Civil Liberties Union (ACLU)</p> <p>Mr. Russell Porter ██████████ Director, Intelligence Fusion Center, Iowa Department of Public Safety; Chair, Criminal Intelligence Coordinating Council (CICC)</p>
9:15 a.m. – 9:30 a.m.	Framing the Day	██████████
9:30 a.m. – 10:00 a.m.	Fusion Center Privacy Policy Development Efforts From a Local Perspective	<p>Mr. Vernon Keenan ██████████ Virginia Bureau of Investigation; Chair, Privacy Committee, CICC/Global ██████████ Working Group</p>
10:00 a.m. – 10:10 a.m.	<i>Break</i>	
10:10 a.m. – 10:55 a.m.	Suspicious Activity Report (SAR) Process Overview and ISE Evaluation Environment	<p>██████████ Senior Advisor, PM-ISE</p>

DIALOGUE ON PRIVACY AND CIVIL LIBERTIES

SEPTEMBER 3, 2008
WASHINGTON, DC

10:55 a.m. – 11:45 a.m.	Privacy and Civil Liberties Perspectives on the SAR Process	Mr. Michael German
11:45 a.m. – 12:00 Noon	<i>Break</i>	
12:00 Noon – 1:00 p.m.	Working Lunch Presentations: <ul style="list-style-type: none"> ▪ Los Angeles Police Department (LAPD) SAR Process ▪ Privacy and Civil Liberties Perspective on LAPD SAR Process 	[REDACTED] Commander Joan McNamara Counterterrorism Unit, LAPD Mr. Peter Bibring Staff Attorney, ACLU of Southern California
1:00 p.m. – 1:10 p.m.	<i>Break</i>	
1:10 p.m. – 2:10 p.m.	Discussion: Addressing Privacy and Civil Liberties Concerns	[REDACTED] Civil Liberties Protection Officer, ODNI Mr. Kenneth P. Mortensen Acting Chief Privacy and Civil [REDACTED], U.S. Department of Justice
2:10 p.m. – 2:45 p.m.	Expanding the Dialogue Nationally	[REDACTED]
2:45 p.m. – 3:00 p.m.	Wrap-Up	[REDACTED]

Page 2 of 2

**Dialogue on Privacy and Civil Liberties
Washington, DC
September 3, 2008**

Mr. Peter Bibring
Staff Attorney
American Civil Liberties Union
of Southern California
1313 West Eight Street
Los Angeles, CA 90017

[Redacted]

Major George Bivens
Director
Intelligence Division
Bureau of Criminal Investigation
Pennsylvania State Police
1800 Elmerton Avenue
Harrisburg, PA 17110

[Redacted]

Mr. Michael T. Bosacker
Director
Minnesota Joint Analysis Center
Minnesota Bureau of Criminal Apprehension
Suite 820
111 Washington Avenue, South
Minneapolis, MN 55401

[Redacted]

[Redacted]
Senior Advisor
Office of the Program Manager
Information Sharing Environment
Office of the Director of National Intelligence

[Redacted]

[Redacted]
Policy and Planning Division
Office of the Program Manager
Information Sharing Environment
Office of the Director of National Intelligence

[Redacted]

Ms. Dawn M. Diedrich
Deputy Director
Georgia Bureau of Investigation
3121 Panthersville Road
Decatur, GA 30034

[Redacted]

[Redacted]
Deputy for Civil Liberties
Office of the Director of National Intelligence

[Redacted]

[Redacted]
Communications and Outreach
Office of the Program Manager
Information Sharing Environment
Office of the Director of National Intelligence

[Redacted]

[Redacted]
Section Chief
Information Sharing and Collaboration
U.S. Department of Homeland Security
Washington, DC 20528

[Redacted]

Colonel Joseph R. Fuentes
Superintendent
New Jersey State Police
Post Office Box 7068
Upper Ferry Road and River Road
West Trenton, NJ 08628

[REDACTED]

Mr. Vernon Keenan
Director
Georgia Bureau of Investigation
3121 Pantherville Road
Decatur, GA 30034

[REDACTED]

Mr. Michael German
Policy Counsel
American Civil Liberties Union
Washington Legislative Office
915 15th Street NW
Washington, DC, 20005

[REDACTED]

[REDACTED]
Deputy for Privacy
Assistant Civil Liberties Protection Officer
Civil Liberties Protection Office
Office of the Director of National Intelligence
Washington, DC 20511

[REDACTED]

Mr. Safiya Ghori-Ahmad
Director
Government Relations
Muslim Public Affairs Council
Suite 210
110 Maryland Avenue, NE
Washington, DC 20002

[REDACTED]

Lieutenant Ron Leavell
Washington State Fusion Center
Seattle Police Department
610 Fifth Avenue
Post Office Box 34986
Seattle, WA 98124

[REDACTED]

[REDACTED]
Civil Liberties Protection Officer
Civil Liberties and Privacy Office
Office of the Director of National Intelligence

[REDACTED]

Mr. J. Patrick McCreary
Associate Deputy Director
Bureau of Justice Assistance
Office of Justice Programs
U.S. Department of Justice
810 Seventh Street, NW
Washington, DC 20531

[REDACTED]

Sergeant Kris Kalis
Counter Terrorism and Criminal intelligence
Bureau
Los Angeles Police Department
Room 630
150 North Los Angeles Street
Los Angeles, CA 90012

[REDACTED]

Commander Joan T. McNamara
Assistant Commanding Officer
Counter-Terrorism and Criminal Intelligence
Bureau
Los Angeles Police Department
150 Los Angeles Street
Los Angeles, CA 90012

[REDACTED]

[REDACTED]
Federal Bureau of Investigation
Washington, DC

Mr. Kenneth P. Mortensen
Acting Chief Privacy and Civil Liberties Officer
Office of the Deputy Attorney General
U.S. Department of Justice

[REDACTED]

Mr. Gregory T. Nojeim
Director and Senior Counsel
Project on Freedom, Security and Technology
Center for Democracy and Technology
Suite 1100
1634 Eye Street, NW
Washington, DC 20006

[REDACTED]

Mr. Thomas J. O'Reilly
Senior Policy Advisor
Bureau of Justice Assistance
Office of Justice Programs
U.S. Department of Justice

[REDACTED]

Mr. Russell M. Porter
Director
Intelligence Fusion Center
Iowa Department of Public Safety
State Public Safety Headquarters
215 East Seventh Street
Des Moines, IA 50319

[REDACTED]

Ms. Julie S. Raffish
Deputy City Attorney
Police General Counsel Division
Los Angeles City Attorney's Office
Eight Floor
200 North Main Street
Los Angeles, CA 90012

[REDACTED]

[REDACTED]
Deputy Program Manager
Office of the Program Manager
Information Sharing Environment
Office of the Director of National Intelligence

[REDACTED]

Mr. Kareem W. Shora
Executive Director
American-Arab Anti-Discrimination Committee
1732 Wisconsin Avenue, NW
Washington, DC 20007

[REDACTED]

Mr. Shakeel Syed
Executive Director
Islamic Shura Council of Southern California
Suite 255
2115 W. Crescent Avenue
Anaheim, CA 92801



[REDACTED]

[REDACTED]
Director for Policy and Programs (Acting)
Office of the Program Manager
Information Sharing Environment

[REDACTED]

Mr. Carl Wicklund
Executive Director
American Probation and Parole Association
Post Office Box 11910
Lexington, KY 40578-1910



DIALOGUE ON PRIVACY AND CIVIL LIBERTIES

SEPTEMBER 3, 2008
WASHINGTON, DC

Purpose

Federal, state, and local officials across the nation are working to establish a mechanism for gathering, documenting, analyzing, and sharing terrorism-related suspicious activities reports, also known as SARs. As processes and protocols are established and evaluated, these officials are mindful that they must be carried out 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. Federal, state, and local officials involved in these efforts have struggled with how best to engage with privacy and civil liberties advocates.

This roundtable session will serve as a first step toward establishing more open and direct interaction between privacy and civil liberties advocacy groups and government entities involved in SAR efforts. The objective of the session is an open dialogue to inform participants about the SAR effort and to surface significant concerns, resulting in the identification of issues and potential solutions that can be used to inform a larger meeting planned for this fall. The day is also designed to help set the stage for future discussions nationally, regionally, and locally between privacy advocates and federal, state, and local officials.

Scope of Topic

The topic to be discussed at this meeting is limited to exploring the privacy and civil liberties implications of implementing the SAR initiative. It is understood that there are broader privacy and civil liberties issues associated with overall efforts to improve the sharing of terrorism-related information, and many of these broader issues will be raised during the larger fall meeting.

Agenda

The roundtable will begin with an overview of the efforts occurring across the country to support the gathering, documenting, analyzing, and sharing of terrorism-related SARs, as well as current efforts to incorporate privacy and civil liberties protections within those efforts. Efforts by the Los Angeles Police Department will be used as a case study to facilitate discussion of broader issues related to SARs. Privacy advocates will have an opportunity to discuss the privacy and civil liberties perspectives on the SAR process and voice their recommendations in addressing privacy and civil liberties issues, policies, and safeguards that should be implemented. The day will conclude with a discussion of expanding the dialogue nationally.

Ground Rules

There will be presentations and an opportunity for open dialogue among all participants to allow for many perspectives. Notes will be taken throughout the day, and a summary of the day's events will be provided to all participants and made available to the public. The meeting is on the record and for attribution. If a participant prefers a statement to be off the record, it will be treated as such and he or she should state that to meeting participants before making the comment.

**INFORMATION SHARING ENVIRONMENT –
SUSPICIOUS ACTIVITY REPORTING FUNCTIONAL STANDARD
AND EVALUATION ENVIRONMENT**

Initial Privacy and Civil Liberties Analysis

September 2008—Version 1

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>.

(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.

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

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.

officials, is sponsoring a project embracing a variety of ISE-SAR Evaluation Environment sites. The umbrella project currently envisions twelve ISE-SAR Evaluation Environment sites to be implemented and activated incrementally as each site is provided the necessary technology package, including hardware, software, and technical assistance.⁴ These ISE-SAR Evaluation Environment sites will be state and major urban area fusion centers and their source agency law enforcement partners. The ISE-SAR Evaluation Environment sites will assess the value of the ISE-SAR process and of the ISE-SAR Functional Standard and the Detailed and Summary ISE-SAR fields in advancing counterterrorism goals, i.e., (1) the usefulness of the ISE-SAR Criteria Guidance (Part B of the ISE-SAR Functional Standard) in identifying pre-operational planning related to terrorism, and (2) the extent to which the sharing of ISE-SARs, both Detailed and Summary, across the levels of government enables discovery and analysis of terrorism trends and supports counter-terrorism efforts. In addition to evaluating the ISE SAR Functional Standard, the ISE-SAR Evaluation Environment will also provide access to a library of free-text SAR summaries containing no privacy field information. Additionally, the participants will provide feedback regarding the administrative and procedural aspects of the ISE-SAR initiative, i.e., the process of designating information as an ISE-SAR, the management of postings in ISE Shared Space, the interagency processes for correcting inaccurate information, and other relevant program implementation issues.

The first three ISE-SAR Evaluation Environment sites, state fusion centers in Florida, New York, and Virginia, are scheduled to begin posting Summary ISE-SARs to their respective ISE Shared Spaces in Q4 FY2008.

Systems for Sharing ISE-SAR Information in the Evaluation Environment Initiative

Section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, as amended, directs that to the greatest extent possible, the ISE should be a decentralized, distributed, and coordinated environment that connects existing systems to share terrorism information. Accordingly, the ISE-SAR Evaluation Environment initiative has been designed to leverage architecture attributes of a distributed model. Participating fusion center entities will designate and format ISE-SARs using the ISE-SAR Functional Standard and post them to their individual Shared Space, controlled by the participating fusion center.⁵ The ISE Enterprise Architecture Framework (EAF) envisions a federated system for managing access authorizations and a common architectural structure for ISE business processes, information

⁴ These twelve ISE-SAR Evaluation Environment sites will be announced in the near future.

⁵ The ISE Shared Spaces concept is a key element of the ISE EAF and addresses the stewardship problems identified by the 9/11 Commission by assigning exclusive control of an ISE-SAR to the submitting entity. ISE Shared Spaces are networked data and information repositories used by ISE participants to make their standardized terrorism-related information, applications, and services accessible to other ISE participants. ISE Shared Spaces also provide an infrastructure solution for those ISE participants with national security system (NSS) network assets, historically sequestered with only other NSS systems, to interface with ISE participants having only civil network assets. Additionally, ISE Shared Spaces also provide the means for foreign partners to interface and share terrorism information with their U.S. counterparts. For more information about the ISE Shared Spaces concept, reference the *ISE Enterprise Architecture Framework* and the *ISE Profile Architecture and Implementation Strategy* at www.ise.gov.

Initial Privacy and Civil Liberties Analysis

flows and relationships, services, and other functions.⁶ However, in accordance with the mandate of the IRTPA, no single system for accessing or storing ISE-SARs is envisioned.

Sharing of law enforcement information between fusion centers and the federal law enforcement community currently occurs via the Regional Information Sharing Systems Network (RISSNET), Law Enforcement Online (LEO), and Homeland Security Information Network (HSIN). With regards to the DHS HSIN, ISE-SAR Evaluation Environment data will be limited to vetted members of the Homeland Security State and Local Intelligence Community of Interest (HS SLIC) who are able to access the data via the HSIN-Intelligence platform. All of these systems will support initial access to ISE-SARs data for the Evaluation Environment sites.

NOTE: This document is drafted with the assumption that the ISE Shared Spaces concept will be operational and that each ISE-SAR Evaluation Environment initiative participating agency will maintain and control information in the Shared Space.

Privacy, Civil Rights, and Civil Liberties Protections in the Evaluation Environment Initiative

As noted, the ISE-SAR Functional Standard does not prescribe a complete set of business rules for source agencies to use in collecting, processing, and sharing SAR data (as distinct from designating and formatting ISE-SARs using the ISE-SAR criteria and IEPD). As stated in the Memorandum of Understanding Between the DOJ's Bureau of Justice Assistance (BJA) and the PM-ISE,⁷ the ISE-SAR Evaluation Environment effort will result in the development and publication of a guide or template for federal, state, local, and tribal entities to use in establishing policies, common business processes, and technical capabilities for the gathering, documenting, processing, analysis, and sharing of terrorism-related suspicious activities. The guide or template will be based on "best practices" identified at the ISE-SAR Evaluation Environment sites.

Currently, the ISE-SAR initiative contemplates implementation of the ISE-SAR Functional Standard in the context of the current business processes at the diverse Evaluation Environment sites. Consistent with this report's recommendations, the ISE-SAR Evaluation Environment sites will save Detailed ISE-SARs to the Shared Space, but until they develop or adopt policies and procedures to ensure that appropriate privacy and civil liberties protections are in place,

⁶ The EAF envisions 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 system it would be possible, for example, to grant full access to one set of users and partial access to another set of users. As more ISE Shared Spaces become operational and the PM-ISE issues technical standards governing access rules and requirements for these ISE Shared Spaces, information sharing through the ISE will become more efficient. For example, once access, system certification, and accreditation rules are standardized and applied to ISE Shared Spaces that support connectivity among ISE participants, users will have direct access to ISE information within those ISE Shared Spaces, including ISE-SARs, rather than having to negotiate multiple systems with multiple access rules.

⁷ The Memorandum of Understanding describes the scope of the ISE-SAR Evaluation Environment activities and the roles and responsibilities of the parties to the agreement.

Initial Privacy and Civil Liberties Analysis

the results to an ISE-SAR search will be viewable only without the privacy fields (Summary ISE-SAR format) (see Recommendation C(2)). Once the ISE-SAR Evaluation Environment sites have demonstrated that the necessary privacy policy framework is in place, they may share ISE-SAR information with privacy fields (Detailed ISE-SAR format). Subsequently, based on experience using the Detailed ISE-SAR format, the ISE-SAR Evaluation Environment sites will assess the additional value of sharing privacy field data, including a determination of when and under what circumstances it is necessary and appropriate to reveal these data.

In addition, the Concept of Operations (CONOPS)⁸ under development for the ISE-SAR Evaluation Environment initiative will require that participating fusion centers adopt an umbrella ISE-SARs Evaluation Environment Privacy and Civil Liberties Protection Policy or evaluate and, if necessary, update their existing privacy and civil liberties policy to ensure the gathering, documenting, processing, and sharing of ISE-SARs is consistent with the umbrella policy (see Recommendation C(1)). In either instance, the policy for ISE-SARs must be consistent with applicable state constitutions, statutes, and local ordinances. Each participating fusion center is encouraged to use the *Guide to Conducting Privacy Impact Assessments for State and Local Information Sharing Initiatives* (DRAFT), produced by DOJ's Global Justice Information Sharing Initiative (Global), to determine whether additional protections are warranted (see Recommendation B(2)(b)).⁹

As part of the ISE-SAR Evaluation Environment initiative, the CONOPS will require each participating site to document the manner in which the ISE-SAR information is being posted and shared via the Shared Space and how the site is complying with its ISE-SAR privacy and civil liberties protection policy (see Recommendation C(1)).

With the goal of assisting fusion centers to establish guidelines (business rules) for law enforcement entities to follow in collecting, processing, and sharing suspicious activity and incident information, the practices of several major city police departments with established SAR processes and privacy protections were reviewed as a part of a BJA funded project, in coordination with the Major Cities Chiefs Association, Global and Global's Criminal Intelligence Coordinating Committee (CICC). The project's findings noted that the evaluated police departments did not have complete SAR processes and that improvements in privacy protections were needed. These departments' practices were evaluated and fashioned into recommendations provided to other cities to facilitate the establishment of a SAR process in additional urban areas. (See *Findings and Recommendations of the SAR Support and Implementation Project*.¹⁰) Specific attention was paid to ensure that procedures respect the information privacy

⁸ The CONOPS describes the requirements and capabilities of a PM-ISE sponsored Evaluation Environment established to test and evaluate the ISE-SAR process in an operational setting at state and major urban area fusion centers.

⁹ DOJ, DHS and Global have identified privacy and civil liberties as a priority. For example, the developed (and soon to be released) Fusion Center Baseline Capabilities document includes privacy and civil liberties requirements. Both the Fusion Center Baseline Capabilities and Fusion Center Guidelines address training, security, data accuracy, governance structures, etc., which all support the implementation and monitoring of privacy and civil liberties efforts.

¹⁰ In June 2008, the *Findings and Recommendations of the SAR Support and Implementation Project* were developed to provide recommendations to the Criminal Intelligence Coordinating Council (CICC) from the Major Cities Chiefs Association. Findings

and other legal rights of Americans.¹¹ The *Findings and Recommendations* comport with the requirements of the ISE Privacy Guidelines.¹² As detailed in the Recommendations section of this analysis, entities seeking to develop a robust SAR business process are advised to adopt the “best practices” set out in the *Findings and Recommendations of the SAR Support and Implementation Project* and to implement the requirements of the ISE Privacy Guidelines for all SAR information. In addition, ISE-SAR business rules should address, among other considerations, the vetting of ISE-SARs for criminal predicate and terrorism nexus, constraints on secondary disclosure, logging and auditing of access to ISE-SARs, and procedures for notifying source organizations of inaccuracies in ISE-SAR data.

Privacy and Civil Liberties Analysis

1. What is an ISE-SAR? Must it relate to criminal activity?

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 pre-operational planning related to terrorism, criminal, or other illicit intention.” As stated in the Introduction, 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.

The term “illicit intention” is not defined by the ISE-SAR Functional Standard. *Ballantine’s Law Dictionary*, 1969, defines “illicit” as “unlawful, illegal, prohibited or forbidden by law.” Because terrorism is a criminal act under applicable laws, the authors of this report recommend that applicable documentation make clear that the suspicious behavior underlying an ISE-SAR must demonstrate a nexus to criminal activity or intent, as opposed to non-criminal, but arguably “illicit,” activity or intent (see Recommendation B(3)(c)).¹³

The ISE-SAR Functional Standard further defines an ISE-SAR as a SAR that has been determined, pursuant to a two-part process (described in Q&A #4), to meet ISE-SAR criteria and have a potential terrorism nexus. Once this determination is made, the information becomes an ISE-SAR and is formatted in accordance with the ISE-SAR Functional Standard. The ISE-SAR

and recommendations are based on the practices of the Los Angeles, Boston, Chicago, and Miami-Dade police departments. At the time of this writing, a final draft of this report is under review at the CICC. At the time of this writing, the final draft is available at <http://online.wsj.com/public/resources/documents/mccarecommendation-06132008.pdf>.

¹¹ The development of SAR processes at the local law enforcement level has been spearheaded by the Los Angeles Police Department (LAPD). For example, LAPD’s policies and procedures provide standardized codes that facilitate reporting and review of terrorism-related suspicious incidents. Reports that meet a criminal predicate are shared with experienced and trained investigators in the Major Crimes Division, who forward to the Joint Regional Intelligence Center analysts (JRIC) those SARs judged to be terrorism-related. Analysts at the JRIC combine the information with information from other jurisdictions to identify patterns and trends within the greater Los Angeles region. The LAPD SAR business process includes multiple levels of vetting to ensure information is legally obtained and that it indicates a potential terrorism nexus.

¹² More information on the ISE Privacy Guidelines can be found at <http://www.ise.gov/pages/privacy-implementing.html>.

¹³ The observed behavior need not be in and of itself a crime, of course.

Functional Standard lists 189 data elements that experience with prior terrorism incidents has demonstrated are helpful in understanding potential incidents of terrorism planning or implementation and are therefore potentially contained in SAR reporting. These data elements can be found on pages 12 through 21 of the ISE-SAR Functional Standard.

2. Why is suspicious activity information collected and documented in the first place?

Suspicious activity information is collected and documented by a variety of organizations for a range of purposes. In many organizations within Federal and SLT Governments, as well as certain private sector entities, suspicious activity information is collected and documented to support core mission responsibilities. For example, local law enforcement organizations collect suspicious activity information as a key part of their mission to prevent, investigate, and prosecute criminal activity. In other organizations, suspicious activity information may be collected and documented solely for the purpose of protecting facilities or personnel.

Not all collection of information by government and the private sector that may be considered “suspicious” in a general sense will be considered eligible for a SAR or for an ISE-SAR under the ISE-SAR Functional Standard. Suspicious activity must be “indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention” for a report documenting such activity to be considered a SAR under this standard (see ISE-SAR Functional Standard, PM-ISE Memorandum, “Definitions,” Section 5(g)).

3. What entity designates a SAR as an ISE-SAR?

The ISE-SAR Functional Standard (Part C – ISE-SAR Information Flow Description, Step 4) states that a SAR is designated as an ISE-SAR at one of two types of government entities:

- A state or major urban area fusion center (for SLT ISE-SAR information), or
- A federal agency¹⁴

In some cases, a federal agency field component (e.g., an FBI Joint Terrorism Task Force (JTTF) or Field Intelligence Group (FIG)) and the state or major urban area fusion center may be co-located. In other cases, the JTTF or FIG may be located separately but will collaborate with state or major urban area fusion centers to provide an integrated view of the terrorist threat. In yet other cases, SLT law enforcement entities may share SAR information directly with a federal agency outside of the fusion center or JTTF/FIG structure.¹⁵ In practice, major city police agencies, such as the Los Angeles Police Department, may play a significant role in the

¹⁴ For the purposes of the ISE-SAR Evaluation Environment, a federal agency could mean a headquarters or field component of a Federal Government agency with a counterterrorism (CT) mission (for federal department or agency ISE-SAR information). At least one federal entity (the Department of Defense) has indicated an intent to use the FBI’s e-Guardian system as its Shared Space for posting ISE-SARs. Accordingly, e-Guardian may be one of several Federal Shared Spaces.

¹⁵ The ISE-SAR Functional Standard does not affect currently supported and/or mandated direct interactions between SLT law enforcement and investigatory personnel and JTTFs or FIGs.

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).

inappropriate reporting, and that the program documentation supporting the ISE-SAR Evaluation Environment (CONOPS, participation agreements, etc.) require ISE-SAR Evaluation Environment sites to obtain assurances from source agencies that all personnel involved in the gathering, processing, reporting, analyzing, and sharing of suspicious activity information have been trained on the ISE-SAR Functional Standard criteria and information collection limitations (see Recommendation B(3)(a)). Such training will help ensure that SAR reporting and designation of ISE-SARs are based on observable behaviors and incidents indicative of criminal activity related to terrorism and not on subjects' protected characteristics or lawful activities.

5. What level of review will source agency information be subject to prior to being posted in the Shared Space?

To be effective, information used to support law enforcement investigations and other counter-terrorism activities must be lawfully obtained and have a terrorism nexus.

As described in the ISE-SAR Functional Standard (Part C – ISE-SAR Information Flow Description), the review and vetting process begins when a front-line law enforcement officer responds to a call for service, self-initiates law enforcement action based on a reported incident or observation, or observes suspicious behavior. To preclude reporting on individuals involved in innocent activities, front line personnel must be able to recognize indicators (incidents, behaviors, and modus operandi of individuals and organizations) of criminal activity associated with domestic and international terrorism and must understand the scope of their legal authority to obtain information. The authors of this report recommend that the ISE-SAR Evaluation Environment CONOPS and other participation agreements require appropriate training of front line personnel and multiple levels of report review by senior officers, investigators and analysts similarly trained on the criteria of the ISE-SAR Functional Standard and legal collection thresholds. (See Recommendation B(3)(a).) To satisfy privacy and civil liberties concerns, each fusion center and local entity participating in the ISE-SAR Evaluation Environment initiative should develop, or follow established, business rules for multi-level review and vetting of suspicious activity reporting by personnel trained in the ISE-SAR process.

6. What is the source of the suspicious activity information (i.e., from where/whom is the information collected)? How is the information collected?

There are many sources of suspicious activity information. In some cases the information is reported to SLT or federal law enforcement or homeland security officials by a concerned individual. The reporting of a suspicious activity or incident can be accomplished by telephone, via Internet, in person, or in writing (e.g., 9-1-1 and dispatch centers). Information concerning suspicious activities may also be directly observed or obtained by an authorized government official or by a private sector security guard (the private sector security guard would pass the information to an authorized government official). Agency resources, policies, and procedures determine how the information is first obtained and processed.

At the federal and SLT levels a common method of receipt is through a “Tip” line. Individuals are encouraged to report observed crime and suspicious activities to the police in a given geographic area using a “Tip” line, which is simply a toll-free or local telephone number that individuals can use to report such information. Some agencies, such as the FBI, also use Internet reporting systems for individuals to submit tips.

JTTFs have established policies and procedures in place for reviewing and determining which tips will be further investigated. Even if a tip is not determined to have a terrorism nexus, the relevant federal or SLT authorities may choose to retain it for other reasons, such as inclusion in an “all-crimes” database. Retention of personal information raises privacy and civil liberties concerns and must be consistent with policies and practices that govern how it is used and maintained.

7. How is received suspicious activity information documented?

Practices vary from jurisdiction to jurisdiction. For purposes of the ISE-SAR Functional Standard, suspicious activity information, whether obtained through direct observation by a government official, reported by an individual on a “Tip” line, or acquired via any other mechanism, becomes a “SAR” when it has been reviewed and validated in accordance with that organization’s policies and documented in a written report(s) by an authorized official. Depending upon the policies and procedures of the receiving organization, there may be one or more documents/forms used to describe the activity. This documentation might contain, for example, information reported by an individual through a “Tip” line and the information has been reviewed and validated in accordance with that organization’s policies. Alternately, a SAR document could contain a lead developed from an investigation or through information obtained by querying incident- and fact- based systems used by law enforcement and public safety organizations, such as the National Crime Information Center (NCIC), Department of Motor Vehicles (DMV), and other systems. It is also possible that the first documentation of a suspicious activity will be in the ISE-SAR format.

8. Are actions taken to ensure data quality (e.g., that the information reported in an ISE-SAR is accurate, timely, and reliable)?

The ISE-SAR Functional Standard does not dictate a common process that applies to data quality. Data contained in reports designated as ISE-SARs derive from information gathered by source or reporting law enforcement organizations. Before the suspicious incident or behavior is documented in the first instance, entities may apply various means, tools, and techniques to verify the accuracy, timeliness, and reliability of details surrounding the observed or reported “suspicious” conduct or event. Most often, this verification entails interviews with individuals who supplied the information or investigations of the reportedly “suspicious” circumstances. Law enforcement officers also may query fact-based systems to validate information relating to the incident or conduct.

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).

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.

Given the wide variability in retention standards, it is impossible to define a fixed retention limit for all ISE-SARs without simply adopting the shortest retention period applicable to any ISE participant organization. One of the lessons learned from the terrorist attack of September 11, 2001, is that individual “dots” of information may not paint a picture until a later-acquired piece of information ties them together; thus discarding ISE-SARs too quickly could negatively affect the government’s counterterrorism activities. Conversely, retention periods are an important aspect of data quality and a valuable information privacy safeguard. Rather than impose a single retention standard for all ISE-SARs, the ISE-SAR Functional Standard allows submitting organizations to manage retention (control) of ISE-SARs within their own ISE Shared Space (see Q&A #15 for ISE Shared Spaces definition.) Accordingly, the following two elements included in the Functional Standard allow submitting organizations to “tag” the privacy fields with “purge” or “review” (and purge if not validated) dates:

- The *Report Purge Date*: the date by which the privacy information (information in privacy fields) will be automatically purged from the record system; general observation data is retained.
- The *Report Purge Review Date*: the date for conducting a review to determine the disposition of the privacy fields in a Detailed ISE-SAR record (i.e., the review date).

Unlike the *Report Purge Date*, which automatically removes the privacy fields, the *Report Purge Review Date* alerts a human to conduct a review to determine, based on a validation process, whether some or all of the privacy fields should be purged. The submitting organizations’ business rules will determine whether or not privacy fields will be purged from the record. The analyst’s determination to extend the report purge date must consider the continued value of the privacy fields in light of policies limiting retention of sensitive data by law enforcement entities. It should be noted, however, that the ability to control the purge or review dates for privacy-protected information extends only to ISE-SARs that reside in the submitting organization’s Shared Space. In the event future functionality authorizes bulk information to be copied (downloaded) from the ISE Shared Space and incorporated into another information system, such information would not automatically be purged or reviewed unless required by the receiving entity’s business rule.

11. Do individuals have any ability to control how SAR privacy information about them is collected, used, or shared by the original collector (source agency)?

Generally, no. However, each government entity that collects and documents suspicious activities at the federal, state, local, or tribal level must do so in accordance with applicable law and policy. Again, it is impermissible for entities to collect information based on factors the consideration of which would violate a subject’s civil rights and civil liberties (e.g., race, ethnicity, national origin, religious preference, or freedoms protected by the Constitution (speech or political association) that have no reasonable relation to the criminal activity).

The Privacy Act of 1974 and Freedom of Information Act (FOIA) provide mechanisms by which individuals can determine what information about them is available in federal records. The

Privacy Act generally requires federal agencies to ensure that the information collected about individuals is complete, accurate, and timely. Similar laws have been enacted in many states. These federal laws, and the laws of many states, however, allow agencies to exempt law enforcement-related records from disclosure and data quality requirements under information access, privacy, and sunshine laws that would otherwise give individuals the ability to access or correct records about themselves.

Under the Privacy Act, federal agencies need not in all cases obtain an individual's consent in order to disclose information collected about the individual. The Privacy Act permits agencies to publish "routine uses," articulating the circumstances in which collected information may be disclosed routinely, provided the use is for an agency purpose compatible with the purpose for which the information was initially collected. Generally speaking, information collected for a law enforcement purpose may be shared outside the agency for law enforcement purposes, without consent of the individual to whom it pertains.

See also Q&A #13 below regarding redress under the ISE Privacy Guidelines.

12. Do individuals have any ability to request and obtain SAR information maintained about them from the original collector?

Theoretically, yes. In the federal system the procedure by which individuals may request and obtain information maintained about them is governed by the FOIA and the Privacy Act. In the state and local arena there exist similar laws and requirements, often referred to as "Sunshine Laws." However, as noted, access to SARs information may be extremely limited under disclosure exemptions available for law enforcement records.

13. Can individuals correct the SAR information if they believe it to be inaccurate? If so, what is that mechanism?

Neither the ISE-SAR Functional Standard nor other provision of law or regulation dictates a common process or standard that applies to the correction of information contained in ISE-SARs by subject individuals.

Because of the disclosure exemptions that typically apply to law enforcement records, ISE-SAR subjects generally will not have access to government files and therefore have no way to ascertain the accuracy of records about them. Privacy laws typically exempt law enforcement records from amendment (correction) requirements as well, so that even when access to records is obtained, e.g., through discovery in litigation, the exemption from amendment still applies. However, consistent with the ISE Privacy Guidelines, both federal agencies and SLT agencies such as fusion centers that anticipate participating in the ISE and receiving terrorism-related information directly from federal agencies will be required to have procedures in place for addressing complaints (redress) from individuals who believe the authorities possess inaccurate information about them and who request that erroneous information be corrected. Additionally, individuals may be able to seek assistance within the appropriate federal or state court system.

As part of the Evaluation Environment effort, consistent with the Data Quality provision of the ISE Privacy Guidelines, sites will be asked to develop a specific data quality and redress process 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)).

14. Will personal information be shared by the SAR Evaluation Environment sites? Will there be variations in availability of Detailed ISE-SARs versus Summary ISE-SARs?

Yes, personal information in designated privacy fields will be shared by the SAR Evaluation Environment sites upon demonstration that adequate privacy protection policies are in place.

The ISE-SAR Functional Standard provides two ISE-SAR information exchange formats—“Detailed” and “Summary”—that are the principal mechanism for varying information content based on the operational situation. By flagging specified privacy fields, the ISE-SAR Functional Standard allows for either a Detailed Report (inclusive of privacy fields) or Summary Report (exclusive of privacy fields) to be made available as appropriate to the circumstances, e.g., whether a mission need is served by sharing personal information, limitations on receipt, or disclosure of privacy elements by particular ISE participants. The Detailed ISE-SAR information exchange includes all defined data elements (including privacy protected fields such as name, address, vehicle registration, etc.). The Summary ISE-SAR information exchange includes all data elements except those flagged as privacy fields. The data fields coded as privacy fields in the ISE-SAR Functional Standard are the minimum data that all jurisdictions would likely consider to be privacy protected. Each ISE participant can exclude additional privacy fields from the Summary ISE-SAR information exchange package in accordance with its own legal and policy requirements.

Using point of contact (POC) information established in the IEPD, entities accessing Summary ISE-SARs will be able to contact the source organization if further analysis or investigation demonstrates the need for additional (detailed) information concerning a particular report. Law enforcement personnel having a legitimate reason to obtain the identity of an individual, or individuals, referred to in a Summary SAR would do so through established investigative channels. In addition, the authors of this report recommend that the CONOPS prohibit users from “reverse engineering” Summary ISE-SAR information in an effort to determine the identity of protected persons (see Recommendation (B(1)(j))). The relative value of the Summary and Detailed ISE-SARs ultimately will be tested as part of the ISE-SAR Evaluation Environment initiative. However, in view of privacy and civil liberties concerns when sharing information about ostensibly “criminal” and “terrorism-related” activity, the authors of this report recommend that the first ISE-SAR Evaluation Environment sites to test the ISE-SAR Functional Standard make available only Summary ISE-SARs. The ISE-SAR Evaluation Environment sites

will save Detailed ISE-SARs to the Shared Space, but until they develop or adopt policies and procedures to ensure that appropriate privacy and civil liberties protections are in place, the results to an ISE-SAR search will be viewable only without the privacy fields. Once the ISE-SAR Evaluation Environment sites have demonstrated that the necessary privacy and civil liberties policies are in place, they may share ISE-SAR information in the Detailed ISE-SAR format. (See Recommendation C(2).)

In addition, 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 code the ISE-SAR to limit the authorized recipients of the ISE-SAR within the ISE Shared Spaces, possibly by using CUI designations. (See President’s Memorandum for the Heads of Executive Departments and Agencies, “Designation and Sharing of Controlled Unclassified Information (CUI),” May 9, 2008.)

15. How will ISE-SARs be maintained and shared (e.g., what systems are used)?

Per the ISE-SAR Functional Standard, the following steps would apply:

- An ISE participant (the “submitting organization”) designates and formats a Detailed ISE-SAR in accordance with ISE-SAR Functional Standard (see Q&A #3).
- The submitting organization stores the ISE-SAR in a dedicated SAR system (the ISE Shared Space). Such system should meet the standards of an ISE Shared Space, as described in Version 1 of the ISE Enterprise Architecture Framework (ISE EAF):

“This infrastructure remains outside a participant’s internal network, yet is still under the management and control [including infrastructure, policy and internal processes] of that ISE participant. The ISE Shared Space is designated to host ISE participant shared services and data. For example, in the case of an ISE-SAR, the Shared Space of a participant would be the access point, and optionally the repository, for SAR data. ISE participants will determine their services and data appropriate for sharing based upon applicable policy and internal processes. Those shared services and data will be placed in a separate area behind the organization’s network firewall, but within the ISE Shared Space. The ISE Shared Space is the key to the ISE Core which is the information transport for the participants’ capabilities.” (Information Sharing Environment Enterprise Architecture Framework, August 2007, p. 32)

As reflected in the ISE-EAF, the agencies’ ISE-SAR Shared Spaces will be capable of sharing data at the appropriate level (Detailed or Summary) based on identified criteria and policies. Each submitting organization must manage its Shared Space to give effect to applicable legal, privacy, and other policy requirements with respect to access to information contained in the privacy fields. SARs in the ISE Shared Space will remain under the exclusive control of the submitting organization, which may replace (update) or delete the record based on additional information or consistent with purging or retention requirements.

Given the breadth of the ISE and the fact that ISE Shared Spaces have not yet been created and enabled, it is not possible to list the specific systems that will be used to store and retrieve ISE-SAR information.

The ISE-SAR Functional Standard and ISE Shared Spaces concept are being implemented and tested as part of the ISE-SAR Evaluation Environment. Each fusion center participating in the ISE-SAR Evaluation Environment will copy the SARs it has designated as ISE-SARs onto its own separate server (“Shared Space”) in accordance with applicable laws, regulations, and policies for protecting privacy information, including purging and retention requirements. The Fusion Center ISE Shared Spaces server is connected to one of several existing unclassified, protected networks (e.g., Regional Information Sharing Systems Network (RISSNET), Law Enforcement Online (LEO), Homeland Security Information Network (HSIN), or (potentially) Director of National Intelligence (DNI) Unclassified (DNI-U)). These systems connect the fusion center ISE Shared Space server to a federated environment architected and enabled to provide an aggregate query function (from a central, DOJ-hosted Web page) for linking the distributed ISE-SAR data.

As the operational aspects of the ISE-SAR initiative evolve, the potential functionality of the agency “SAR” server or an ISE Shared Space may develop further. The authors of this report recommend that the CONOPS under development for the ISE-SAR Evaluation Environment limit functionality in the ISE Shared Spaces to “read only” access and not enable annotation of postings by users of the federated search system (see Recommendation B(1)(l)). Thus a participating entity that queries the federated system and identifies a connection between two or more records in various Shared Spaces would need to take affirmative steps to alert the respective source organizations to update their records. Future functionality may permit users to access and incorporate ISE-SARs posted by submitting organizations into their own information systems or to participate in a community of users, e.g., Wikipedia style, where they can add to the submission. Should these capabilities be realized, the privacy and civil liberties ramifications will be assessed for each possible “use” scenario.

16. With whom (agencies, organizational elements, and personnel) is a Detailed ISE-SAR shared?

In the initial ISE-SAR Evaluation Environment sites, and until adequate privacy protections have been determined to be in place, Detailed ISE-SARs will be placed in the Shared Space but will not be shared. Eventually (most likely after the Evaluation Environment is completed), Detailed ISE-SARs should be available to all credentialed participants possessing access to the RISSNET, LEO, and designated HSIN networks. These unclassified, secure systems are virtual, secure connections between different servers that ride the Internet. They vet members prior to granting access to information databases on the “network.” In the case of RISSNET, for example, access is limited to agencies with law enforcement responsibilities or functions, and users may have access only to specific databases on the network. Depending upon the access rules governing the system or network, submitting organizations may need to exclude from

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.

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>.

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.

The PM-ISE will require participants in the ISE-SAR Evaluation Environment to provide feedback regarding notice of errors in three areas in order to maximize the effectiveness of ISE-SAR sharing and protect the privacy and civil liberties of record subjects. These three areas are:

- Feedback to originators when fact information is incorrectly designated as ISE-SAR
- Feedback to all participants if further evidence determines that an ISE-SAR was designated incorrectly
- Recommended changes to the ISE-SAR Criteria Guidance (Part B of the ISE-SAR Functional Standard)

22. What security measures or safeguards will be implemented to protect the information in ISE Shared Spaces and in the federated system (e.g., encryption, classification, other)?

Although ISE-SARs will not be classified, they will be considered law enforcement sensitive and thus warrant protection. The President's new directive concerning Controlled Unclassified Information (CUI) has not yet been fully implemented; however, it is anticipated that ISE-SARs will be handled with appropriate markings and safeguards to protect sensitive information. As with other such information, ISE-SARs shall be stored, processed, and disseminated in a protected information environment that provides adequate security controls. These safeguards may include:

- Controlled access to the information that will allow only authorized ISE users to access, retrieve, and display ISE-SAR information and restricts writing and updates to authorized members of the submitting organization
- Encrypted transmission of information shared between participating organizations

The distributed model itself affords protections and is superior to a centralized model in that it allows for control of data; the ISE-SAR is updated as necessary by authorized members of the source organization, rather than pushed to a repository beyond the submitting agency's control where it remains static and ages. In addition, the distributed model better protects the information, in that it allows for individualized data use agreements between participants. As further protection, the ISE-SAR Evaluation Environment sites will be strictly governed. Formal agreements for the sharing of data with other federal, state, local, or tribal law enforcement agencies will be established among participants, outlining the policies, procedures, and practices for the handling and use of information (including adherence to the requirements of the ISE Privacy Guidelines).

23. Can the data be modified? By whom? Is there a system for tracking modifications?

The CONOPS currently under development for the ISE-SAR Evaluation Environment initiative prescribes that ISE-SARs remain under exclusive control of the submitting organization, which

may update the initial record based on additional information provided by the source agency. For purposes of the Evaluation Environment effort, the submitting organization is the only organization authorized to replace (update) or delete ISE-SARs. As previously noted, should the ISE-SAR be imported into another agency's system or subject to collaborative efforts on the part of authorized users, examination of applicable business rules and related privacy and civil liberties protections would be warranted.

24. Will the data be available for searching?

Yes. In the ISE-SAR Evaluation Environment, ISE-SARs will be available in ISE Shared Spaces for search and retrieval in accordance with the ISE EAF. The CONOPS under development for the ISE-SAR Evaluation Environment envisions that, ultimately, depending on roles, authorizations, and specified purpose, ISE participants may retrieve, as appropriate, either the Detailed or Summary ISE-SAR record. However, the authors of this report recommend that the CONOPS being developed will permit the first Evaluation Environment sites to share only Summary ISE-SARs from their ISE Shared Space, with detailed privacy fields disclosed only through individualized contact with the submitting agency. The CONOPS will stipulate that Detailed ISE-SARs may be accessed through the Shared Space only after the ISE-SAR Evaluation Environment sites have adopted appropriate policies for protecting privacy and civil liberties. The authors of this report recommend that the CONOPS prohibit users from "reverse engineering" Summary ISE-SAR information in an effort to determine the identity of protected persons (see Recommendation B(1)(j)). Thus, users with access only to Summary ISE-SAR information will not be able to access the privacy fields within the Detailed ISE-SARs.

In addition the authors of this report recommend that the CONOPS require the ISE-SAR Evaluation Environment sites to recognize only those inquiries that provide a case, incident, or other justification; will limit the number of records that can be accessed in response to the inquiry; and, will permit "read only" access (see Recommendation B(1)(l)). In the future, should users be enabled to more freely access and incorporate ISE-SARs from the submitting organization's SAR system or ISE Shared Space or modify a submission, a full examination of the applicable business rules and policies will need to be undertaken. Central to that examination, for example, would be whether the policies and practices of the submitting organization (e.g., purge dates, dissemination limitations) continue in effect for ISE-SARs accessed and incorporated into another agency's system.

25. How will the data be retrieved? Can it be retrieved by personal identifier?

The ISE-SAR Functional Standard assumes that ISE-SAR information may be retrieved using a variety of search keys, including personal identifiers in the event that a user has access, based on need, to Detailed ISE-SARs. Using such personal identifiers as the search key results in a more narrowly focused set of search results than would be available using broader categories such as geographic area. Federal entities administering their ISE-SARs by personal identifier

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

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

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:

Initial Privacy and Civil Liberties Analysis

1. **Develop business processes:** Implement mechanisms to ensure suspicious activity reporting protects civil rights and civil liberties, including business processes that
 - a. incorporate checks/procedures to ensure against “profiling” on race, ethnicity, national origin, or religious grounds or violating a person’s constitutional rights (training and written guidance in these areas will assist law enforcement professionals to determine when these criteria have proper investigatory significance)²⁰ (see Q&A #28);
 - b. include steps to vet or validate the accuracy of the 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 Q&A #8 and #13);
 - c. require an ISE-SAR be based on the ISE-SAR criteria (Part B of the ISE-SAR Functional Standard) and establish a potential nexus to terrorism (see Q&A #4);
 - d. provide multiple layers of review and vetting (see Q&A #5);
 - e. require a demonstration of need for personal information elements (privacy fields) before sharing those elements from the Detailed ISE-SARs (see Q&A #14);
 - f. provide notice to sources or users of errors in the content or designation of an ISE-SAR (see Q&A #21);
 - g. provide notice of source reliability and content validity of an ISE-SAR (see Q&A #8);
 - h. include maintenance of detailed information logs (queries, accesses) (see Q&A #29);
 - i. include an audit element and technical safeguard requirements (see Q&A #29);
 - j. prohibit users from “reverse engineering” Summary ISE-SAR information in an effort to determine the identity of protected persons (see Q&A #14 and 24);
 - k. implement user restrictions for SE-SARs, such as user training, and user notification mechanisms (see Q&A #19); and
 - l. limit functionality in the ISE Shared Spaces so that access to 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 (see Q&A #15, 24, and 30).

2. **Develop privacy, civil rights, and other civil liberties protections consistent with the ISE Privacy Guidelines:** Develop and implement privacy policies that afford protections that

²⁰ See, e.g., International Association of Chiefs of Police (2006) “Protecting Civil Rights: A Leadership Guide for State, Local, and Tribal Law Enforcement.” available at: <http://www.cops.usdoj.gov/files/ric/Publications/e06064100.pdf>
http://www.theiacp.org/documents/pdfs/RCD/PCR_LdrshpGde_Part3.pdf.

Initial Privacy and Civil Liberties Analysis

are at least as comprehensive as those required of federal agencies participating in the ISE under the ISE Privacy Guidelines.

- a. As highlighted throughout this analysis, paragraph 11 of the ISE Privacy Guidelines reflects that non-federal entities, to participate in the ISE, must “develop and implement appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in these [ISE Privacy] Guidelines.” The ISE-SAR Evaluation Environment sites that anticipate receiving information from federal entities (e.g., fusion centers and some local agencies) should designate a “privacy official” to coordinate review of existing policies and adoption of ISE-SARs policy and to oversee ISE-SARs privacy policy implementation. (See Q&A #13.)
- b. To evaluate whether their terrorism-related information sharing operations appropriately consider the information privacy and legal rights of Americans, ISE-SAR Evaluation Environment sites should review their privacy and civil liberties policies and related training. To this end, ISE-SAR Evaluation Environment sites should be encouraged to consult the Global’s templates for privacy policy development and the *Guide to Conducting Privacy Impact Assessments for State and Local Information Sharing Initiatives (DRAFT)*²¹. (See Q&A #19.)
- c. Federal entities documenting suspicious activities should be mindful that most Detailed ISE-SARs contain protected information subject to the requirements of the ISE Privacy Guidelines. Accordingly, federal entities that share Detailed ISE-SARs must ensure that protected information in ISE-SAR systems and ISE Shared Spaces is protected consistent with ISE Privacy Guidelines and with the requirements of federal privacy law. Likewise, federal entities documenting suspicious activities must do so consistent with civil rights and civil liberties requirements and should employ mechanisms affording the necessary protections. See, e.g., United States Department of Justice, Civil Rights Division (2003), “Guidance Regarding the Use of Race in Law Enforcement Agencies.”²² (See Q&A #28.)

3. Develop and Provide Appropriate Training and Documentation:

- a. Recommend training and guidance documentation on how to apply the criteria in Part B of the ISE-SAR Functional Standard to minimize the risks of over-inclusiveness and inappropriate reporting (See Q&A #4);
- b. Recommend program documentation supporting the ISE-SAR Evaluation Environment (CONOPS, participation agreements, etc.) require ISE-SAR Evaluation Environment sites to obtain assurances from source agencies that all personnel (e.g., front line

²¹ The *Guide to Conducting Privacy Impact Assessments for State and Local Information Sharing Initiatives* was developed by Global’s Privacy and Information Quality Working Group. At the time of this writing, the document is under final review and is on the agenda for the Global Justice Advisory Committee October 2008 meeting.

²² United States Department of Justice, Civil Rights Division (2003), “Guidance Regarding the Use of Race in Law Enforcement Agencies” document is available at http://www.usdoj.gov/crt/split/documents/guidance_on_race.htm

Initial Privacy and Civil Liberties Analysis

personnel, senior and expert officers, investigators/analysts) involved in the gathering, processing, reporting, analyzing, and sharing of suspicious activity information have been trained on the ISE-SAR Functional Standard criteria (See Q&A #4); the ISE-SAR business process and information flow; and on the privacy and civil liberties implications of suspicious activity reporting (e.g., constitutional and other legal protections). (See application of the ISE Privacy Guidelines in the ISE-SAR context (see Q&A #28) and U.S. person-related collection limitations (see Q&A #19).)

- c. The grantor agency should formally obtain participants' agreement to comply with the terms and requirements of the initiative as reflected in the CONOPS and other program implementation guidance. (Best practice.)
- d. Applicable documentation should be revised to clarify meaning of "illicit activity," (see Q&A #1) and to otherwise be consistent with the recommendations in this Analysis).
- e. Recommend that agencies participating in the ISE-SAR Evaluation Environment develop privacy and civil liberties protection policies and guidance documentation that is designed to accompany, complement, and/or be integrated with its SAR documentation and guidance.

C. Initiating the ISE-SAR Evaluation Environment Effort

As an initial matter, the authors of this report recommend the following steps:

1. ISE-SAR Evaluation Environment sites should develop or adopt and implement robust privacy, civil rights, and civil liberties protection policies for all its information collection, use, storage, and sharing activities (best practice).

In particular, the CONOPs should require that participating fusion centers adopt an umbrella ISE-SARs Evaluation Environment Privacy and Civil Liberties Protection Policy or evaluate and, if necessary, update their existing privacy and civil liberties policy to ensure that the gathering, documenting, processing, and sharing of ISE-SARs is consistent with the umbrella policy. The CONOPs will also require each participating site to document the manner in which the ISE-SAR information is being posted and shared via the Shared Space and how the site is complying with its ISE-SAR privacy and civil liberties protection policy. (See general discussion preceding Privacy and Civil Liberties Analysis).

2. ISE-SAR Evaluation Environment sites will save Detailed ISE-SARs to the Shared Space, but until adequate privacy and civil liberties policies are in place, the results to an ISE-SAR search will be viewable only without the privacy fields (see Q&A #14).
3. ISE-SAR Evaluation Environment initiative sites should document steps taken to address the recommendations and key issues outlined in this analysis; this documentation will assist the authors of this report in evaluating whether the use of the

Initial Privacy and Civil Liberties Analysis

Detailed IEPD is appropriate and to develop a final ISE-SAR Privacy and Civil Liberties Analysis of the ISE-SAR Functional Standard, IEPD and ISE-SAR Evaluation Environment initiative (best practice).

D. PGC's Legal Issues Working Group Participation

As the ISE-SAR Functional Standard deploys to the field through the ISE-SAR Evaluation Environment initiative, the PM-ISE will enlist the assistance of the PGC's Legal Issues Working Group to ensure that participating entities receive ongoing advice and guidance with respect to protecting information privacy, civil rights, and other civil liberties. The PGC's Legal Issues Working Group will identify one or more subject matter experts to serve in an advisory capacity to the ISE-SAR Steering Committee, which in turn will deploy these experts to the ISE-SAR Evaluation Environments for field visits, consultations, and training.

Conclusion

The ISE-SAR Evaluation Environment contemplates an iterative process involving phased implementation of the ISE-SAR Functional Standard and IEPDs in diverse operating environments and continuous reexamination of the assumptions, processes, and standards for designating and sharing ISE-SARs. The authors of this report will advise the relevant ISE-SAR project committees on an ongoing basis and participate in the review and evaluation of site activities.

[REDACTED]

From: German, Michael [REDACTED]
Sent: Friday, January 16, 2009 6:13 PM
To: [REDACTED]
Subject: SAR meeting
Attachments: Suspicious Activity Examples.docx

Hi [REDACTED]

Thanks again for arranging the meeting last Wednesday. You asked for specific examples of incidents where suspicious activity collection resulted in over-zealous police behavior. Attached is a list we compiled in preparing our fusion center report update. Each incident is footnoted for your convenience in evaluating them. If you would like more, let me know.

Photography seems to be the most obviously abused. Here are links to stories about photographers being harassed by authorities:

<http://www.stationstops.com/2008/03/18/mta-ignored-by-employees-after-insisting-do-not-harass-photographers/>

<http://digital-photos.tribe.net/thread/2438792b-5031-464b-97c6-d51d81983882>

http://seattletimes.nwsourc.com/html/localnews/2001979027_locks14m.html

And here are links to websites I mentioned encouraging people to take pictures of "infrastructure" to frustrate security efforts:

<http://lightchasersphotography.com/blog/how-to-shoot-photographs-like-a-terrorist/>

<http://www.boingboing.net/2005/07/28/no-taking-pix-of-san.html>

I will send you a list of specific concerns with language on the criteria and privacy fields in the Functional Standards by next Friday (I've reached out to the other groups to incorporate any specific concerns they might have and I want to give them a little time to get back to me).

Have a nice weekend.

Best,

Mike <<Suspicious Activity Examples.docx>>

Michael German

Policy Counsel

American Civil Liberties Union

Washington Legislative Office

915 15th Street, NW

Washington, DC 20005

[REDACTED]

Taking video footage

- Sheriff's deputies in Texas stopped an Al-Jazeera television crew that was filming on a public road more than a mile away from a nuclear power plant and conducted "extensive background checks" on them. The police said they "found no criminal history or other problems."ⁱ

Taking pictures

- Mariam Jukaku, a 24-year old Muslim-American journalism student at Syracuse University, was stopped by Veterans Affairs police in New York for taking photographs of flags in front of a VA building as part of a class assignment. After taking her into an office for interrogation and taking her driver's license the police deleted the photographs from her digital camera before releasing her.ⁱⁱ
- Shirley Scheier, a 54-year-old artist and Associate Professor of Fine Art at the University of Washington was stopped by police in Washington State for taking pictures of power lines as part of an art project. Police frisked and handcuffed Scheier, and placed her in the back of a police car for almost half an hour. She was eventually released, after officers photographed maps that Scheier used to find the power station. The officers also told her she would be contacted by the FBI about the incident.ⁱⁱⁱ
- Neftaly Cruz, a 21-year-old senior at Penn State, was arrested in his own backyard in Philadelphia for snapping a picture of police activity in his neighborhood with a cell phone camera. He was taken down to the police station where police threatened to charge him with conspiracy, impeding police, and obstruction of justice, but he was later released without charge.^{iv}

Expressing political and religious beliefs

- After making public comments criticizing the FBI's treatment of Muslims in Pittsburgh, Dr. Moniem El-Ganayni, a nuclear physicist and naturalized American citizen had his security clearance improperly revoked by the U.S. Department of Energy (DOE) despite 18 years of dedicated service. Though they never told him the reason his clearance was revoked, during seven hours of interviews, representatives from the DOE and the FBI never alleged a breach of security but instead questioned El-Ganayni about his religious beliefs, his work as an imam in the Pennsylvania prison system, his political views about the U.S. war in Iraq, and the speeches he'd made in local mosques criticizing the FBI.^v
- According to documents released in response to an ACLU lawsuit, the Maryland State Police (MSP) used undercover officers to spy on non-violent peace activists and anti-death penalty groups. The undercover agents consistently reported that the activists acted legally at all times, yet the investigations continued for over 14 months. Information about the groups' political activities gathered during the investigations "was shared with seven different agencies, including the National Security Agency and an un-named military intelligence official."^{vi} A longtime peace activist who was an apparent target of

the surveillance, Max Obuszewski, had his identifying information entered into a federal database under the “primary crime” heading of “Terrorism - anti-government,” even though absolutely no violent activity was even alleged in the reports.^{vii}

- A plain-clothes Harvard University detective was caught photographing people at a peaceful protest for “intelligence gathering” purposes.^{viii} HUPD officers are sworn special State Police officers with deputy sheriff powers, and they often work “in conjunction with other agencies, including the Massachusetts State Police, Boston Police, Cambridge Police, Somerville Police, and many federal agencies.”^{ix} A university spokesman refused to say what the HUPD does with the photographs it takes for “intelligence gathering” purposes, so it is unknown whether this information was shared with the CFC.

Taking measurements

- A Middle Eastern man in traditional clothing sparked a three-day police manhunt in Chicago when a passenger on the bus he was riding notified the police that he was clicking a hand counter during the trip. A Joint Terrorism Task Force investigation into the episode revealed he was using the counter to keep track of his daily prayers, a common Muslim practice.^x

ⁱ Heather Menzies, *Deputies Question Al Jazeera Film Crew*, BAY CITY TRIBUNE, June 3, 2008, available at <http://www.baycitytribune.com/story.lasso?ewcd=f84a0eb52a0424a>.

ⁱⁱ Matthew Rothschild, *VA Police Delete Photographs Taken by Muslim-American Journalism Student*, THE PROGRESSIVE, September 17, 2007, available at http://www.progressive.org:80/mag_mc091707.

ⁱⁱⁱ American Civil Liberties Union of Washington State, *Art Professor Detained for Taking Photos on Public Property*, November 15, 2007, <http://www.aclu-wa.org/detail.cfm?id=787>.

^{iv} NBC10.COM, *Cell Phone Picture Called Obstruction of Justice*, <http://www.nbc10.com/news/9574663/detail.html> (last visited July 11, 2008).

^v Press Release, American Civil Liberties Union, *Government Revoked Muslim Nuclear Physicist’s Security Clearance To Retaliate For Criticism Of U.S. Policy, Says ACLU* (June 26, 2008) (on file with author), available at <http://www.aclu.org/freespeech/gen/35789prs:20080626.html>.

^{vi} Shaun Waterman, *Documents Show Md. Police Spied on Anti-War, Death Penalty Protestors*, United Press International, Jul. 17, 2008, available at: http://www.upi.com/Emerging_Threats/2008/07/17/Documents_show_Md_police_spied_on_anti-war_death-penalty_protestors/UPI-74771216337696/

^{vii} American Civil Liberties Union of Maryland press release, *ACLU of Maryland Lawsuit Uncovers Maryland State Police Spying Against Peace and Anti-Death Penalty Groups*, July 17, 2008, available at: http://www.aclu-md.org/aPress/Press2008/071708_PeaceGroups.html

^{viii} David Abel, *ACLU Queries Harvard’s Police*, BOSTON GLOBE, April 15, 2008, http://www.boston.com/news/education/higher/articles/2008/04/15/aclu_queries_harvards_police/.

^{ix} Harvard University Police Department website, http://www.hupd.harvard.edu/about_hupd.php.

^x Guy Lawson, *The Fear Factory*, ROLLING STONE, Feb. 7, 2008m at 61, 64, available at http://www.rollingstone.com/politics/story/18137343/the_fear_factory.

From: [German, Michael](#)
To: [REDACTED]
Subject: Comments on Functional Standard
Date: Friday, January 23, 2009 4:42:50 PM

Hi [REDACTED]

The following remarks are in response to your request for informal comments on possible amendments to the Information Sharing Environment Functional Standard for Suspicious Activity Reporting (Version 1.0). I understand that a meeting will be scheduled with other privacy and civil liberties organizations to discuss these issues in the coming weeks, but the ACLU offers these suggestions in the interim so that you may consider them as you begin reviewing the criteria guidance and privacy fields.

As you know, the ACLU is concerned that the behaviors described in the ISE-SAR Criteria Guidance (Part B, page 27) are overbroad and will result in unnecessary law enforcement interaction with innocent persons and the inappropriate collection and dissemination of personal information. The document unfortunately sets a tone for such over-collection in the definition of "Suspicious Activity Report," which includes "behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention." The initial part of the definition is unnecessarily hypothetical and disconnected from an appropriate legal standard that would authorize the collection of criminal intelligence information, and the last phrase, "or other illicit intention," suggests information not related to criminal activity may be collected. The ISE Initial Privacy and Civil Liberties Analysis states that the word "illicit" in the SAR definition was intended to mean "illegal," and that a nexus to criminal activity or intent must be demonstrated to initiate a SAR. This would mean that the final phrase is redundant. We suggest amending the definition of a SAR to "behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity."

The Criteria Guidance itself is problematic because it lists innocuous, innocent, and First Amendment-protected activity alongside obviously criminal activity, with no distinction requiring additional facts to report the former. The combined effect of the inclusion of noncriminal activity both in specific behaviors and in the definition of a SAR is to suggest that SAR investigations operate under a different set of rules than ordinary criminal investigation by local law enforcement. Nothing would dispel that suggestion more easily than a plain statement to the contrary. Accordingly, we recommend including in the "Purpose" or "Scope" sections an explicit statement that the same constitutional standards apply to local law enforcement officers conducting SAR inquiries as would apply when conducting ordinary criminal investigations and nothing in the guidance should be taken to suggest otherwise.

Several behaviors listed in the Criteria Guidance, eliciting information, acquisition of expertise, photography, and observation (which is repeated as “surveillance”), are innocuous, innocent and First Amendment-protected activities and the accompanying descriptions of these behaviors do not include facts that would lead a reasonable law enforcement officer to suspect criminal activity. Other listed behaviors, such as breach/attempted intrusion, misrepresentation, theft/loss/diversion, sabotage/tampering/vandalism, cyber attack, and expressed or implied threats, on the other hand, do suggest obviously criminal activity. The remaining behaviors, testing of security, flyover, materials acquisition/storage, weapons discovery and recruiting, include language in their descriptions that could indicate either criminal or non-criminal behavior. Lumping these behaviors together, without distinction between them or further description, seems to equate these activities under the same umbrella of suspicion, which will likely lead to inappropriate contact and collection, including racial and/or religious profiling as officers use their own discretion to decide what “photography” might suggest possible terrorist activity. We suggest listing the obviously criminal activity first, so they stand out in matter of importance. The behaviors that could be criminal or non-criminal should be listed second, with more detailed descriptions that emphasize the necessity for facts raising a suspicion of criminality before reporting is appropriate. Finally, the First Amendment-protected activities should be either removed from this section entirely, or set forth in a manner that makes clear the activity itself is innocuous and should not be reported absent other facts and circumstances that would create a reasonable suspicion of criminality (including evidence of pre-operational planning related to terrorism). A clarification that race and religion should not be considered as factors that create reasonable suspicion (except if used as specific suspect descriptions) would also help stem potential abuses.

As I suggested in the meeting, it may also be appropriate to include a new section that describes an incremental approach to the SAR process where particular facts might trigger a certain limited response, such as 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 level of inquiry and possibly the filing of a SAR. Some discussion of the *Terry v. Ohio* stop-and-frisk standards might be appropriate as well. Unusual observed behavior that does not justify a stop or even a request for identifying information could always be reported as an incident without including personally-identifiable information.

Regarding the privacy fields, the ACLU is concerned that the privacy fields identified in the Functional Standards document would allow information that could be used to trace or distinguish a particular individual to be included in “Summary” SARs. The ISE Initial Privacy and Civil Liberties Analysis recommends that CONOPS prohibit agencies from “reverse

engineering” summary SARs to identify individuals, but it would be better designate all fields that could be used to trace or distinguish an individual as privacy fields. These would include most particularly the date of birth field, and all date of issue/date of expiration fields for particular personal identification documents (rather than the specific dates perhaps the year of birth and year of issue/expiration of documents would suffice). The Aircraft fields do not designate Aircraft ID numbers or tail numbers as privacy fields, when this information could clearly identify the owner/registrant (it should be noted that Vehicle Identification Numbers and DOT registration information for vehicles are designated as privacy fields). Similarly there are specific fields regarding addresses that in particular situations could identify the subjects if they are residents of that address. These fields should be designated as privacy fields so that no information in a summary SAR could possibly be used to trace or distinguish a particular individual.

Thanks for the opportunity to submit these comments and I look forward to meeting with you on these issues again soon.

Best,

Mike

Michael German

Policy Counsel

American Civil Liberties Union

Washington Legislative Office

915 15th Street, NW

Washington, DC 20005

[REDACTED]

[REDACTED]

From: [John Wilson](#)
To: [REDACTED]
Cc: [REDACTED]
Subject: Tips and Leads Issue Paper
Date: Tuesday, February 10, 2009 3:11:57 PM
Attachments: [Tips and Leads Issue Paper 10.07.pdf](#)

Mike,

Attached, as promised at our January 14, 2009, meeting at PM-ISE, is the subject Tips and Leads Issue Paper.

John
John J. Wilson
Senior Research Associate
Institute for Intergovernmental Research
Phone:

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]



Tips and Leads Issue Paper

Global Justice Information Sharing Initiative
◆
Intelligence Working Group
◆
Privacy Committee

October 2007



Tips and Leads Issue Paper

Introduction and Background

The events of September 11, 2001, like no others, have made the average American aware that law enforcement, public safety, and private sector agencies should collect and share information to make our country a safer place for all its citizens and visitors. Conversely, the public is concerned about what types of information are being collected and stored by law enforcement, and when and how that information is being used and shared, raising concerns about the potential for civil liberty and privacy abuses.

Law enforcement officials require an array of information to effectively detect and investigate criminal and terrorism activity. Information comes to law enforcement agencies through a number of horizontal and vertical channels (e.g., dispatch, criminal investigations, the public, other law enforcement agencies, arrests, and incident reports), and many standards have been established for its maintenance and use. Unfortunately, not all information fits neatly into an already established category. In many cases, it is unclear whether information is useable or meaningful, requiring law enforcement officials to further investigate, analyze, and evaluate the data to determine its accuracy and potential usefulness. Currently, state, local, and tribal agencies lack the guidance and standards for this “gray area” of information.

In furtherance of the recommendations in the *National Criminal Intelligence Sharing Plan*¹ (NCISP), the Privacy Committee of the Global Intelligence Working Group (GIWG) developed this issue paper to provide guidance to state, local, and tribal law enforcement agencies regarding the handling of information received as a result of tips, leads, and suspicious incidents.

The NCISP emphasizes that credible information can result only from information that has been evaluated and used to draw conclusions. Yet it recognizes that the collection and use of such information can affect the fundamental rights of individuals. The NCISP offers an effective approach to protecting privacy and civil liberties by supporting training and policies that eliminate unnecessary discretion in the decision-making process. The GIWG Privacy Committee strongly supported this approach when developing guidance for handling tips and leads data.

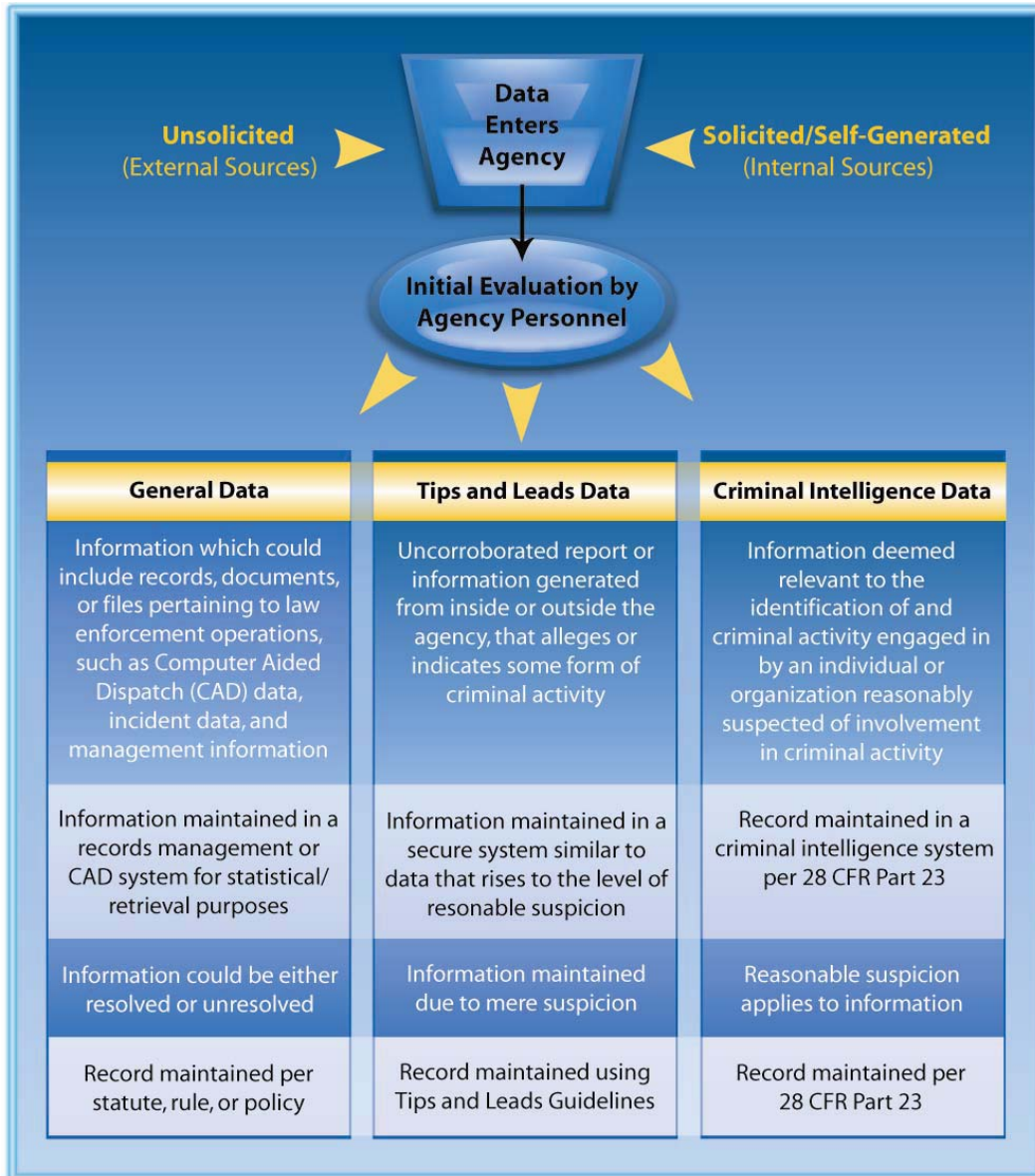
Tips and leads data are not criminal intelligence as defined by 28 Code of Federal Regulation (CFR) Part 23. However, law enforcement officials recognize the need to protect this type of information and protect individuals’ privacy and civil liberties. Accordingly, this issue paper was prepared to provide guidelines on collecting, maintaining, retaining, disseminating, and purging

¹ Recommendation 9 of the *National Criminal Intelligence Sharing Plan* states that “in order to ensure that the collection/submission, access, storage, and dissemination of criminal intelligence information conforms to the privacy and constitutional rights of individuals, groups, and organizations, law enforcement agencies shall adopt, at a minimum, the standards required by the Criminal Intelligence Systems Operating Policies Federal Regulation (28 CFR Part 23), regardless of whether or not an intelligence system is federally funded.”

tips, leads, and suspicious incident information. As recommended in the NCISP, agencies should develop privacy policies incorporating the guidance provided herein.

Law Enforcement Information Production

Information received by law enforcement agencies can be categorized into three general areas, as depicted in the diagram below:



Common practice involves the validation of information by agency personnel upon receipt. Data is categorized as unsubstantiated or uncorroborated after attempts to validate or

determine the reliability of the information fail (middle column above). Frequently, the agency feels the information should be kept for potential connections in the future but does not know how the data should be handled, where it should be stored, or when it should be disseminated.

An agency's privacy policy should . . . acknowledge and address important issues that currently are not included in some criminal intelligence policies. For example, the policy should acknowledge the existence of information that is received or possessed by law enforcement agencies that does not rise to the level of "reasonable suspicion of criminal activity" and provide guidance on how to process that information. Often, this information—sometimes referred to as a "temporary" or "working" file—is received unsolicited by law enforcement agencies and cannot simply be dismissed.²

It is this type of temporary or working-file information—commonly known as tips and leads information—that is addressed in this issue paper.

The Importance of State, Local, and Tribal Involvement in the National Information Sharing Environment

As previously indicated, law enforcement agencies deal with tips, leads, and suspicious data on a daily basis. Although this information in and of itself may not be indicative of a potential crime, when collated and analyzed with correlating pieces of data from other sources, the information may be key in the prevention of a criminal act, including a potential act of terrorism. It is imperative that state, local, and tribal line-level officers realize the vital role they play in the preliminary receipt and investigation of this information and the potential impact it may have on an ongoing criminal or terrorism investigation.

As acknowledged in the *Information Sharing Environment (ISE) Implementation Plan*, the needs of state, local, and tribal governments continue to mount as these governments incorporate counterterrorism and homeland security activities into their day-to-day missions. Specifically, they need to ensure that personnel protecting local communities from a terrorist attack—or responding to an attack—have access to timely, credible, and actionable information and intelligence regarding individuals and groups intending to carry out attacks within the United States (including homegrown terrorists), their organization and financing, at-risk potential targets, preattack indicators, and other major events or circumstances requiring action by state, local, and tribal governments.³

The federal government is promoting the establishment of a nationwide integrated network of state and major urban area fusion centers to facilitate effective terrorism information sharing with state, local, and tribal law enforcement agencies, and as of August 2007, more than 40 states have created fusion centers. The principal role of the fusion center is to compile, analyze, and disseminate criminal and terrorist information and intelligence, as well as other

² NCISP, page 6.

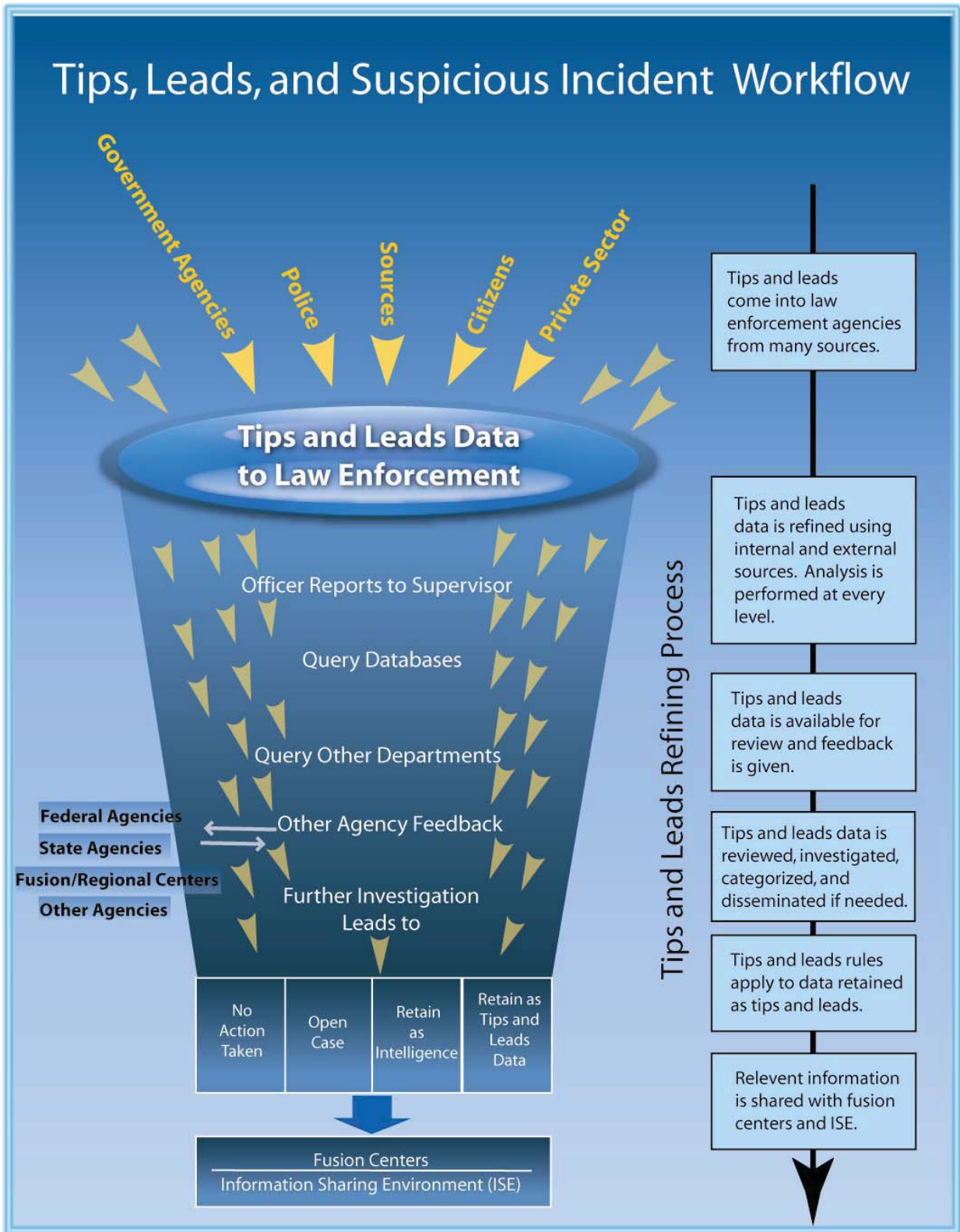
³ Information Sharing Environment Implementation Plan, November 2006, page 18.

Global Justice Information Sharing Initiative ♦ Intelligence Working Group ♦ Privacy Committee

information, to support efforts to anticipate, identify, prevent, and/or monitor criminal and terrorist activity. Consistent with their respective roles and responsibilities, the federal government will provide terrorism information to state, local, and tribal authorities primarily through these fusion centers. Conversely, the ISE Implementation Plan indicates that statewide and major area fusion centers will ensure that locally generated terrorism information is communicated to the federal government.⁴

It may be difficult to determine whether a single incident occurring within a local jurisdiction has a nexus to terrorism, but it is important to acknowledge that many outwardly unrelated tips, leads, and suspicious incidents may in fact be related and could have multijurisdictional and national implications when analyzed, shared, and combined with other seemingly unrelated information at the local, state, regional, and federal levels. Terrorist activities are being funded via local-level crimes, and state, local, and tribal law enforcement officers in our communities are best positioned not only to observe criminal and other activity that might be the first signs of a terrorist plot but also to help thwart attacks before they happen. The following graphic depicts a suggested workflow process for tips, leads, and suspicious data as it enters an agency. It outlines a refining process that includes assessment, analysis, review, categorization, and dissemination, if appropriate, to local, state, regional, and federal agencies and fusion centers in furtherance of the national information sharing environment.

⁴ Ibid. Page 75, Chapter 7, Implementation Action 2.21.



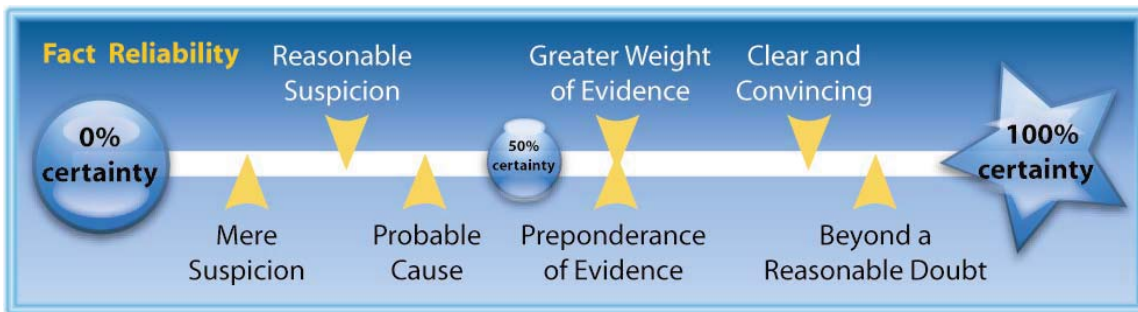
The GIWG Privacy Committee recommends that every state, local, and tribal law enforcement agency should incorporate a tips, leads, and suspicious incident refining process into its daily operations and provide appropriate training for personnel involved in the process.

Definition of Tips and Leads

The GIWG Privacy Committee defines tips and leads information as an uncorroborated report or information that alleges or indicates some form of possible criminal activity. Tips and leads can also be referred to as suspicious incident reports (SIRs) or suspicious activity reports (SARs). Tips and leads information does not include incidents that do not have an offense attached, criminal history records, records management data, or Computer Aided Dispatch (CAD) data.

A tip or lead can result from a variety of sources including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information has some suspicion or mere suspicion attached to it, but without further inquiry or analysis it is unknown whether the information is accurate or useful. Unlike intelligence information that has undergone an evaluation process to determine the likely possibility that the information is accurate, tips and leads information hangs between being of no use to law enforcement and being extremely valuable if time and resources are available to determine its meaning.

Across a spectrum for levels of suspicion, information ranges from no suspicion to fact. Mere suspicion information (tips and leads) falls short of any established national standards used by law enforcement.



Each agency must make a determination of the types of data that will be categorized as tips and leads. The criteria for collecting and labeling information as a tip or lead should be clearly articulated in each agency’s privacy policy. Following are specific areas that should be addressed when developing a privacy policy that incorporates tips and leads data:

Collection

Tips, leads, and suspicious incident data are collected in a variety of ways. They can be received or obtained through unsolicited information that the public provides; from confidential/anonymous sources; from the media and other law enforcement, public safety, or regulatory agencies; or from analysis of information. Tips and leads data can also be solicited

or self-generated information, received from the public in response to law enforcement officers' requests for information about a certain crime. However the information is received, it has not been validated for truthfulness, accuracy, or reliability of the source—determinations that aid law enforcement in deciding whether the information is credible and has value.

Controls

Similar to the intelligence process detailed in the NCISP,⁵ tips and leads information should be subjected to an assessment process to determine its credibility and value. The GIWG Privacy Committee determined that appropriate controls should be recommended for each step of that process:

Receipt/Collection—At the time of receipt or collection, tips and leads data should be assessed and reviewed, using supporting information if available, for sensitivity and confidence. An attempt should be made to validate or refute the information provided by a tip or lead. Collection of purely First Amendment activity information should be prohibited.

Storage—Storage of tips and leads information should be handled similarly to data that rises to the level of reasonable suspicion. Those requirements should include an audit and inspection process, supporting documentation, and logical separation or labeling of the data from other information.

Access—Because of the uncertainty about what the information says or how credible it is, it is recommended that access to tips and leads data should be handled similarly to access to data that rises to the level of reasonable suspicion. Access should be allowed only where there is a need to know and a right to know the information in the performance of a law enforcement, homeland security, or public safety activity. Law enforcement agencies may want to implement a process whereby access is role-based.

Dissemination—Tips and leads information, if systematically collected and stored for interagency distribution, should be disseminated primarily in response to an inquiry, and only for law enforcement, homeland security, and public safety purposes. For example, uncorroborated tips and leads information should not be regularly disseminated in bulletins and other like products. However, it may be included in secure information databases and disseminated to relevant law enforcement, homeland security, and public safety agencies that have the need to know and right to know the information in the performance of a law enforcement activity and to such agencies and other government or nongovernment organizations or individuals when credible information indicates potential imminent danger to life or property.

⁵ Intelligence Process graphic, NCISP, page 3.

Retention—The retention period for tips and leads information should be long enough for an agency to work a tip and lead to determine its credibility and value. Agencies may consider articulating the need to retain tips, leads, or suspicious incidents for longer periods of time to access and conduct analysis on the data for national security purposes. Tips and leads should have a “disposition” label so an inquirer knows the status and purpose for the retention. Disposition labels might include “undetermined/unresolved” or “cleared/unfounded.” Different disposition labels may indicate different retention periods, with “cleared/unfounded” tips and leads information being retained for a shorter time than “undetermined/unresolved” tips and leads. Agencies should also consider the need for maintaining tips and leads data for purposes of statistical reporting and performance measurement when setting retention and purge procedures.

Security—It is recommended that physical and electronic security measures be similar to those used for information rising to the level of reasonable suspicion.

Current Efforts and Promising Practices

The information below describes three current efforts that address a process for handling tips and leads information:

- **U.S. Attorney General’s Guidelines on General Crimes, Racketeering, and Terrorism Enterprises** (Attorney [AG] Guidelines) (U.S. Department of Justice [DOJ], 2002) offer one model for authorized information gathering in response to tips and leads information. The AG Guidelines recognize three levels of investigative activity: (1) the “prompt” and “extremely limited” (neither of which is further defined in the Guidelines) checking of initial leads, (2) preliminary inquiries, and (3) full investigations.

The **checking of initial leads** is undertaken whenever *information is received of such a nature that some follow-up as to the possibility of criminal activity is warranted*. This is a limited activity conducted with an eye toward determining whether further investigation is warranted. The next level, a **preliminary inquiry**, is undertaken when the information developed or the nature of the information received (reliable source, imminent threat) indicates *the possibility of criminal activity* and whose *responsible handling requires some further scrutiny* beyond checking initial leads. Mail opening and nonconsensual electronic surveillance are prohibited investigative techniques in the checking of initial leads or the conduct of a preliminary inquiry. They also require supervisory approval, written documentation of the allegation or other information that is deemed to warrant the approval, and completion within 180 days, with no more than two extensions of up to 90 days available with approval of the Special Agent in Charge. Any further approvals of extensions are subject to Federal Bureau of Investigation (FBI) headquarters approval. Where the checking of initial leads fails to disclose sufficient information to justify a preliminary inquiry or an investigation or a preliminary inquiry fails to disclose sufficient

information to justify an investigation, activity on the case must be immediately terminated and a record made of the closing.

Where a checking of initial leads or a preliminary inquiry produces *facts or circumstances that reasonably indicate that a federal crime has been, is being, or will be committed*, a **general crimes (full) investigation** may be initiated using the full panoply of lawful investigative techniques. Parallel standards are used to authorize criminal intelligence and racketeering enterprise investigations. All investigations must be based on a *reasonable factual predicate* and have a *valid law enforcement purpose*. In determining reasonable indication, the agent may take into account facts or circumstances that a prudent investigator would consider. There must be an objective, factual basis for initiating the investigation (more than a hunch but less than reasonable suspicion or probable cause).

Finally, the AG Guidelines permit information collected during the checking of initial leads, preliminary inquiries, and investigations to be disseminated freely within the DOJ and to state, local, and federal criminal justice agencies when the information: (1) falls within the investigative or protective jurisdiction or litigative responsibility of the agency; (2) may assist in preventing a crime or the use of violence or any other conduct dangerous to human life; or (3) is required to be furnished by Executive Order, statute, interagency agreement, or Presidential Directive. (These criteria reflect basic need-to-know and right-to-know standards). The FBI maintains a database that permits prompt retrieval of information on the status (open or closed) and subjects of all inquiries and investigations.

- **Georgia Information Sharing and Analysis Center (GISAC)** method for handling tips, leads, and suspicious incident data is a comprehensive refining process that details how multiple agencies can work together to address and properly handle this type of data.

Receipt of Leads/Tips: GISAC receives tips from law enforcement agencies via the Georgia Terrorism Tip-Line, a joint GISAC and Federal Bureau of Investigation (FBI) call center, and through calls directly to agents assigned to GISAC. Through the Georgia Terrorism Intelligence Project (GTIP), GISAC receives and disseminates lead information through a direct link to 11 other local law enforcement agencies in the metro-Atlanta area, and throughout the state via a Web-based lead tracking system called E-Team. To aid in deconfliction between GISAC and the Atlanta FBI, GISAC provides the FBI with access to E-Team, through which the FBI monitors all GISAC leads and enters any leads from its Guardian system.

As a matter of design, GISAC chose to educate and include other state and local law enforcement agencies in collecting threat/suspicious activity information by obtaining identifiers and other pertinent details and reporting the information to GISAC. Personnel at GISAC ensure that the information is evaluated, investigated, and forwarded where it needs to go for additional investigation or prosecution. All identified individuals are checked through state and local databases as well as through the FBI's intelligence system. In

Global Justice Information Sharing Initiative ♦ Intelligence Working Group ♦ Privacy Committee

addition, GISAC ensures that the law enforcement officers who provide the information receive follow-up calls with results of the tips or leads, even if the results are negative. GISAC takes calls from the public but does not advertise a public telephone number for reporting suspicious activity. This procedure is followed for a couple of reasons:

- 1) Local 911 services and police agencies will most likely receive calls first. If a call is regarding an emergency or if immediate action is required, local authorities are in a position to address the situation.
- 2) When citizens call 911, the local police authorities are included in the information flow. Local officers are closer to the community and know whether something is normal or unusual.

Through education, police agencies and/or 911 centers are advised to call GISAC with suspicious information, no matter how nonthreatening it may seem. GISAC collects the information and evaluates it. Citizens are able to report suspicious activity online through the Georgia Office of Homeland Security's Web site. They are clearly instructed to call 911, or the caller's local law enforcement agency, for reports requiring immediate attention.

Documentation of Leads: Each tip or lead received by GISAC is recorded into E-Team and assigned for follow-up by a GISAC supervisor. Leads may be assigned to a GISAC agent, tasked out to a Georgia Bureau of Investigation (GBI) regional office, or sent to an intelligence analyst for further review and to assess the credibility and significance of the information. All leads received by GISAC are reported to the FBI/Joint Terrorism Task Force (JTTF) to aid in deconfliction and to determine whether the leads warrant FBI/JTTF involvement.

After a lead is assigned to an agent, the appropriate investigative measures are taken to proceed with the lead. If further intelligence information is needed, the agent contacts an analyst assigned to GISAC for assistance. GISAC has six criminal intelligence analysts, one analyst from the Georgia Department of Corrections, and two Georgia Emergency Management Agency representatives dedicated solely to the homeland security mission. Analysts have access to various databases including the Georgia Department of Labor, Secretary of State, Georgia Crime Information Center, and Georgia Department of Revenue. In addition, all analysts have access to public records, FBI intelligence indices, and GBI intelligence systems. Throughout this process, all activity and intelligence checks conducted by agents and analysts are recorded in E-Team for documentation. Intelligence data is not entered onto E-Team because of its wide accessibility; instead it is delivered directly to the agent assigned to the lead. The assigned agent updates the lead and passes it on to a GISAC supervisor, who decides whether the lead can be closed with no further investigation or warrants opening a full investigation. Tips and leads that are opened to investigation are recorded in FBI and/or GBI case management systems as case or intelligence investigations. Information that is compliant with 28 CFR Part 23 is also recorded in GBI's intelligence

system. All tips and leads recorded into E-Team, even closed leads, are archived within E-Team and are available for retrieval or queries for future relevance.

Dissemination of Leads: All agencies with access to E-Team are able to review updates to tips and leads as they are developed. If dissemination outside the agencies with access to E-Team is required, GISAC will determine the target audience and develop a report accordingly. GISAC and FBI work jointly on these products to ensure that all information that can be disseminated is shared.

- Florida’s Intelligence System’s Operating Guidelines:** State laws and policies are likely to significantly affect how tips and leads and other investigative information are received, investigated, stored, and disseminated. Dissemination must consider the right of the public under State Sunshine Laws to obtain information in public records that pertains to them. A good example is **Florida’s Public Records Statute** (Chapter 119, Sections 119.01–119.19, 2004). The statute broadly defines *criminal intelligence information* to mean “information with respect to an identifiable person or group of persons collected by a criminal justice agency in an effort to anticipate, prevent, or monitor possible criminal activity” (Sec. 119.011 (3) (a)). *Criminal investigative information* is defined to mean “information with respect to an identifiable person or group of persons compiled by a criminal justice agency in the course of conducting a criminal investigation of a specific act or omission, including, but not limited to, information derived from laboratory tests, reports of investigators or informants, or any type of surveillance” (Sec. 119.011 (3) (b)). Section 119.07 (6) (b) 1 exempts “active” criminal intelligence information and “active” criminal investigative information from the law’s public inspection and copying requirements. The statute defines *criminal intelligence information* as “active as long as it is related to intelligence gathering conducted with a reasonable, good faith belief that it will lead to detection of ongoing or reasonably anticipated criminal activities” and *criminal investigative information* as “active as long as it is related to an ongoing investigation which is continuing with a reasonable, good faith anticipation of securing an arrest or prosecution in the foreseeable future” or where “directly related to pending prosecutions or appeals” (Sec. 119.011 (6) (d) 1 and 2). This statutory scheme is carefully reflected in the **Florida Intelligence System’s Operating Guidelines** (Florida Guidelines) (May 2005), including the treatment of tips and leads information. The Florida Guidelines establish a dissemination protocol in Part IV.I that must be followed to disseminate system information to other members of the criminal justice community, including need to know/right to know and a detailed procedure for “third agency” dissemination under a “Third Agency Rule.” One system information module, for tips and tasks, is used to capture the tips and leads received by law enforcement agencies. This information must be reviewed within 90 days after entry to make a determination of its status. Tips and leads information that is determined not to be valid must be purged from the system. Valid information, unless subsequently substantiated, must be purged from the system within two years of entry (Part XII.B and E.4).

Global Justice Information Sharing Initiative ♦ Intelligence Working Group ♦ Privacy Committee

While tips and leads information may qualify under Florida's statutory definition as "criminal intelligence information," it would not be considered "criminal intelligence information" under the definition of the term adopted by the NCISP, 28 CFR Part 23, and the academic and professional authorities cited herein. This illustrates why it is critical to consult state statutes and policies when establishing operational guidelines and policies for intelligence and information sharing.

**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

Title	First Name	Last Name	Group	Agency	Email	Invited	Confirmed	Not Attending	Office Number	Added By
Mr.	Peter	Bibring	Advocate	ACLU of Southern California	[REDACTED]		√	X	[REDACTED]	
Mr.	Michael	German	Advocate	American Civil Liberties Union	[REDACTED]		√		[REDACTED]	
Mr.	Carl	Wicklund	Advocate	American Probation and Parole Association	[REDACTED]		√	X	[REDACTED]	
Mr.	Kareem	Shora	Advocate	American-Arab Anti-Discrimination Committee	[REDACTED]		√	X	[REDACTED]	
Mr.	Nawar	Shora	Advocate	American-Arab Anti-Discrimination Committee	[REDACTED]		√		[REDACTED]	
Mr.	Gregory	Nojeim	Advocate	Center for Democracy and Technology	[REDACTED]		√		[REDACTED]	
Mr.	Harley	Geiger	Advocate	Center for Democracy and Technology	[REDACTED]		√		[REDACTED]	
Mr.	Shakeel	Syed	Advocate	Islamic Shura Council of Southern California	[REDACTED]		√		[REDACTED]	
Ms.	Brenda	Abdelall	Advocate	Muslim Advocates	[REDACTED]		√		[REDACTED]	
Ms.	Safiya	Ghori-Ahmad	Advocate	Muslim Public Affairs Council	[REDACTED]		√		[REDACTED]	
Mr.	Harris	Tarin	Advocate	Muslim Public Affairs Council	[REDACTED]		√		[REDACTED]	
Mr.	Marc	Rotenberg	Advocate	EPIC	[REDACTED]		√		[REDACTED]	Mike German
Ms.	Lillie	Coney	Advocate	EPIC	[REDACTED]		√		[REDACTED]	Mike German
Mr.	Mohamed	Elbiary	Advocate	Freedom and Justice Foundation	[REDACTED]		√		[REDACTED]	
Mr.	Ken	Hunt	Fed	DHS	[REDACTED]		√		[REDACTED]	
Ms.	Kirsten	Moncada	Fed	U.S. Department of Justice	[REDACTED]		√	X	[REDACTED]	
Ms.	Joo	Chung	Fed	U.S. Department of Justice	[REDACTED]		√		[REDACTED]	
Mr.	[REDACTED]	[REDACTED]	Fed	Office of the Director of National Intelligence	[REDACTED]		√		[REDACTED]	
Ms.	[REDACTED]	[REDACTED]	Fed	Office of the Director of National Intelligence	[REDACTED]		√		[REDACTED]	
Mr.	[REDACTED]	[REDACTED]	Fed	Office of the Director of National Intelligence	[REDACTED]		√		[REDACTED]	
Ms.	[REDACTED]	[REDACTED]	Fed	Office of the Program Manager, ISE	[REDACTED]		√		[REDACTED]	
Mr.	[REDACTED]	[REDACTED]	Fed	Office of the Program Manager, ISE	[REDACTED]		√		[REDACTED]	
Mr.	[REDACTED]	[REDACTED]	Fed	Office of the Program Manager, ISE	[REDACTED]		√		[REDACTED]	
Mr.	Thomas	O'Reilly	Fed	Office of the Program Manager, ISE	[REDACTED]		√		[REDACTED]	
Mr.	Russell	Porter	Local/State	U.S. Department of Justice	[REDACTED]		√		[REDACTED]	
Lieutenant	Ron	Leavell	Local/State	Iowa Department of Public Safety	[REDACTED]		√		[REDACTED]	
Ms.	Susan	Courtwright-Rodriguez	Fed	Seattle Police Department	[REDACTED]		√		[REDACTED]	
Mr.	Timothy	Skinner	Fed	Office for Civil Rights and Civil Liberties	[REDACTED]		√	X	[REDACTED]	
Staffing				Office for Civil Rights and Civil Liberties	[REDACTED]		√		[REDACTED]	
Ms.	[REDACTED]	[REDACTED]	Fed	Office of the Program Manager, ISE	[REDACTED]		√		[REDACTED]	
Mr.	John	Wilson	Fed	Supporting the Office of the Program Manager, ISE	[REDACTED]		√		[REDACTED]	
Mr.	Bob	Cummings	Fed	Supporting the Office of the Program Manager, ISE	[REDACTED]		√		[REDACTED]	

Title	First Name	Last Name	Group	Agency	Email	Invited	Confirmed	Added By	Not Attending
Mr.	Peter	Bibring	Advocate	ACLU of Southern California	[REDACTED]				
Mr.	Michael	German	Advocate	American Civil Liberties Union	[REDACTED]				
Mr.	Carl	Wicklund	Advocate	American Probation and Parole Association	[REDACTED]				
Mr.	Kareem	Shora	Advocate	American-Arab Anti-Discrimination Committee	[REDACTED]				
Mr.	Gregory	Nojrim	Advocate	Center for Democracy and Technology	[REDACTED]				
Mr.	Harley	Geiger	Advocate	Center for Democracy and Technology	[REDACTED]				
Mr.	Shakeel	Syed	Advocate	Islamic Shura Council of Southern California	[REDACTED]				
Ms.	Brenda	Abdelali	Advocate	Muslim Advocates	[REDACTED]				
Ms.	Safiya	Ghori-Ahmad	Advocate	Muslim Public Affairs Council	[REDACTED]				
Mr.	Marc	Rotenberg	Advocate	EPIC	[REDACTED]			Mike German	
Ms.	Lillie	Coney	Advocate	EPIC	[REDACTED]			Mike German	
Mr.	Mohamed	Elibiary	Advocate	Freedom and Justice Foundation	[REDACTED]				
Mr.	Ken	Hunt	Fed	DHS	[REDACTED]				
Ms.	Kirsten	Moncada	Fed	U.S. Department of Justice	[REDACTED]				
Mr.	[REDACTED]	[REDACTED]	Fed	Office of the Director of National Intelligence	[REDACTED]				
Ms.	[REDACTED]	[REDACTED]	Fed	Office of the Director of National Intelligence	[REDACTED]				
Mr.	[REDACTED]	[REDACTED]	Fed	Office of the Director of National Intelligence	[REDACTED]				
Ms.	[REDACTED]	[REDACTED]	Fed	Office of the Program Manager, ISE	[REDACTED]				
Mr.	[REDACTED]	[REDACTED]	Fed	Office of the Program Manager, ISE	[REDACTED]				
Mr.	Thomas	O'Reilly	Fed	Office of the Program Manager, ISE	[REDACTED]				
Mr.	Russell	Porter	Local/State	U.S. Department of Justice	[REDACTED]				
Lieutenant	Ron	Leavell	Local/State	Iowa Department of Public Safety Seattle Police Department	[REDACTED]				
Staffing									
Ms.	[REDACTED]	[REDACTED]	Fed	Office of the Program Manager, ISE	[REDACTED]				
Mr.	John	Wilson	Fed	Supporting the Office of the Program Manager, ISE	[REDACTED]				
Mr.	Bob	Cummings	Fed	Supporting the Office of the Program Manager, ISE	[REDACTED]				

From: [Mohamed Elbiary](#)
To: [REDACTED]
Subject: RE: follow-up and some heart-felt feedback
Date: Thursday, February 26, 2009 4:58:02 PM

Noon est is fine. It'll be 11 am cst. I'll await your call.

Thanks,

ME (Mohamed Elbiary)
"All we can do is build one brick at a time!" Hamada

-----Original Message-----

From: [REDACTED]
Sent: Thursday, February 26, 2009 3:26 PM
To: [REDACTED]
Subject: Re: follow-up and some heart-felt feedback

I am sorry I misread your email. How about noon east coast time
[REDACTED]
Senior Advisor
Office of the Program Manager for the Information Sharing Environment

----- Original Message -----

From: Mohamed Elbiary [REDACTED]
To: [REDACTED]
Sent: Thu Feb 26 15:55:57 2009
Subject: RE: follow-up and some heart-felt feedback

Thanks John for your response and hard work. My cell is [REDACTED] and I can do tomorrow anytime with the exception of a block from 1-3 PM CST. If that doesn't work for you then I'll make the time next week that works for you.

Thanks,

ME (Mohamed Elbiary)
"All we can do is build one brick at a time!" Hamada

-----Original Message-----

From [REDACTED]
Sent: Thursday, February 26, 2009 2:37 PM
To: m [REDACTED]
Subject: Re: follow-up and some heart-felt feedback

Hi

First of all thank you for your email. I appreciated your comments at our meeting as I do today. I would like to take a few moments to talk with you so I can explain how we are dealing with this issue and to gain some insight from you on how best to communicate what you expressed in your email to fusion center directors across the nation. Is there a number I can reach you at either later today or tomorrow afternoon?

Thanks

[REDACTED]

██████████
Senior Advisor
Office of the Program Manager for the Information Sharing Environment

----- Original Message -----

From: Mohamed Elbiary ██████████
To: ██████████; ██████████ >; ██████████
Sent: Thu Feb 26 14:22:31 2009
Subject: follow-up and some heart-felt feedback

Hi ██████████

I wanted to reiterate my appreciation for the meeting at DNI last Wednesday on the SARs Initiative. It was a pleasure meeting all of you personally and it certainly enriched my experience working on these issues. Please excuse the length of this email, but I feel that just like Intelligence is supposed to speak truth to power, I must do a little Voir Dire myself now with y'all.

As you are most probably aware by now, the day after our meeting the North Central Texas Fusion System (NCTFS) issued a bulletin to about 1,500 local law enforcement officials in about 200 agencies essentially pushing out very unprofessional analysis. People like me are a dime a dozen and we all would like to help our country, but trust is extremely important. So when we lose confidence that our partners are seriously committed to reform, then we lose trust and simply walk away. Whether it was an NSC official contacting us years ago to advise on one issue, DHS/NCTC seeking our counsel on counter-radicalization or the FBI requesting our assistance with a de-radicalization and reintegration of a subject; we have never shied away from stepping up and doing what we can to serve our country.

I hope you didn't take offense at my strong comment that I see the federal agencies as trying to have it both ways on the SARs issue. As you read the attached Bulletin, please ask yourself how simple folks in the Muslim community seeing this political stuff coming from an intelligence entity would feel. They feel like they did nothing wrong, are still the same folks as they were on September 10th, but that the government has unleashed the dogs of hell upon them to deal with. This minority community fulfills a tripwire role that no one else and certainly surveillance cannot replace. As I mentioned in our meeting, I approach much of these ISE issues very cognizant of the radicalization angle. One of the necessary components of radicalization as Dr. Wiktorwitz at NCTC would tell you is alienation and marginalization, which a Bulletin like this certainly causes.

Our hope over the past several years engaging NS policy folks like yourselves was built on a presumption that the feds want to do the right thing. It has been many years and from the grassroots in Dallas and across other areas of the country, I want to share the frustrations of many that feel we're not any closer in 2009 than 2002 in getting all this right. I urge you to reconsider the following macro points as you continue your work:

1. That SARs do not qualify as "criminal intelligence investigation" and therefore are "tips and leads" and don't fall under 28 CFR part 23's "reasonable doubt" standard. To a certain extent, such a signal from the feds invites abuse at the local level. When competent leadership isn't engaged, then every king of the mole hill leads his little empire as he sees fit.
2. Issuing a policy guideline at a minimum to all 50 state DHS Directors suggesting that they create a taskforce to assess their state's Criminal Intelligence architecture with a focus on the fusion centers to make sure that proper

auditing and oversight is provided by the state's executive branch.

3. The ODNI as the top IC entity in this structure should have a publicly transparent process created in partnership with DHS and DOJ where an IG type office audits down to the core entities like Fusion Centers and can bring to light public corruption issues as well as abuse of power situations. Today it's confusing even for someone like me where the buck really stops and a few bad apples can certainly destroy public confidence in a lot of worthwhile efforts.

I offer these suggestions all in a constructive manner whether last week or today and hope its accepted as such. "Cooperative Federalism" should be bi-directional, Feds should get the assistance they need but with that comes responsibility to make sure that innocents aren't being harmed along the way. As you'll see from the PAB attached, Fusion Centers are not simply collecting and sharing SARs then passing off CT investigative leads to the JTTFs but at least this one is actively drumming up political SARs by triggering local investigations.

Salaam and God bless,

ME (Mohamed Elibiary)

"All we can do is build one brick at a time!" Hamada

From: [REDACTED]
To: [REDACTED]
Subject: Re: Thanks
Date: Tuesday, March 31, 2009 7:37:21 AM

[REDACTED]

----- Original Message -----

From: [REDACTED]
To: [REDACTED]
Sent: Mon Mar 30 18:30:07 2009
Subject: Fw: Thanks

[REDACTED]

----- Original Message -----

From: [REDACTED]
To: German, Michael [REDACTED] KENNENC0
Cc: [REDACTED]
Sent: Mon Mar 30 17:28:22 2009
Subject: RE: Thanks

Hi Mike,

Thanks for the additional input - this is helpful. And thanks again for your time today. We greatly appreciate it.

Have a great week,

[REDACTED]

From: German, Michael [REDACTED]
Sent: Monday, March 30, 2009 5:25 PM
To: KENNENC0; JAYNEEF
Subject: Thanks

Hi [REDACTED]

Thanks again for inviting me up to talk about the new draft functional standards. I had a thought in regards to the discussion of the definition of "Suspicious Activity" on page 2: "intelligence gathering" is part of "pre-operational planning" related to terrorism, so I wonder if you could clear up any possible confusion by just removing the "intelligence gathering" part so it reads: incident or behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity."

If you decide to keep the "intelligence gathering" language make sure it is clear that the "intelligence gathering" must also be "related to terrorism or other criminal activity" phrase (perhaps as we discussed putting an "and/or" between the two would convey that both the intelligence gathering and the pre-operational planning must be related to terrorism or other criminal activity, but I'm afraid this could also be confusing).

Hope this helps.

Mike

Michael German

Policy Counsel

American Civil Liberties Union

Washington Legislative Office

915 15th Street, NW

Washington, DC 20005

[REDACTED]

[REDACTED]



Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations

Nationwide Suspicious Activity Reporting Initiative

Prepared by the
Program Manager, Information Sharing Environment

May 2010

For more information, go to:

www.ise.gov

**PRIVACY, CIVIL RIGHTS, AND CIVIL
LIBERTIES ANALYSIS AND
RECOMMENDATIONS**

**NATIONWIDE SUSPICIOUS ACTIVITY
REPORTING INITIATIVE**

Prepared by the
Program Manager, Information Sharing Environment

May 2010

Table of Contents

I. Introduction..... 1

II. The Critical Role of Privacy, Civil Rights and Civil Liberties Protections in the ISE-SAR EE 2

III. Recommendations for the Nationwide Implementation of the NSI in 2010 3

IV. Policies and Processes Supporting the NSI Privacy Framework 9

A. Recommendations of the *Initial Privacy and Civil Liberties Analysis* 9

B. Strengthening the NSI Privacy Framework through Collaboration with Privacy and Civil Liberties Advocacy Groups 10

C. The Revised ISE-SAR Functional Standard 11

D. Standardized Approach to Privacy, Civil Rights, and Civil Liberties Privacy Policies... 15

E. Federal Privacy Technical Assistance and Training 16

V. Success Stories and Best Practices from EE Sites..... 16

A. Success Stories 16

B. Best Practices 17

VI. Conclusion 17

Appendix A – ISE-SAR EE Privacy and Civil Liberties Assessment Questionnaire..... 18

Appendix B – Observations of EE Participating Sites During the ISE-SAR EE 22

A. Overview of Results 22

B. Methodology 22

C. Results of Follow-up Assessments 22

Appendix C – Organizations That Participated in Outreach Efforts 28

Appendix D – Acronyms and Abbreviations 30

Appendix E – Referenced Documents 31

I. Introduction

This *Nationwide Suspicious Activity Reporting Initiative (NSI) Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations* (“*Analysis*”) provides an update to the *Initial Privacy and Civil Liberties Analysis*¹ of the now concluded Information Sharing Environment Suspicious Activity Reporting (ISE-SAR) Evaluation Environment (EE) and Functional Standard.² The *Initial Privacy and Civil Liberties Analysis* reflects the commitment to ensuring that privacy, civil rights, and civil liberties protections were built into the policies and processes of the sites³ participating in the ISE-SAR EE and resulted in: (1) the revision and adoption of the ISE-SAR Functional Standard (“*Functional Standard*”); and (2) the development of a robust and comprehensive privacy, civil rights, and civil liberties protection framework for the NSI, known as the NSI Privacy Framework.⁴

The EE served as the demonstration phase or pilot phase of the NSI. The initial sites that participated in the EE implemented the recommendations from the *Initial Privacy and Civil Liberties Analysis* and currently participate in the NSI. Additional sites will be added now that the Initiative has moved from the demonstration phase of the EE to the nationwide implementation of the NSI.

The EE validated the recommendations of the *Initial Privacy and Civil Liberties Analysis*, thus enabling Federal partners to draw upon the experiences of the EE participating sites in fortifying and refining the NSI Privacy, Civil Rights, and Civil Liberties Framework.⁵ The enhanced framework is comprised of the recommendations from the *Initial Privacy and Civil Liberties Analysis*, the revised Functional Standard, and the experiences of the EE participating sites reflected in this Analysis. The implementation of the NSI Privacy Framework will ensure

¹ *Information Sharing Environment – Suspicious Activity Reporting Functional Standard and Evaluation Environment: Initial Privacy and Civil Liberties Analysis* (September 2008).

² Further information regarding the development and implementation of the EE can be found in the accompanying reports: (1) *Final Report: Information Sharing Environment Suspicious Activity Reporting Evaluation Environment* (January 2010) (*Final Report: ISE-SAR EE*) from the Department of Justice Bureau of Justice Assistance; and (2) *The Nationwide Suspicious Activity Reporting Initiative Status Report* (February 2010), from the Office of the Program Manager for the Information Sharing Environment.

³ The EE ultimately encompassed twelve NSI Environment sites and three Federal agencies. The EE participating sites included: Boston Police Department (PD), Chicago PD, Florida Department of Law Enforcement (FDLE), Houston PD, Las Vegas Metropolitan PD, Los Angeles PD (LAPD), Metropolitan (Washington) DC PD, Miami-Dade Fusion Center, New York State Intelligence Center, Arizona Counter Terrorism Information Center, Seattle Police Department and the Virginia Fusion Center. As for the Federal agencies involved in the EE, the Federal Bureau of Investigations (FBI) participated through its eGuardian system; the Department of Homeland Security (DHS) shared Federal Air Marshal Service (FAMS) data; and the Department of Defense (DoD) — also using eGuardian — gathered and shared SARs in support of its Force Protection mission. Not all sites and agencies are sharing data at this time due to the requirement that each site fully implement the NSI Privacy Framework.

⁴ See Section IV of this *Analysis* for a comprehensive discussion of the NSI Privacy Framework.

⁵ Throughout the remainder of this document, the term “NSI Privacy, Civil Rights, and Civil Liberties Framework” is normally abbreviated to “NSI Privacy Framework.”

that privacy, civil rights, and civil liberties will continue to be appropriately protected as the Initiative moves beyond the EE to the nationwide implementation of the NSI in 2010.

This Analysis uses the experiences of the EE participating sites to further build upon the commitment made in the *Initial Privacy and Civil Liberties Analysis* by:

- Reviewing the development and implementation of EE participating sites' privacy, civil rights, and civil liberties protections;
- Outlining the observations of EE participating site experiences;
- Updating the initial privacy and civil liberties issues identified by and resolved between Federal sponsoring agencies, participating State and local partners, and privacy and civil liberties advocates during the EE; and
- Making recommendations to be followed during the nationwide implementation of the NSI.

In sum, the NSI Privacy Framework enabled the EE participating sites to fulfill the dual mandates of maximizing information sharing while protecting privacy, civil rights, and civil liberties. The effectiveness of this framework is underscored by the fact that the EE participating sites did not report any breaches of personal information with regard to SAR or ISE-SAR information. Nor did they receive any complaints for redress during the EE.

Going forward, NSI participants must continue to work together to ensure that robust privacy policies and procedures are adopted, properly implemented, and continuously assessed. Participants must also actively seek out opportunities to further enhance privacy, civil rights, and civil liberties protections.

II. The Critical Role of Privacy, Civil Rights and Civil Liberties Protections in the ISE-SAR EE

The key objective of the ISE-SAR EE was to establish, at each of the EE participating sites, policies and business processes that support the gathering, documenting, processing, analyzing, and sharing of SARs while also ensuring that privacy, civil rights, and civil liberties were protected in accordance with Federal, state, and local constitutions, laws, and regulations. As a condition of participation, the EE participating sites were required to implement a privacy, civil rights, and civil liberties protection framework. This framework included the adoption of appropriate policies, the institution of specialized business processes, and the training of all involved personnel before they were permitted to post or access ISE-SARs.

The EE enabled participants to assess the value of the ISE-SAR process and the ISE-SAR Functional Standard⁶ and to provide a limited evaluation of the value of the Detailed versus Summary ISE-SAR formats⁷ in advancing counterterrorism goals. Following the end of the EE pilot phase, all participants provided feedback to Federal privacy officials regarding the administrative and procedural aspects of the Initiative, including the process for designating reports as ISE-SARs, the management of postings in ISE Shared Space, the processes for correcting inaccurate information, and other relevant program implementation issues. The ISE-SAR EE proved to be a valuable tool for refining the recommendations made in the *Initial Privacy and Civil Liberties Analysis*, and confirming that these recommendations must be addressed in the nationwide implementation of the NSI.⁸

III. Recommendations for the Nationwide Implementation of the NSI in 2010

The ISE-SAR EE resulted in significant implementation progress, while revealing areas that will require enhanced focus during the broader NSI implementation in 2010. Although the sites' experiences varied,⁹ all sites recognized the importance of maintaining strong privacy 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.

⁶ The ISE-SAR Top-Level Business Process is set forth in Section II(D) of the ISE-SAR Functional Standard, Version 1.5 (May 2009).

⁷ See *Final Report: ISE-SAR EE*, at pages 11 and 43, for a discussion of the EE participating sites' use of the Summary and Detailed formats. The participating sites' evaluation was limited because the Evaluation Environment operated for a relatively short period of time. More data will be necessary to provide a full assessment of the implementation of the NSI Privacy Framework. It is, therefore, recommended that the NSI continue to evaluate the benefits of the Detailed and Summary ISE-SAR formats.

⁸ The Program Manager for the Information Sharing Environment (PM-ISE) and the Department of Justice Bureau of Justice Assistance (DOJ BJA) conducted follow-up assessments of EE implementation using a questionnaire. See Appendix A for the ISE-SAR EE *Privacy and Civil Liberties Assessment Questionnaire*, and Appendix B for the *Observations of EE Participating Sites During the ISE-SAR EE*.

⁹ 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.

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 Privacy Fields of the Detailed ISE-SAR format.¹⁰ 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.¹¹

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:

- 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 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 by in the Functional Standard; line

¹⁰ 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.

¹¹ See Appendix B, Section C (1) for further discussion.

- 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 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 ~~must~~ engage in outreach to members of the public, private sector partners, and privacy 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 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;¹²
- d. Other sites hosted community open house days and/or provided tours of facilities upon request from the public or the media; and
- e. Several have reported plans to make the privacy policy available on a public website, either a fusion center-specific or Departmental website.

Going forward, the following three controls ~~must~~ should be implemented in order to further promote transparency and collaboration. First, the sites must ensure the broadest possible review of privacy policies and procedures, with due consideration given to stakeholder recommendations. Second, the sites must consistently provide thorough explanations in response to public inquiries about sites' privacy policies, information availability, and redress procedures. Third, the methods used by the sites to promote outreach and collaboration must be continually assessed for the purpose of identifying and sharing best practices. Transparency

¹² 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 able to distinguish between innocent cultural behaviors and behavior indicative of criminal activity, and local communities will play a more supportive role in combating terrorism-related crime.

and collaboration will foster public trust and enable sites to better respond to the concerns of citizens and advocacy groups.

RECOMMENDATION 3: To mitigate the risk of profiling based on race, ethnicity, national origin, or religion, and to improve mission effectiveness, NSI participating sites must adhere to the standardized vetting process and consistently use the ISE-SAR Functional Standard criteria in the identification, documentation, and sharing of ISE-SAR information.

Federal, State and local NSI partners recognize that mitigation of the risks associated with profiling is critical to the success of the Initiative. NSI partners must, therefore, remain vigilant in implementing the enhanced privacy, civil rights, and civil liberties protections for SARs and ISE-SARs, in order to avoid the dangers of profiling.

The privacy, civil rights, and civil liberties protections are multi-faceted and robust. First, NSI partners must implement the standardized vetting process for SARs. Second, NSI partners must ensure the consistent and objective application of the revised ISE-SAR Functional Standard criteria. The implementation of the revised ISE-SAR Functional Standard constitutes an essential safeguard supporting the NSI Privacy Framework and enhancing mission effectiveness. ~~The revised Functional Standard expressly states 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). The revision tightened the definition of "Suspicious Activity" by limiting it to "observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity."~~ This threshold serves as the basis for a SAR or an ISE-SAR to be collected and shared by law enforcement, homeland security, and counterterrorism agencies and must be fully and consistently implemented in each NSI site's policies and business processes. Third, NSI partners must provide specialized training and guidance to NSI personnel in order to strengthen their ability of personnel to recognize suspicious behaviors in a uniform and objective manner. Finally, as the NSI effort grows, the sites' vetting process, application of the "reasonably indicative" threshold, and efforts to prevent profiling must be regularly assessed.

RECOMMENDATION 4: The sites must designate a trained privacy officer who, in addition to carrying out delegated responsibilities, has access to the services of legal counsel with privacy expertise to provide ongoing legal advice and assistance regarding privacy, civil rights, and civil liberties.

The EE demonstrated that the sites should designate a privacy officer and, as needed, ensure that such officer is properly trained. The privacy officer, if not an attorney, should have access

to legal expertise in developing and implementing privacy, civil rights, and civil liberties policies and procedures and resolving legal issues. Few EE participating sites were able to designate or hire personnel with subject matter expertise to manage privacy, civil rights, and civil liberties issues on a full-time basis. In most cases, the sites relied upon legal staff from parent agencies or state attorneys general offices to identify the relevant State and local legal and regulatory requirements for incorporation in their respective ISE-SAR or comprehensive privacy, civil rights, and civil liberties policies. Sites also used records managers and compliance officers to ensure ISE-SAR policy compliance with state open records laws and other state and local requirements.

Access to the services of a subject matter expert in the areas of privacy, civil rights, and civil liberties would have expedited privacy policy development and implementation during the EE and would have enabled the sites to access or share personal information contained in Privacy Fields earlier. Privacy officers and legal counsel are therefore necessary to ensure compliance with NSI Privacy Framework and to identify opportunities to further enhance privacy, civil rights, and civil liberties protections.

RECOMMENDATION 5: An ongoing, formalized review process must be established to ensure that business processes are aligned with privacy policies and procedures, and to assess the need for additional privacy, civil rights, and civil liberties protections.

All ISE-SAR EE participating sites recognized the importance of intermittently conducting reviews of their privacy policies and business processes. Many sites also indicated that they would conduct interim policy reviews as needed.

In order to ensure a standardized approach, a formalized review process must be established. At least annually, an onsite review team should assess adherence to and implementation of the NSI Privacy Framework. The review should include: (1) an assessment of accountability actions, including documented changes in business processes that reflect the enhanced privacy protections; (2) documentation of any breaches involving personal information; (3) assessment of the handling of information requests, error notifications, and complaints for redress; and (4) documentation of the delivery of required training activities.

RECOMMENDATION 6: Each participating site must exercise due diligence in implementing appropriate physical, technical, and administrative measures to safeguard information under its control from unauthorized access, disclosure, modification, use or destruction.

The EE served to highlight security controls which are critical for ensuring appropriate safeguarding of personal information. Going forward, all NSI sites must exercise due diligence by: (1) limiting access to ISE-SARs to agencies and individuals with proper credentials and

roles; (2) requiring a reason for all searches; (3) implementing an appropriate electronic warning banner for users accessing the ISE Shared Space; (4) mandating the maintenance of inquiry/access logs and audit trails; and (5) requiring that all records provide notice about the nature and quality of the information, including confidence and dissemination codes.

RECOMMENDATION 7: Each participating site must emphasize and establish procedures to ensure personal responsibility and accountability for protecting privacy, civil rights, and civil liberties.

Although none of the EE participating sites reported a breach of personal information with regard to SAR or ISE-SAR information, personnel must remain vigilant in adhering to the site's privacy protection framework. Each site should ensure that all assigned personnel with access to SAR and ISE-SAR information review and acknowledge, on an annual basis, that they have read and understand the site's privacy policies and procedures and that they will execute their responsibilities in accordance with the site's policies and procedures.¹³

Sites should provide and require privacy training regarding their privacy policies, procedures, business processes, and updates thereto. NSI sites should also provide ongoing training which focuses on safeguarding personal information. Such training would strengthen the ability of personnel to prevent breaches involving personal information and should underscore the obligations of personnel to report privacy policy violations and breaches involving personal information. Training should be structured to ensure that personnel are informed of their individual, job-related responsibilities for protecting privacy, civil rights, and civil liberties and the consequences for violation of those responsibilities. Finally, to address some confusion regarding the threshold for ISE-SARs, personnel at NSI sites should receive training regarding the "reasonably indicative" threshold for documenting ISE-SARs and the interaction of that threshold with other requirements such as 28 CFR Part 23.

RECOMMENDATION 8: Federal sponsoring agencies should work to ensure that technical assistance, guidance, and support focusing on privacy policy adoption, implementation, and training remain available and are expanded as needed to serve all NSI sites.

The sites confirmed that the technical assistance provided during the ISE-SAR EE facilitated the site's development and implementation of the privacy protection framework. Federal partners should ensure that technical assistance and training teams are available to NSI sites to ensure that adequate resources and policy guidance are available to resolve NSI issues.

¹³ This requirement should apply to all personnel, including employees, contractors, and other support personnel. Some EE participating sites also provided training to personnel from other state and local partner agencies.

RECOMMENDATION 9: When ISE Shared Spaces become better populated with new ISE-SARs, Federal partners should devise and conduct a more robust test of the value of the Summary Format.

During the EE, two data formats were developed for packaging ISE-SARs, namely, the Summary format and the Detailed format. The Summary format excludes Privacy Field information containing personally identifiable information (PII), whereas the Detailed format includes such information.¹⁴ The Federal partners and the EE participating sites were not able to fully assess the utility of the Summary format due to a lack of sufficient data. There may, however, be value in making data in the Summary Format available to non-law enforcement public safety agencies, entities involved in critical infrastructure protection, and first responders for use in identifying patterns and trends, on condition that appropriate privacy, civil rights, and civil liberties safeguards are in place.

RECOMMENDATION 10: Federal and SLT agencies should ensure that the experiences gained during the ISE-SAR EE and the fuller NSI implementation are considered as other ISE capabilities are developed.

Although the privacy, civil rights, and civil liberties concerns addressed in this Analysis are discussed in the context of the NSI, these concerns are not unique to SAR and ISE-SAR information. SARs are but one source of terrorism-related information, and the policies, procedures, and processes developed to handle SARs may also directly apply to other types of 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 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;

¹⁴ For further information regarding the EE participating sites use of these formats, see *Final Report: ISE-SAR EE*, at pages 11 and 43.

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 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 and civil liberties advocacy groups.¹⁵ Advocacy groups served an essential role in shaping the privacy protection framework for ISE-SAR information sharing activities by assisting with the development and review of products (e.g., templates and training), and by participating in several meetings with the ISE-SAR EE implementation team to address EE implementation efforts.

These meetings confirmed that the implementation of privacy protections would require a multi-faceted and iterative approach. The PM-ISE and its Federal partners looked to the experiences of the sites during the EE for validation of the recommendations from the *Initial Privacy and Civil Liberties Analysis* and verification that the recommendations had application to the broader National SAR Initiative. The experiences of the EE participating sites confirmed the value of the NSI Privacy Framework as an appropriate minimum standard for protection in

¹⁵ See Appendix C for a listing of the advocacy groups which participated in the collaborative process.

view of the fact that hundreds of qualifying ISE-SARs were successfully posted to the Shared Space and that there were no incidents of inadvertent sharing of such data.

NSI partners agree that the following elements are the minimum essential measures for the NSI Privacy Framework and are the key to meaningful privacy and civil rights/civil liberties protections:

1. Each NSI participating agency must conduct the NSI process pursuant to its statutory authorities and its privacy and civil liberties policies and procedures that are consistent with the ISE Privacy Guidelines;
2. Each NSI participating agency must submit privacy and civil liberties policies and procedures for review to ensure consistency with the ISE Privacy Guidelines prior to posting or accessing personal information (i.e., Privacy Fields) in the ISE Shared Space;
3. Implementation must include training of front-line, investigative, analytic and supervisory personnel regarding their respective site's privacy policy, as well as behaviors and indicators of terrorism-related criminal activity;
4. Each NSI participating agency must institute 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; and
5. Sites should engage in outreach and collaboration at a local level with privacy and civil liberty advocacy groups.

Adherence to and implementation of all elements of the NSI Privacy Framework are essential preconditions to sharing personal information contained in Privacy Fields. Compliance with this approach will not only strengthen the protection of privacy, civil rights, and civil liberties 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*¹⁶ 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 Standard¹⁷ 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.

¹⁶ *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing* (October 2007).

¹⁷ See Version 1.5 of the ISE-SAR Functional Standard.

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 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 gathering, collection, and ISE-SAR determination process in order to ensure that ISE-SARs are “reasonably indicative of criminal activity associated with terrorism.”

1. *The Threshold 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 threshold raises the bar 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.

The revision of the Functional Standard established a new “reasonably indicative of pre-operational planning related to terrorism or other criminal activity” standard both for collecting SAR information and for determining if it should be identified as an ISE-SAR based on the two-step review process to determine if it has a potential terrorism nexus.¹⁸ This threshold serves as the basis for a SAR or an ISE-SAR to be collected and shared by law enforcement, homeland

¹⁸ The EE partners worked closely with privacy and civil liberties advocates to address and mitigate privacy concerns raised by the original Functional Standard (Version 1.0), including the requirement that a SAR be based on “Official documentation of observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention” and that an ISE-SAR be based on the same standard, coupled with a determination that the SAR has a “potential terrorism nexus.” The concern was that threshold 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 establish a new “reasonably indicative of pre-operational planning related to terrorism or other criminal activity” standard both for collecting SAR information and for determining if it should be identified as an ISE-SAR based on the two-step review process to determine if it has a potential terrorism nexus. By establishing a new threshold based on “reasonably indicative,” supervisors at source agencies and trained analysts and investigators at fusion centers and other agencies have a standard of review 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 protections. The revisions to Version 1.0 of the ISE-SAR Functional Standard resulted in Version 1.5.

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.

security, and counterterrorism agencies. The “reasonably indicative” threshold requires that the terrorism-related activity conform to one or more of the criteria identified in Part B of the ISE SAR Functional Standard.

The threshold based on “reasonably indicative,” allows supervisors at source agencies and trained analysts and investigators at fusion centers and other agencies have a standard of review 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 protections. Furthermore, this revised threshold 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 a more narrowly targeted threshold. It produces sufficiently high quality information to enable agencies and analysts to “connect the dots.” tightened the definition of “Suspicious Activity” by limiting it to “observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.”⁴⁹ This threshold serves as the basis for a SAR or an ISE SAR to be collected and shared by law enforcement, homeland security, and counterterrorism agencies. The “reasonably indicative” threshold requires that the activity conform to one or more of the criteria identified in Part B of the ISE SAR Functional Standard. This threshold requires more than “mere suspicion” but less than the “reasonable suspicion” standard applicable to criminal intelligence information. The “reasonably indicative” threshold 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 a more narrowly targeted threshold. It produces sufficiently high quality information to enable agencies and analysts to “connect the dots.”

⁴⁹ The EE partners worked closely with privacy and civil liberties advocates to address and mitigate privacy concerns raised by the original Functional Standard (Version 1.0), including the requirement that a SAR be based on “Official documentation of observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention” and that an ISE SAR be based on the same standard, coupled with a determination that the SAR has a “potential terrorism nexus.” The concern was that threshold 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 establish a new “reasonably indicative of pre-operational planning related to terrorism or other criminal activity” standard both for collecting SAR information and for determining if it should be identified as an ISE SAR based on the two-step review process to determine if it has a potential terrorism nexus. By establishing a new threshold based on “reasonably indicative,” supervisors at source agencies and trained analysts and investigators at fusion centers and other agencies have a standard of review 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 protections. The revisions to Version 1.0 of the ISE SAR Functional Standard resulted in Version 1.5.

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.

Comment [A1]: I disagree. The behavioral criteria in the FS distinguish an ISE-SAR from a SAR — both of which must meet the “reasonably indicative” standard. However, the FS does not define those behaviors that apply to “other criminal activity.”

In addition, the “reasonably indicative” threshold is an essential privacy, civil rights and civil liberties protection for Americans because it emphasizes a behavior-focused approach to identifying suspicious activity and mitigates the risk of profiling based upon race, ethnicity, national origin, or religious affiliation.²⁰ As the ACLU explained in May 2009:

The revised guidelines for suspicious activity reporting establish that a reasonable connection to terrorism or other criminal activity is required before law enforcement may collect Americans’ personal information and share it within the ISE. These changes to the standard, which include reiterating that race cannot be used as a factor to create suspicion, give law enforcement the authority it needs without sacrificing the rights of those it seeks to protect.²¹

2. *The Standardized, Multi-Level Vetting Process*

The implementation of the revised ISE-SAR Functional Standard constitutes an essential safeguard supporting the NSI Privacy Framework. This standard requires the use of a multi-level business process to identify those SARs 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.²² The analyst or officer would then determine whether the facts and circumstances taken as a whole are “*reasonably indicative of pre-operational planning related to terrorism.*”²³ If this determination is made, the report will be documented and made available as an ISE-SAR to all appropriate ISE participants in the agency’s Shared Space.²⁴

²⁰ The revised Functional Standard expressly states 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).

²¹ Quote from Michael German, National Policy Counsel, ACLU (May 2009).

²² The criteria for making this determination are set forth in Part B of the ISE-SAR Functional Standard (Version 1.5).

²³ 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 constitutionally protected activity, but which may be criminal in nature. The 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.

²⁴ 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 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 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

DOCUMENT 29 (cont'd)

The enhancements to the ISE-SAR Functional Standard protect privacy, civil rights and civil liberties by ensuring that each SAR is gathered for a valid law enforcement or counterterrorism purpose by trained staff, 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. This process must be incorporated in business processes of NSI sites during the nationwide implementation of the NSI.

D. Standardized Approach to Privacy, Civil Rights, and Civil Liberties Privacy Policies

A critical first step for each NSI site in implementing the NSI Privacy Framework is the development of a written privacy policy as a precondition to sharing or receiving any personal information contained in Privacy Fields. The site's privacy policy must be "at least as comprehensive" as the ISE Privacy Guidelines and the Baseline Capabilities in order to satisfy the requirements of: (1) purpose specification; (2) notice mechanisms; (3) data quality; (4) data security; (5) accountability, enforcement, and audit; and (6) redress.

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 included the following:

1. Completing a comprehensive privacy policy based on DOJ Global Justice's *Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Template*;
2. Formulating an ISE-SAR specific policy based upon the *ISE-SAR Evaluation Environment Privacy, Civil Rights, and Civil Liberties Protection Policy Template*;²⁵ or
3. Refining its existing privacy policy to ensure that it addressed all the ISE Privacy Guidelines requirements for enhanced protection of terrorism-related information.

Each participating site developed a draft privacy policy and provided it to the Privacy Policy Review Team for assessment and feedback. Once the Privacy Policy Review Team determined that the draft policy was "at least as comprehensive" as the ISE Privacy Guidelines, the team recommended the completed policy for approval to the Privacy Guidelines Committee (PGC) Co-Chairs²⁶ and the PM-ISE. Upon approval, DOJ's Bureau of Justice Assistance (BJA) was formally notified that the EE participant was authorized to "go live" in sharing and accessing Privacy Field information in the ISE Shared Spaces.

components is designed to provide early indications to all NSI participating agencies of behaviors and indicators of criminal activity associated with terrorism.

²⁵This template was developed by Federal partners in collaboration with privacy and civil liberties advocacy groups. The PGC's Legal Issues Working Group finalized and approved the template for distribution to the EE participating sites in January 2009.

²⁶ The PGC Co-Chairs include privacy officials from ODNI, DOJ and DHS.

E. Federal Privacy Technical Assistance and Training

Federal partners provided technical assistance, subject matter expertise, and training to ISE-SAR EE participants. Technical assistance included making privacy and civil liberties subject matter experts available to assist in developing and strengthening participant site privacy policies. The provision of technical assistance enabled Federal partners to ensure a standardized approach to privacy policy development at EE participating sites and to provide guidance regarding privacy and civil liberties issues with widespread impact beyond the state and local level.

In addition to assisting with privacy policy development, DHS and DOJ/BJA, through their joint Privacy Technical Assistance Program, developed and provided training on privacy, civil rights, and civil liberties issues to personnel at ISE-SAR EE participant sites. Federal partners also provided role-based ISE-SAR training modules which included privacy and civil liberties components targeted to executives, senior leadership, front-line officers, and analysts.

EE participating sites indicated that privacy technical assistance and training were valuable in maximizing participation in the ISE-SAR EE. They also confirmed that without the provision of assistance, the ISE-SAR EE would not have resulted in meaningful implementation progress.

V. Success Stories and Best Practices from EE Sites

During the follow-up discussions with each EE participating site, several success stories and best practices emerged demonstrating the success of efforts to protect privacy, civil rights, and civil liberties.

A. Success Stories

- The commander of the Florida Fusion Center (FFC) received a telephone call from an individual concerning the FCC's ISE-SAR privacy and civil liberties policy. The FFC commander walked the individual through the privacy policy and protections and answered each of his questions. Upon completion, the caller identified himself as a Certification Assessor from the Commission on Accreditation for Law Enforcement Agencies and congratulated the FFC commander on the thoroughness of her response to his questions.
- Through its formal community outreach campaign, iWatch, the Los Angeles Police Department (LAPD) has informed, trained, and educated its community on SARs including privacy and civil liberties protections at outreach events throughout the Los Angeles metropolitan region. Community training on SAR privacy and civil liberties emphasizes suspicious behaviors over individual characteristics. LAPD considers its iWatch campaign to be the "community part of its SARs process."

- The Florida Department of Health, a state government agency participating in the FFC's terrorism liaison officer program, had previously limited its reporting of SAR information due to its privacy concerns with releasing personal health information. Through the SAR training, the Florida Department of Health understood that its submission to the FFC of SAR information based upon suspicious behaviors was permissible. One of those reports resulted in an open investigation on a person of interest related to terrorism.

B. Best Practices

- The Arizona Counter Terrorism Information Center (ACTIC) actively monitors civil rights and privacy issues raised by other fusion centers around the country through fusion center regional conferences and other outreach events and uses lessons learned as a guide for adjusting its own policies and procedure.
- The FFC sought an extensive policy review from a variety of external stakeholders, including review by the Florida's state advisory board on privacy and civil liberties, citizen advisory groups, and the legal counsels of all of the site's partner agencies in the process of developing its privacy, civil rights, and civil liberties protection policy.

VI. Conclusion

Since the inception of the NSI, Federal and SLT partners have remained steadfast in their commitment to protecting privacy, civil rights, and civil liberties. In moving from the ISE-SAR EE demonstration phase to the national implementation of the NSI, the NSI Privacy Framework will remain a critical touchstone and be regularly reviewed and updated as necessary. Federal and SLT partners must continue to work together to ensure that robust privacy policies and procedures are adopted, properly implemented, and continuously assessed. The NSI sites must continue efforts to identify opportunities for strengthening and improving privacy, civil rights, and civil liberties protections. The NSI Program Manager's Office should lead efforts to ensure continued oversight of framework implementation, with guidance from the ISE PGC and the President's Privacy and Civil Liberties Oversight Board. Maintaining an unrelenting focus on the protection of privacy, civil rights, and civil liberties will assure the public that the legal rights of all Americans are fully protected and will continue to be a national priority.

Appendix A – ISE-SAR EE Privacy and Civil Liberties Assessment Questionnaire

[AGENCY NAME]

ISE-SAR Evaluation Environment

Final Project Privacy & Civil Liberties Protections Assessment

The purpose of the ISE-SAR Evaluation Environment (EE) was to develop a learning environment in which to determine whether a national standard (the SAR Functional Standard) for reporting and evaluating suspicious activity could facilitate the identification of patterns of criminal activity with a nexus to terrorism. To enable implementation of the ISE-SAR EE, it was essential that policies be implemented for ensuring that privacy, civil rights, and civil liberties are protected in the ISE-SAR identification process and in the sharing of ISE-SAR information. These privacy policies also support transparency to the public regarding the sharing of information about terrorism-related suspicious activity between fusion centers and with other law enforcement and homeland security agencies. This assessment seeks to capture the experience of agencies participating in the ISE-SAR EE regarding development and implementation of privacy and civil liberties protections for identifying and sharing ISE SAR information and the integration of these protections into agency business processes and activities. This Privacy Assessment is a requirement of the *Initial Privacy and Civil Liberties Analysis* of the Suspicious Activity Reporting Functional Standard and Evaluation Environment (September 2008 - Version 1).

Site Visit information

Date: [Date and Time of Call, Eastern Standard Time]

Method of Visit: Conference Call

Personnel: [Names and Titles of Site Personnel]

DEVELOPING AND IMPLEMENTING AGENCY PRIVACY POLICIES

- 1) During the ISE-SAR EE, did your agency develop and implement either a comprehensive information and intelligence privacy policy using the Fusion Center Privacy Policy Development Template or an ISE-SAR specific Privacy Policy?
 - a) If so, has the Privacy Policy been promulgated agency wide?
- 2) Has your agency communicated its Privacy Policy to the public, community organizations, and other groups as appropriate?
- 3) Have you conducted a Privacy Impact Assessment for your ISE-SAR activity?
- 4) Did your agency utilize legal/privacy advisors when developing the agency's privacy policy?
- 5) Does the jurisdiction where your agency is located (regional, state, urban) have specific privacy laws or regulations that you incorporated into your privacy policy?
 - a) If yes, please describe these laws or regulations.
 - b) Did any of these laws or regulations impact the development of your agency's privacy and civil liberties policies?
- 6) Does your agency have a plan for regular review of your privacy policy, i.e. biannual review?

IMPLEMENTING AGENCY PRIVACY POLICIES INTO ISE-SAR BUSINESS PROCESSES

- 1) In what ways, if at all, did privacy and civil liberties considerations affect your agency's ability to integrate ISE-SAR activities pre-existing business processes? Describe.
- 2) How does your agency ensure that an ISE-SAR meets the criteria established by the ISE-SAR Functional Standard?
- 3) Does your agency have a mechanism for timely informing the original submitter of SAR information that the SAR has been determined to be an ISE-SAR?
- 4) If an ISE-SAR is determined to be erroneous in content or designation after being posted to the ISE Shared Space, what processes have you implemented to remedy the situation (correction, notice, etc.)?
- 5) What is your procedure for handling SARs that do not meet the criteria of an ISE-SAR? Do you retain and use those SARs and, if so, how do you ensure the privacy and civil liberties protection of those SARs?
- 6) How does your agency ensure that appropriate quality controls are in place for SARs and ISE-SARs (example of controls may include use of labels and markings to indicate questionable accuracy of SAR or ISE-SAR)?
- 7) Are periodic audits of SAR and ISE-SAR data conducted by command-level staff or agency designees?
 - a) If yes, describe your audit process.

ISE-SAR PRIVACY AND CIVIL LIBERTIES PROTECTIONS

- 1) What procedures, both internally and with SAR source agencies, has your agency established to ensure against “profiling” on the basis of race, ethnicity, national origin, religion, or other suspect classifications?
- 2) What procedures, both internally and with SAR source agencies, has your agency established to ensure that individuals’ other Constitutional rights are not violated in the gathering of SAR information?
- 3) Have you received any privacy or civil liberties complaints arising from your SAR or ISE-SAR activities?
 - a) How does your agency handle privacy or civil liberties complaints?
 - b) Do you track complaints? Do you track resolution of complaints?
 - c) Are complaints shared with any external organizations (for example, Attorney General’s office, Inspector General, Internal Affairs, etc.)?
- 4) Has your agency experienced any inadvertent sharing of ISE-SARs (such as a technical or personnel glitch that inadvertently caused a release)?
 - a) Did the inadvertent sharing come to light as sources?
 - b) What procedures does your agency follow to correct an incident where an ISE-SAR is inadvertently shared? Internal fixes? External notification? Other?
 - c) Are cases of inadvertent sharing reported external to your agency? If so, to whom (for example, Attorney General’s office, Inspector General, Internal Affairs, etc.)?

TRAINING AGENCY PERSONNEL ON PRIVACY AND CIVIL LIBERTIES PROTECTIONS AS PART OF THE SAR PROCESS

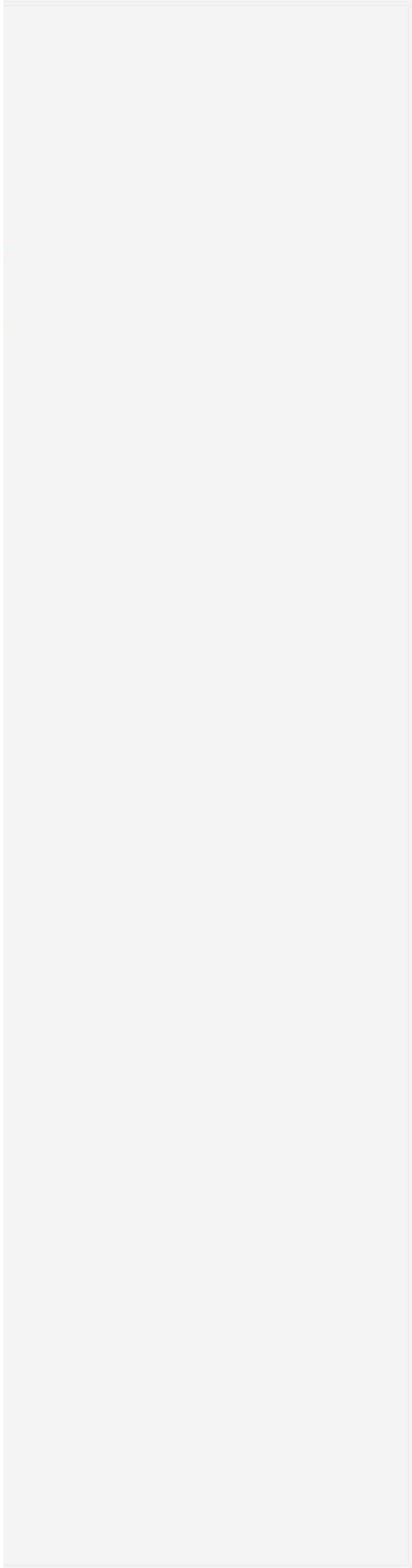
- 1) Have you trained personnel with ISE-SAR responsibilities on privacy and civil liberties protections applicable to the gathering, processing, analyzing, and sharing of SARs and ISE-SARs?
 - a) Provide examples of training provided to your staff to support the ISE-SAR EE.
- 2) Has your agency identified privacy and civil liberties issues for which additional training is needed?
 - a) If so, what types of additional training would your agency need?

CHALLENGES AND LESSONS LEARNED DURING ISE-SAR EE

- 1) What is the most significant change you have made to business processes as a result of the privacy and civil liberties considerations implicated by the ISE-SAR EE?

- a) Describe other privacy and civil liberties considerations and resulting process changes.
- 2) Were privacy and civil liberties issues identified in any "lessons learned?"
 - a) If yes, please describe the lessons learned and the relationship to privacy and civil liberties concerns or protections.
 - b) Have you modified your privacy policy or business processes as a result of the lessons learned?

DRAFT



Appendix B – Observations of EE Participating Sites During the ISE-SAR EE

A. Overview of Results

All EE participating sites adopted the recommendations in the *Initial Privacy and Civil Liberties Analysis* and implemented the NSI Privacy Framework. This Appendix will address the methodology used during the EE to evaluate implementation policies and procedures and will highlight common themes that emerged during the assessment. This Appendix will also show that each EE participating site had unique experiences in implementing this framework.

B. Methodology

The PM-ISE and DOJ/BJA conducted follow-up assessments of EE implementation through conference calls with each EE participating site in the Fall of 2009. For the purpose of assessing privacy, civil rights, and civil liberties protections, a survey questionnaire²⁷ was developed by the PM-ISE, with input from the PGC Legal Issues Working Group. During conference calls with the EE participating sites, PM-ISE staff used the questionnaire to frame the discussion and then documented the responses from each site in a draft privacy and civil liberties assessment. The draft assessments were electronically submitted to each participating site for formal review and vetting.

Each site was requested to formally review and vet the draft response and to return it to the PGC Executive Director. Four of the twelve sites returned their assessment questionnaires using this process. Given the limited number of corrections to the draft responses made by these four sites, the PM-ISE determined that the draft privacy and civil liberties assessments would suffice for the purposes of analyzing the protection of privacy, civil rights, and civil liberties during the EE.

C. Results of Follow-up Assessments

The experiences of the EE participating sites in implementing the SAR process and the NSI Privacy Framework are summarized as follows:

1. Developing Privacy Policies Consistent with ISE Privacy Guidelines

With respect to policy alignment, a number of sites had privacy policies in place prior to participating in the ISE-SAR EE consistent with their State and local requirements. However, all of the EE participating sites noted that they devoted additional effort and resources to ensuring

²⁷ See ISE-SAR EE Privacy and Civil Liberties Assessment Survey Questionnaire contained in Appendix A of this Analysis.

that their existing privacy policies and procedures were fully compliant with the privacy, civil rights, and civil liberties requirements for ISE-SAR participation.

The development and implementation of the elements of the privacy policy framework generally took longer than anticipated at most EE participating sites. Most sites reported an average length of about six months to develop, review, approve, and implement the policy for the following reasons:

- 1) A number of sites experienced delays in coordinating the review of draft privacy policies with internal and external stakeholders; and
- 2) Coordinating the review and approval of policies between multiple State and local parties, including legal counsels, required several iterations of draft policy documents and extended the length of time before which the EE participating site was authorized to “go live” in sharing and receiving Privacy Field information.

These delays resulted in an inability to participate in information sharing activities for several sites. A few sites found that assigning a staff member as the single point of contact for development and coordination was a key factor in getting privacy policies completed faster.

The designation of privacy officials proved to be another area for improvement. There has been nominal progress in putting privacy officers in place at EE participating sites. Many sites noted that they were in the process of hiring a privacy officer or privacy and civil liberties subject matter expert.

To address this issue, most sites relied upon internal or departmental legal staff to determine the applicable SLT legal and regulatory requirements to be incorporated into ISE-SAR privacy policies. Some sites relied upon the expertise of records managers and compliance officers in the development and review of ISE-SAR policies. One site sought an extensive policy review from a variety of external stakeholders, including review by the state's advisory board on privacy and civil liberties, citizen advisory groups, and site partner agency legal counsels. Another site noted that while it did not involve the state's homeland security privacy officer in the development of its privacy policy, the site does coordinate with this privacy officer in planning other operational initiatives.

Some states have both a state fusion center and one or more Urban Area Security Initiative (UASI) fusion center sites in the state. None of the UASI sites coordinated with its designated state fusion center on the development of its privacy policy.

2. Privacy Policy Adoption and Community Outreach

Implementation strategies for adopting privacy and civil liberties policies and processes varied across the twelve EE participating sites. Every site with a privacy policy in place during the EE required personnel²⁸ involved in the SAR process to review and certify acceptance of the site's

²⁸ This included personnel assigned to the center from other organizations.

privacy policy. A number of sites plan to or are in the process of developing in-house training modules.

The majority of outreach efforts to the public and to privacy and civil liberties advocacy groups occurred after the site completed development of its privacy policy. Sites pursued varying approaches to informing the public. A number of sites posted privacy policies to a public website, either a fusion center-specific or Departmental website. Other sites chose to include information on the ISE-SAR process in agency command and staff presentations. Finally, one site organized community training sessions on the SAR process, to include training on privacy and civil liberties, as part of its larger community outreach efforts.

A few sites focused on outreach to local advocacy groups as part of their commitment to transparency throughout the development and implementation of the SAR process. All of these sites confirmed the critical role of transparency in addressing concerns of citizens and watchdog groups. One site walked staff from the local ACLU through the site's Special Orders and Process steps; now, the ACLU is a partner that regularly compliments this site's efforts to protect privacy and civil liberties. A few sites also discussed holding open house events and providing facility tours. Another means of outreach involved the "Building Communities of Trust" initiative, where EE participating sites invited local privacy and civil liberties advocacy groups to participate in planning meetings and subsequent outreach events.

With respect to the use of Privacy Impact Assessments (PIAs) as a tool for ensuring transparency, very few sites were familiar with the concept of PIA. Only one of the EE participating sites has conducted a PIA. Two sites indicated that command staff was considering conducting a PIA sometime in the future. A brief description of a PIA was provided to the remaining sites, after which several sites noted that it sounded useful and recommended that guidance and templates for use of PIAs be made available to NSI sites.

3. Integrating Privacy Protections into Business Processes

The *Initial Privacy and Civil Liberties Analysis* recommended that sites "integrate the management of [SAR] processes with existing processes and systems . . . thereby leveraging existing policies and protocols that protect privacy, civil rights, and civil liberties." All EE participating sites confirmed their full compliance with the SAR Functional Standard. However, some sites found that they needed to update their existing business processes and procedures to comply with requirements of their privacy policies. For example, one site specifically described how it had changed existing business processes to comply with privacy policy requirements for redress, labeling, data quality, retention, and purging.

As for the sites' SAR submission status, most sites described business processes that included a requirement to provide feedback status to SAR originators. Those still engaged in developing an implementation strategy reported plans to include a process for providing feedback to source agencies (the agency documenting/submitted the SAR) that the SAR has been designated as an ISE-SAR. Finally, in cases where EE participating sites referred ISE-SARs to the

local FBI Joint Terrorism Task Force (JTTF), most of the sites have policies for notifying the source agency of the referral to the JTTF.

With respect to monitoring the status of ISE-SARs submitted to JTTFs, a number of sites reported terminating tracking/final outcomes upon submission of the ISE-SAR to the JTTF.

The sites were also assessed in terms of whether and to what extent they provided feedback on erroneous SAR information. Most sites indicating that feedback would be provided to the original submitter when SARs contained erroneous information. Several sites also indicated that SARs would be updated to correct the erroneous information. Few sites reported using labels to indicate when a SAR contained erroneous information. The majority of participants, however, confirmed that quality controls built into the SAR vetting process, especially multiple levels of analysis and review, would minimize the possibility of posting an ISE-SAR with erroneous information to the ISE Shared Space. Additionally, several sites emphasized the need to ensure that all NSI participating sites strictly adhere to the vetting and feedback processes to assure information quality and integrity.

With respect to inadvertent sharing, the *Initial Privacy and Civil Liberties Analysis* acknowledged the concerns of some advocates that the privacy and civil liberties of individuals could be placed at risk in the event that an ISE-SAR containing personal information was inadvertently shared. However, it is significant to note that none of the participants reported any instances where ISE-SARs were inadvertently shared. Moreover, all sites had established departmental policies and processes in place to address an inappropriate use of information or data breaches, should such a breach occur.

As for quality control and auditing, the majority of EE participating sites reported that they are subject to regular audits by Internal Affairs or Inspectors General offices. Quality control and audit functions were also performed through daily reviews of new SARs and ISE-SARs by senior level and/or experienced staff. This process served to address quality control and auditing needs.

4. Profiling Protections and Constitutional Rights

All EE participating sites reported strong emphasis within their departments and agencies on upholding constitutional rights of individuals and avoidance of any actions that could be interpreted as profiling. All sites cited training programs for site personnel and partners that focused on the importance of behavior-based SAR collection, i.e. gathering information associated with suspicious behavior rather than suspicious persons.

The supporting departments or agencies of a number of EE participating sites have previous experience with mitigating the risk of “profiling” based upon race, ethnicity, national origin, religion, etc. At least two sites noted that their departments were subject to tracking and auditing requirements for “profiling” activities at vehicle traffic stops as a result of earlier lawsuits or Federal consent decrees. Several sites reported rejecting or avoiding the use of any SAR that included information which could create the appearance of profiling or could impact an individual’s civil rights or civil liberties, even if that information came from a partner agency

or the site's supporting department or agency. Moreover, in cases where a SAR meets the criteria of an ISE-SAR, any formats containing race or ethnicity information that are not deemed critical to the ISE-SAR are not uploaded to the ISE Shared Space.

Many sites were subject to mandates for regular training of all personnel (e.g. sworn officers or State employees) on civil rights and civil liberties issues, including the First and Fourth Amendments. Additionally, many sites provide follow-up feedback and training to front-line officers or partner agencies if these sources submit SARs that contain information that indicates profiling based on factors such as race or ethnicity.

Finally, there were no reports or complaints of privacy or civil liberties violations at any participating sites. All sites reported the existence of a formal process within their supporting departments or agencies to review, investigate, and address such complaints.

5. Training and Documentation

Most sites indicated a reliance upon existing privacy and civil liberties training offerings from Federal partners. All sites reported that their site personnel have achieved Federal 28 CFR Part 23 training certification and participated in SAR training (chief executive, analyst, and front-line officer training). Some sites have sent personnel to attend training conducted by DOJ BJA and DHS at regional fusion center conferences and meetings. Some of the sites had sent personnel to attend civil rights and civil liberties training sessions conducted by the DHS Office of Civil Rights and Civil Liberties. A number of EE participating sites also reported supplementing this training through the use of local civil liberties training which also covered First and Fourth Amendment issues and state privacy and civil liberties laws.

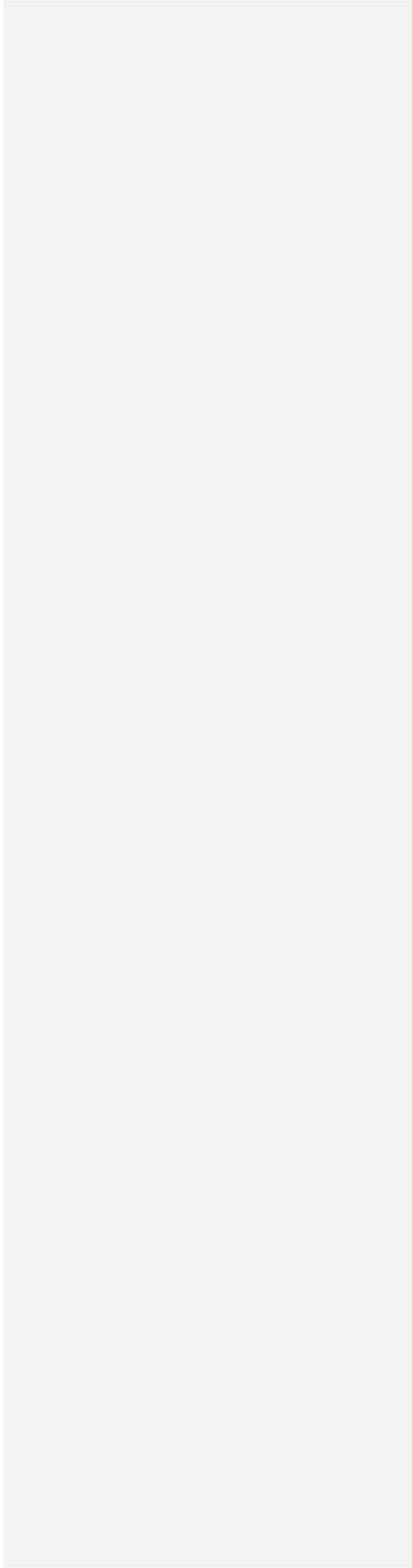
As for the development of in-house and academy training, many sites reported ongoing efforts or plans to develop in-house training for site personnel and partners on privacy and civil liberties requirements for the ISE-SAR process and are working with police academies to develop a curriculum for new cadets and in-service [continuing officer] training. The majority of sites specified that training curricula would include a focus on training front-line officers to establish clear expectations of the information gathering requirements for SARs given that front line officers generate the largest number of incoming reports. A number of sites also reported that their police academies have already integrated information on the SAR process, including information on privacy policies, into current cadet training and in-service training offerings.

Several EE participating sites remarked upon the differences in perspective and understanding between law enforcement and non-law enforcement personnel with respect to the SAR process. All of these sites confirmed that training is critical to bridging these perspective differences and that training should be provided at regular opportunities.

Finally, the assessment covered the training of citizenry. Citizens are a source of reporting SAR information that is documented by law enforcement agencies and a few sites have devoted time and attention to the training of citizens as a way to improve the relevancy of incoming information pertaining to suspicious behavior from the public. One site noted that information on the SAR process has been incorporated into the curriculum of the city's citizen academy.

Another reported providing feedback directly to citizens who have called in to report tips, particularly when those reports don't contain information indicative of suspicious behavior. One site commander provided suspicious behavior training to an individual citizen who called to report that several men of Middle Eastern origin had moved into the house next to her property; the site noted that training of citizens is part of the site's ongoing commitment to ensuring a focus on the recognition and reporting of suspicious behaviors and not on personal attributes.

DRAFT



Appendix C – Organizations That Participated in Outreach Efforts

Privacy and Civil Liberties Advocates

American-Arab Anti-Discrimination Committee

American Civil Liberties Union of Southern California

American Civil Liberties Union - Washington Legislative Office

Center for Democracy and Technology

Electronic Information Privacy Center

Freedom and Justice Foundation

Islamic Shura Council of Southern California

Muslim Advocates

Muslim Public Affairs Council

State, Local, and Tribal Law Enforcement Agencies

Georgia Bureau of Investigation

Intelligence Fusion Center
Iowa Department of Public Safety

Los Angeles Police Department

Los Angeles City Attorney's Office
New Jersey State Police

Pennsylvania State Police

Washington State Fusion Center
Seattle Police Department

Law Enforcement Professional Organizations

American Probation and Parole Association

Federal Agencies

Civil Liberties and Privacy Office
Office of the Director of National Intelligence

Information Sharing and Collaboration
U.S. Department of Homeland Security

Office of the Chief Information Officer
U.S. Department of Justice

Bureau of Justice Assistance
Office of Justice Programs
U.S. Department of Justice

National Threat Center Section
Counterterrorism Division
Federal Bureau of Investigation

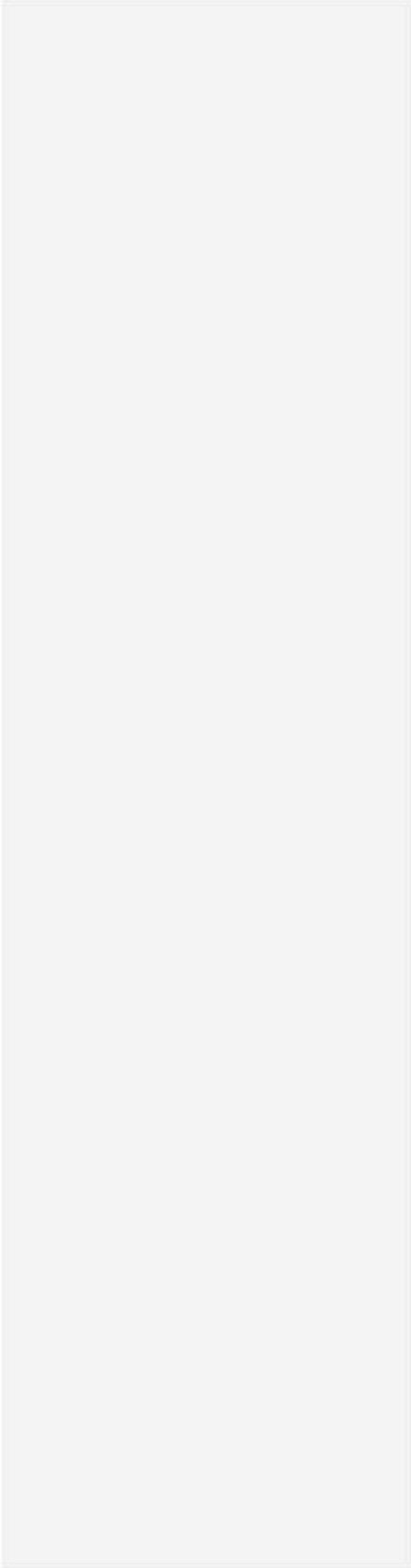
Acting Chief Privacy and Civil Liberties
Officer
Office of the Deputy Attorney General
U.S. Department of Justice

State and Local Program Office
U.S. Department of Homeland Security

Privacy and Civil Liberties Unit
Office of the General Counsel
Federal Bureau of Investigation

Office of the Program Manager,
Information Sharing Environment

DRAFT



Appendix D – Acronyms and Abbreviations

ACLU	American Civil Liberties Union
BJA	Bureau of Justice Assistance
DHS	Department of Homeland Security
DoD	Department of Defense
DOJ	Department of Justice
EE	Evaluation Environment
FBI	Federal Bureau of Investigation
ISE	Information Sharing Environment
JTTF	Joint Terrorism Task Force
NSI	Nationwide Suspicious Activity Reporting Initiative
ODNI	Office of the Director of National Intelligence
PIA	Privacy Impact Assessment
PGC	Privacy Guidelines Committee
PM-ISE	Program Manager, Information Sharing Environment
SAR	Suspicious Activity Reporting
SLT	State, local, and tribal
UASI	Urban Area Security Initiative

Appendix E – Referenced Documents

This appendix provides a comprehensive listing of the documents referenced in this Analysis.

Baseline Capabilities for State and Major Urban Area Fusion Centers: A Supplement to the Fusion Center Guidelines (September 2008)

<http://it.ojp.gov/documents/baselinecapabilitiesa.pdf>

The 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 (“ISE Privacy Guidelines”) (December 2006),

<http://www.ise.gov/docs/privacy/PrivacyGuidelines20061204.pdf>.

National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing (October 2007),

http://www.ise.gov/docs/nsis/nsis_book.pdf.

The Initial Privacy and Civil Liberties Analysis of the Information Sharing Environment - Suspicious Activity Reporting (ISE-SAR) Functional Standard and Evaluation Environment (September 2008),

http://www.ise.gov/docs/sar/ISE_SAR_Initial_Privacy_and_Civil_Liberties_Analysis.pdf.

Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project, (October 2008),

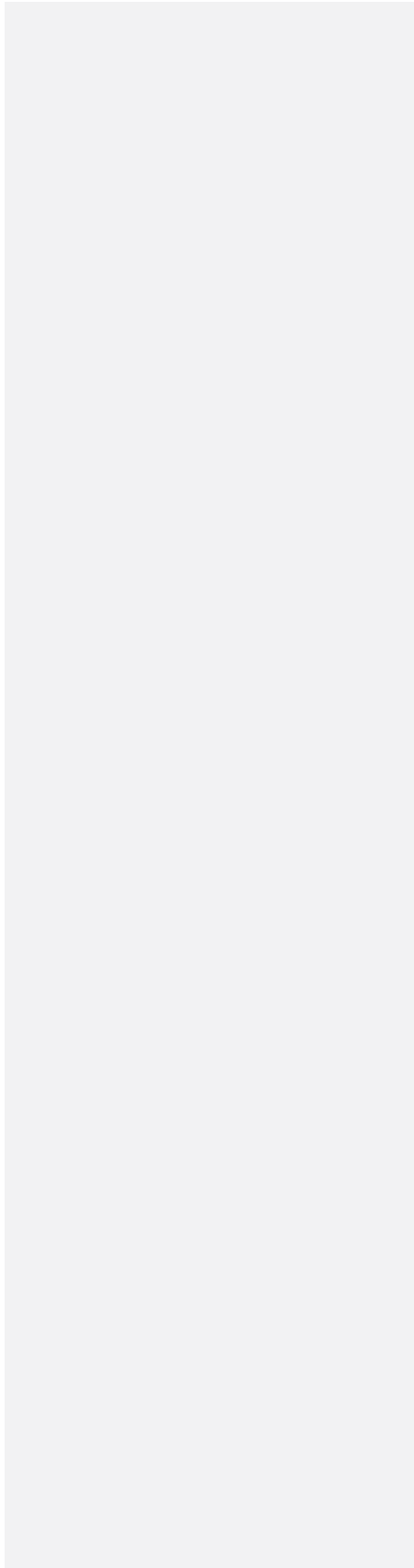
http://www.it.ojp.gov/documents/SAR_Report_October_2008.pdf

The ISE-SAR Functional Standard, Version 1.5 (May 2009),

http://www.ise.gov/docs/ctiss/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf

Final Report: Information Sharing Environment Suspicious Activity Reporting Evaluation Environment (January 2010), Department of Justice Bureau of Justice Assistance.

The Nationwide Suspicious Activity Reporting Initiative Status Report (February 2010), Office of the Program Manager for the Information Sharing Environment.



Office of the Director of National Intelligence
Attention: Program Manager, Information Sharing Environment
Washington, DC 20511

(202) 331-2490

For more information, go to:

<http://www.ise.gov>



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

PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES ANALYSIS AND RECOMMENDATIONS

NATIONWIDE SUSPICIOUS ACTIVITY REPORTING INITIATIVE

**Prepared by the
Program Manager, Information Sharing Environment**

July 2010

Table of Contents

I. Introduction 3

II. The Critical Role of Privacy, Civil Rights, and Civil Liberties Protections in the ISE-SAR EE 5

III. Recommendations for the Nationwide Implementation of the NSI in 2010 5

IV. Policies and Processes Supporting the NSI Privacy Framework..... 12

 A. Recommendations of the *Initial Privacy and Civil Liberties Analysis* 12

 B. Strengthening the NSI Privacy Framework through Collaboration with Privacy, Civil Rights, and Civil Liberties Advocacy Groups..... 12

 C. The Revised ISE-SAR Functional Standard..... 14

 1. *The Process for Identifying, Documenting, and Sharing SAR Information and the Protection of Privacy, Civil Rights, and Civil Liberties of Americans*..... 14

 2. *The Standardized, Multi-Level Vetting Process*..... 16

 D. Standardized Approach to Privacy, Civil Rights, and Civil Liberties Privacy Policies 17

 E. Federal Privacy Technical Assistance and Training 17

V. Success Stories and Best Practices from EE Sites..... 18

 A. Success Stories 18

 B. Best Practices..... 19

VI. Conclusion..... 19

Appendix A – ISE-SAR EE Privacy and Civil Liberties Assessment Questionnaire 20

Appendix B – Observations of EE Participating Sites During the ISE-SAR EE..... 24

 A. Overview of Results..... 24

 B. Methodology..... 24

 C. Results of Follow-up Assessments 24

Appendix C – Organizations That Participated in Outreach Efforts..... 30

Appendix D – Acronyms and Abbreviations 32

Appendix E – Referenced Documents and Resources 33

I. Introduction

This *Nationwide Suspicious Activity Reporting Initiative (NSI) Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations* (“*Analysis*”) provides an update to the *Initial Privacy and Civil Liberties Analysis*¹ of the now concluded Information Sharing Environment Suspicious Activity Reporting (ISE-SAR) Evaluation Environment (EE) and Functional Standard.² The *Initial Privacy and Civil Liberties Analysis* reflects the commitment to ensuring that privacy, civil rights, and civil liberties protections were built into the policies and processes of the sites³ participating in the ISE-SAR EE and resulted in: (1) the revision and adoption of the ISE-SAR Functional Standard (“revised Functional Standard”), currently Version 1.5⁴; and (2) the development of a robust and comprehensive privacy, civil rights, and civil liberties protection framework for the NSI, known as the NSI Privacy Framework.⁵

The EE served as the demonstration phase or pilot phase of the NSI. The initial sites that participated in the EE implemented the recommendations from the *Initial Privacy and Civil Liberties Analysis* and currently participate in the NSI. Additional sites will be added now that the Initiative has moved from the demonstration phase of the EE to the nationwide implementation of the NSI.

The EE validated the recommendations of the *Initial Privacy and Civil Liberties Analysis*, thus enabling Federal partners to draw upon the experiences of the EE participating sites in fortifying and refining the NSI Privacy, Civil Rights, and Civil Liberties Framework.⁶ The enhanced framework is comprised of the recommendations from the *Initial Privacy and Civil*

¹ *Information Sharing Environment – Suspicious Activity Reporting Functional Standard and Evaluation Environment: Initial Privacy and Civil Liberties Analysis* (September 2008).

² Further information regarding the development and implementation of the EE can be found in the accompanying reports: (1) *Final Report: Information Sharing Environment Suspicious Activity Reporting Evaluation Environment* (January 2010) (*Final Report: ISE-SAR EE*) from the Department of Justice Bureau of Justice Assistance; and (2) *The Nationwide Suspicious Activity Reporting Initiative Status Report* (February 2010), from the Office of the Program Manager for the Information Sharing Environment.

³ The EE ultimately encompassed twelve NSI Environment sites and three Federal agencies. The EE participating sites included: Boston Police Department (PD), Chicago PD, Florida Department of Law Enforcement (FDLE), Houston PD, Las Vegas Metropolitan PD, Los Angeles PD (LAPD), Metropolitan (Washington) DC PD, Miami-Dade Fusion Center, New York State Intelligence Center, Arizona Counter Terrorism Information Center, Seattle Police Department and the Virginia Fusion Center. As for the Federal agencies involved in the EE, the Federal Bureau of Investigations (FBI) participated through its eGuardian system; the Department of Homeland Security (DHS) shared Federal Air Marshal Service (FAMS) data; and the Department of Defense (DoD) — also using eGuardian—gathered and shared SARs in support of its Force Protection mission. Not all sites and agencies are sharing data at this time due to the requirement that each site fully implement the NSI Privacy Framework.

⁴ All references to the “revised ISE-SAR Functional Standard” refer to Version 1.5

⁵ See Section IV of this *Analysis* for a comprehensive discussion of the NSI Privacy Framework.

⁶ Throughout the remainder of this document, the term “NSI Privacy, Civil Rights, and Civil Liberties Framework” is normally abbreviated to “NSI Privacy Framework.”

Liberties Analysis, the revised Functional Standard, and the experiences of the EE participating sites reflected in this Analysis. The implementation of the NSI Privacy Framework will ensure that privacy, civil rights, and civil liberties will continue to be appropriately protected as the Initiative moves beyond the EE to the nationwide implementation of the NSI in 2010. This Analysis was prepared in consultation with the Co-Chairs⁷ of the ISE Privacy Guidelines Committee (PGC) and uses the experiences of the EE participating sites to further build upon the commitment made in the *Initial Privacy and Civil Liberties Analysis* by:

- Reviewing the development and implementation of EE participating sites' privacy, civil rights, and civil liberties protections;
- Outlining the observations of EE participating site experiences;
- Updating the initial privacy and civil liberties issues identified by and resolved between Federal sponsoring agencies, participating State and local partners, and privacy, civil rights, and civil liberties advocates during the EE; and
- Making recommendations to be followed during the nationwide implementation of the NSI.

In sum, the NSI Privacy Framework enabled the EE participating sites to fulfill the dual mandates of maximizing information sharing while protecting privacy, civil rights, and civil liberties. The effectiveness of this framework is underscored by the fact that the EE participating sites did not report any breaches of personal information with regard to SAR or ISE-SAR information. Nor did they receive any complaints for redress during the EE.

Going forward, NSI participants must continue to work together to ensure that robust privacy policies and procedures are adopted, properly implemented, and continuously assessed. Participants must also actively seek out opportunities to further enhance privacy, civil rights, and civil liberties protections.

⁷ The Co-Chairs of the ISE Privacy Guidelines Committee are the Chief Privacy and Civil Liberties Officer, Department of Justice; the Civil Liberties Protection Officer, Office of the Director of National Intelligence; the Chief Privacy Officer, Department of Homeland Security; and the Officer for Civil Rights and Civil Liberties, Department of Homeland Security. In addition, the Chair of the PGC Legal Issues Working Group contributed to the development of this Analysis as well as the questionnaire found in Appendix A.

II. The Critical Role of Privacy, Civil Rights, and Civil Liberties Protections in the ISE-SAR EE

The key objective of the ISE-SAR EE was to establish, at each of the EE participating sites, policies and business processes that support the gathering, documenting, processing, analyzing, and sharing of SARs while also ensuring that privacy, civil rights, and civil liberties were protected in accordance with Federal, state, and local constitutions, laws, and regulations. As a condition of participation, the EE participating sites were required to implement a privacy, civil rights, and civil liberties protection framework. This framework included the adoption of appropriate policies, the institution of specialized business processes, and the training of all involved personnel before they were permitted to post or access ISE-SARs.

The EE enabled participants to assess the value of the ISE-SAR process and the ISE-SAR Functional Standard⁸ and to provide a limited evaluation of the value of the Detailed versus Summary ISE-SAR formats⁹ in advancing counterterrorism goals. Following the end of the EE pilot phase, all participants provided feedback to Federal privacy officials regarding the administrative and procedural aspects of the Initiative, including the process for designating reports as ISE-SARs, the management of postings in the ISE Shared Space, the processes for correcting inaccurate information, and other relevant program implementation issues. The ISE-SAR EE proved to be a valuable tool for refining the recommendations made in the *Initial Privacy and Civil Liberties Analysis*, and confirming that these recommendations must be addressed in the nationwide implementation of the NSI.¹⁰

III. Recommendations for the Nationwide Implementation of the NSI in 2010

The ISE-SAR EE resulted in significant implementation progress, while revealing areas that will require enhanced focus during the broader NSI implementation in 2010. Although the sites'

⁸ The ISE-SAR Top-Level Business Process is set forth in Section II(D) of the ISE-SAR Functional Standard, Version 1.5 (May 2009).

⁹ See *Final Report: ISE-SAR EE*, at pages 11 and 43, for a discussion of the EE participating sites' use of the Summary and Detailed formats. The participating sites' evaluation was limited because the Evaluation Environment operated for a relatively short period of time. More data will be necessary to provide a full assessment of the implementation of the NSI Privacy Framework. It is, therefore, recommended that the NSI continue to evaluate the benefits of the Detailed and Summary ISE-SAR formats.

¹⁰ The Program Manager for the Information Sharing Environment (PM-ISE) and the Department of Justice Bureau of Justice Assistance (DOJ BJA) conducted follow-up assessments of EE implementation using a questionnaire. See Appendix A for the ISE-SAR EE *Privacy and Civil Liberties Assessment Questionnaire*, and Appendix B for the *Observations of EE Participating Sites During the ISE-SAR EE*.

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

NSI Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations

- d. Other sites hosted community open house days and/or provided tours of facilities upon request from the public or the media; and
- e. Several have reported plans to make the privacy policy available on a public website, either a fusion center-specific or Departmental website.

Going forward, the following controls should be implemented in order to further promote transparency and collaboration. First, the sites must ensure the broadest possible review of privacy policies and procedures, with due consideration given to stakeholder recommendations. Second, the sites must consistently provide thorough explanations in response to public inquiries about sites' privacy policies, information availability, and redress procedures. Third, the methods used by the sites to promote outreach and collaboration must be continually assessed for the purpose of identifying and sharing best practices. Transparency and collaboration will foster public trust and enable sites to better respond to the concerns of citizens and advocacy groups.

RECOMMENDATION 3: To mitigate the risk of profiling based on race, ethnicity, national origin, or religion, and to improve mission effectiveness, NSI participating sites must adhere to the standardized vetting process and consistently use the ISE-SAR Functional Standard criteria in the identification, documentation, and sharing of ISE-SAR information.

Federal, State, and local NSI partners recognize that mitigation of the risks associated with profiling is critical to the success of the Initiative. NSI partners must, therefore, remain vigilant in implementing the enhanced privacy, civil rights, and civil liberties protections for SARs and ISE-SARs, in order to avoid the dangers of profiling.

The privacy, civil rights, and civil liberties protections are multi-faceted and robust. First, NSI partners must implement the standardized vetting process for SARs. Second, NSI partners must ensure the consistent and objective application of the revised ISE-SAR Functional Standard criteria. The implementation of the revised ISE-SAR Functional Standard constitutes an essential safeguard supporting the NSI Privacy Framework and enhancing mission effectiveness. The revised Functional Standard expressly states that factors such as race, ethnicity, national origin, or religious affiliation or activity should not be considered as the sole factors that create suspicion (except if used as part of a specific suspect description). The revised Functional Standard serves as the basis for information to be collected for a SAR or ISE-SAR and shared by law enforcement, homeland security, and counterterrorism agencies; therefore the ISE-SAR Functional Standard must be fully and consistently implemented in each NSI site's policies and business processes. Third, NSI partners must provide specialized

able to distinguish between innocent cultural behaviors and behavior indicative of criminal activity; and local communities will play a more supportive role in combating terrorism-related crime.

NSI Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations

training and guidance to NSI personnel in order to strengthen the ability of personnel to recognize suspicious behaviors in a uniform and objective manner. Finally, as the NSI effort grows, Federal, State, and local NSI partners must regularly assess the sites' vetting process, including determinations of "reasonably indicative", and efforts to prevent profiling.

RECOMMENDATION 4: The sites must designate a trained privacy, civil rights, and civil liberties officer who, in addition to carrying out delegated responsibilities, has access to the services of legal counsel with sufficient expertise to provide ongoing legal advice and assistance regarding privacy, civil rights, and civil liberties.

The EE demonstrated that each site should designate a privacy, civil rights, and civil liberties officer and, as needed, ensure that such officer is properly trained. The designated officer, if not an attorney, should have access to legal expertise in developing and implementing privacy, civil rights, and civil liberties policies and procedures and resolving legal issues. Few EE participating sites were able to designate or hire personnel with subject matter expertise to manage privacy, civil rights, and civil liberties issues on a full-time basis. In most cases, the sites relied upon legal staff from parent agencies or state attorney general offices to identify the relevant State and local legal and regulatory requirements for incorporation in their respective ISE-SAR or comprehensive privacy, civil rights, and civil liberties policies. Sites also used records managers and compliance officers to ensure ISE-SAR policy compliance with state open records laws and other state and local requirements.

Access to the services of a subject matter expert in the areas of privacy, civil rights, and civil liberties would have expedited privacy policy development and implementation during the EE and would have enabled the sites to access or share personal information contained in Privacy Fields earlier. Privacy officers and legal counsel are therefore necessary to ensure compliance with NSI Privacy Framework and to identify opportunities to further enhance privacy, civil rights, and civil liberties protections.

RECOMMENDATION 5: An ongoing, formalized review process must be established to ensure that business processes are aligned with privacy policies and procedures, and to assess the need for additional privacy, civil rights, and civil liberties protections.

All ISE-SAR EE participating sites recognized the importance of intermittently conducting reviews of their privacy policies and business processes. Many sites also indicated that they would conduct interim policy reviews as needed.

In order to ensure a standardized approach, a formalized review process must be established. At least annually, an onsite review team should assess adherence to and implementation of the NSI Privacy Framework. The review should include: (1) an assessment of accountability

actions, including documented changes in business processes that reflect the enhanced privacy protections; (2) documentation of any breaches involving personal information; (3) an assessment of the handling of information requests, error notifications, and complaints for redress; and (4) documentation of the delivery of required training activities.

RECOMMENDATION 6: Each participating site must exercise due diligence in implementing appropriate physical, technical, and administrative measures to safeguard information under its control from unauthorized access, disclosure, modification, use, or destruction.

The EE served to highlight security controls which are critical for ensuring appropriate safeguarding of personal information. Going forward, all NSI sites must exercise due diligence by:

- a. Limiting access to ISE-SARs to agencies and individuals with proper credentials and roles;
- b. Requiring a reason for all searches;
- c. Implementing an appropriate electronic warning banner for users accessing the ISE Shared Space;
- d. Mandating the maintenance of inquiry/access logs and audit trails; and
- e. Requiring that all records provide notice about the nature and quality of the information, including confidence and dissemination codes.

RECOMMENDATION 7: Each participating site must emphasize and establish procedures to ensure personal responsibility and accountability for protecting privacy, civil rights, and civil liberties.

Although none of the EE participating sites reported a breach of personal information with regard to SAR or ISE-SAR information, personnel must remain vigilant in adhering to the site's privacy protection framework. Each site should ensure that all assigned personnel with access to SAR and ISE-SAR information review and acknowledge, on an annual basis, that they have read and understand the site's privacy policies and procedures and that they will execute their responsibilities in accordance with the site's policies and procedures.¹⁵

Sites should provide and require privacy training regarding their privacy policies, procedures, business processes, and updates thereto. NSI sites should also provide ongoing training which focuses on safeguarding personal information. Such training would strengthen the ability of personnel to prevent breaches involving personal information and should underscore the obligations of personnel to report privacy policy violations and breaches involving personal

¹⁵ This requirement should apply to all personnel, including employees, contractors, and other support personnel. Some EE participating sites also provided training to personnel from other state and local partner agencies.

information. Training should be structured to ensure that personnel are informed of their individual, job-related responsibilities for protecting privacy, civil rights, and civil liberties and the consequences for violation of those responsibilities. Finally, to address some confusion regarding documentation of SARs (and subsequently ISE-SARs), personnel at source agencies and NSI sites should receive training in making “reasonably indicative” determinations.

RECOMMENDATION 8: Federal sponsoring agencies should work to ensure that technical assistance, guidance, and support focusing on privacy policy adoption, implementation, and training remain available and are expanded as needed to serve all NSI sites.

The sites confirmed that the technical assistance provided during the ISE-SAR EE facilitated each site’s development and implementation of the privacy protection framework. Federal partners should ensure that technical assistance and training teams are available to NSI sites to ensure that adequate resources and policy guidance are available to resolve NSI issues.

RECOMMENDATION 9: When ISE Shared Spaces become better populated with new ISE-SARs, Federal partners should devise and conduct a more robust test of the value of the Summary Format.

During the EE, two data formats were developed for packaging ISE-SARs, namely, the Summary format and the Detailed format. The Summary format excludes Privacy Field information containing personally identifiable information (PII), whereas the Detailed format includes such information.¹⁶ The Federal partners and the EE participating sites were not able to fully assess the utility of the Summary format due to a lack of sufficient data. There may, however, be value in making data in the Summary Format available to non-law enforcement public safety agencies, entities involved in critical infrastructure protection, terrorism researchers, subject matter experts, and first responders for use in identifying patterns and trends, on condition that appropriate privacy, civil rights, and civil liberties safeguards are in place.

RECOMMENDATION 10: Federal, State, local, and Tribal agencies should ensure that the experiences gained during the ISE-SAR EE and the fuller NSI implementation are considered as other ISE capabilities are developed.

Although the privacy, civil rights, and civil liberties concerns addressed in this Analysis are discussed in the context of the NSI, these concerns are not unique to SAR and ISE-SAR information. SARs are but one source of terrorism-related information, and the policies, procedures, and processes developed to handle SARs may also directly apply to other types of

¹⁶ For further information regarding the EE participating sites’ use of these formats, see *Final Report: ISE-SAR EE*, at pages 11 and 43.

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

rights, and civil liberties advocacy groups.¹⁷ Advocacy groups served an essential role in shaping the privacy protection framework for ISE-SAR information sharing activities by assisting with the development and review of products (e.g., templates and training), and by participating in several meetings with the ISE-SAR EE implementation team to address EE implementation efforts.

These meetings confirmed that the implementation of privacy protections would require a multi-faceted and iterative approach. The PM-ISE and its Federal partners looked to the experiences of the sites during the EE for validation of the recommendations from the *Initial Privacy and Civil Liberties Analysis* and verification that the recommendations had application to the broader National SAR Initiative. The experiences of the EE participating sites confirmed the value of the NSI Privacy Framework as an appropriate minimum standard for protection in view of the fact that hundreds of qualifying ISE-SARs were successfully posted to the Shared Space and that there were no incidents of inadvertent sharing of such data.

NSI partners agree that the following elements are the minimum essential measures for the NSI Privacy Framework and are the key to meaningful privacy and civil rights/civil liberties protections:

1. Each NSI participating agency must conduct the NSI process pursuant to its statutory authorities and its privacy, civil rights, and civil liberties policies and procedures that are consistent with the ISE Privacy Guidelines;
2. Each NSI participating agency must submit privacy, civil rights, and civil liberties policies and procedures for review to ensure consistency with the ISE Privacy Guidelines prior to posting or accessing personal information (i.e., Privacy Fields) in the ISE Shared Space;
3. Implementation must include training of front-line, investigative, analytic, and supervisory personnel regarding their respective site's privacy policy, as well as behaviors and indicators of terrorism-related criminal activity;
4. Each NSI participating agency must institute 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; and
5. Sites should engage in outreach and collaboration at a local level with privacy, civil rights, and civil liberties advocacy groups.

Adherence to and implementation of all elements of the NSI Privacy Framework are essential preconditions to sharing personal information contained in Privacy Fields. Compliance with this approach will not only strengthen the protection of privacy, civil rights, and civil liberties

¹⁷ See Appendix C for a listing of the advocacy groups which participated in the collaborative process.

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.

D. Standardized Approach to Privacy, Civil Rights, and Civil Liberties Privacy Policies

A critical first step for each NSI site in implementing the NSI Privacy Framework is the development of a written privacy policy as a precondition to sharing or receiving any personal information contained in Privacy Fields. The site's privacy policy must be "at least as comprehensive" as the ISE Privacy Guidelines and the Baseline Capabilities in order to satisfy the requirements of: purpose specification; notice mechanisms; data quality; data security; accountability, enforcement, and audit; and redress.

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 included the following:

1. Completing a comprehensive privacy policy based on DOJ Global Justice's *Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Template*;²⁷
2. Formulating an ISE-SAR specific policy based upon the *ISE-SAR Evaluation Environment Privacy, Civil Rights, and Civil Liberties Protection Policy Template*;²⁸ or
3. Refining its existing privacy policy to ensure that it addressed all the ISE Privacy Guidelines requirements for enhanced protection of terrorism-related information.

Each participating site developed a draft privacy policy and provided it to the Privacy Policy Review Team for assessment and feedback. Once the Privacy Policy Review Team determined that the draft policy was "at least as comprehensive" as the ISE Privacy Guidelines, the team recommended the completed policy for approval to the PGC Co-Chairs and the PM-ISE. Upon approval, DOJ's Bureau of Justice Assistance (BJA) was formally notified that the EE participant was authorized to "go live" in sharing and accessing Privacy Field information in the ISE Shared Spaces.

E. Federal Privacy Technical Assistance and Training

Federal partners provided technical assistance, subject matter expertise, and training to ISE-SAR EE participants. Technical assistance included making privacy, civil rights, and civil liberties subject matter experts available to assist in developing and strengthening participant site privacy policies. The provision of technical assistance enabled Federal partners to ensure a standardized approach to privacy policy development at EE participating sites and to provide guidance regarding privacy and civil liberties issues with widespread impact beyond the state and local level.

²⁷ The Fusion Center Privacy Policy Template was updated in April 2010 to include language for SAR privacy provisions.

²⁸ This template was developed by Federal partners in collaboration with privacy and civil liberties advocacy groups. The PGC's Legal Issues Working Group finalized and approved the template for distribution to the EE participating sites in January 2009.

In addition to assisting with privacy policy development, DHS and DOJ/BJA, through their joint Privacy Technical Assistance Program, developed and provided training on privacy, civil rights, and civil liberties issues to personnel at ISE-SAR EE participant sites. Federal partners also provided role-based ISE-SAR training modules which included privacy, civil rights, and civil liberties components targeted to executives, senior leadership, front-line officers, and analysts.

EE participating sites indicated that privacy technical assistance and training were valuable in maximizing participation in the ISE-SAR EE. They also confirmed that without the provision of assistance, the ISE-SAR EE would not have resulted in meaningful implementation progress.

V. Success Stories and Best Practices from EE Sites

During the follow-up discussions with each EE participating site, several success stories and best practices emerged demonstrating the success of efforts to protect privacy, civil rights, and civil liberties.

A. Success Stories

- The commander of the Florida Fusion Center (FFC) received a telephone call from an individual concerning the FCC's ISE-SAR privacy, civil rights, and civil liberties policy. The FFC commander walked the individual through the privacy policy and protections and answered each of his questions. Upon completion, the caller identified himself as a Certification Assessor from the Commission on Accreditation for Law Enforcement Agencies and congratulated the FFC commander on the thoroughness of her response to his questions.
- Through its formal community outreach campaign, iWatch, the Los Angeles Police Department (LAPD) has informed, trained, and educated its community on SARs including privacy and civil liberties protections at outreach events throughout the Los Angeles metropolitan region. Community training on SAR privacy and civil liberties emphasizes suspicious behaviors over individual characteristics. LAPD considers its iWatch campaign to be the "community part of its SARs process."
- The Florida Department of Health, a state government agency participating in the FFC's terrorism liaison officer program, had previously limited its reporting of SAR information due to its privacy concerns with releasing personal health information. Through the SAR training, the Florida Department of Health understood that its submission to the FFC of SAR information based upon suspicious behaviors was permissible. One of those reports resulted in an open investigation on a person of interest related to terrorism.

B. Best Practices

- The Arizona Counter Terrorism Information Center (ACTIC) actively monitors privacy, civil rights, and civil liberties issues raised by other fusion centers around the country through fusion center regional conferences and other outreach events and uses lessons learned as a guide for adjusting its own policies and procedure.
- The FFC sought an extensive policy review from a variety of external stakeholders, including review by the Florida's state advisory board on privacy and civil liberties, citizen advisory groups, and the legal counsels of all of the site's partner agencies in the process of developing its privacy, civil rights, and civil liberties protection policy.

VI. Conclusion

Since the inception of the NSI, Federal and SLT partners have remained steadfast in their commitment to protecting privacy, civil rights, and civil liberties. In moving from the ISE-SAR EE demonstration phase to the national implementation of the NSI, the NSI Privacy Framework will remain a critical touchstone and be regularly reviewed and updated as necessary. Federal and SLT partners must continue to work together to ensure that robust privacy, civil rights, and civil liberties policies and procedures are adopted, properly implemented, and continuously assessed. The NSI sites must continue efforts to identify opportunities for strengthening and improving privacy, civil rights, and civil liberties protections. The NSI Program Manager's Office should lead efforts to ensure continued oversight of framework implementation, with guidance from the ISE PGC and the President's Privacy and Civil Liberties Oversight Board. Maintaining an unrelenting focus on the protection of privacy, civil rights, and civil liberties will assure the public that the legal rights of all Americans are fully protected and will continue to be a national priority.

Appendix A – ISE-SAR EE Privacy and Civil Liberties Assessment Questionnaire

[AGENCY NAME]
ISE-SAR Evaluation Environment
Final Project Privacy & Civil Liberties Protections Assessment

The purpose of the ISE-SAR Evaluation Environment (EE) was to develop a learning environment in which to determine whether a national standard (the SAR Functional Standard) for reporting and evaluating suspicious activity could facilitate the identification of patterns of criminal activity with a nexus to terrorism. To enable implementation of the ISE-SAR EE, it was essential that policies be implemented for ensuring that privacy, civil rights, and civil liberties are protected in the ISE-SAR identification process and in the sharing of ISE-SAR information. These privacy policies also support transparency to the public regarding the sharing of information about terrorism-related suspicious activity between fusion centers and with other law enforcement and homeland security agencies. This assessment seeks to capture the experience of agencies participating in the ISE-SAR EE regarding development and implementation of privacy and civil liberties protections for identifying and sharing ISE SAR information and the integration of these protections into agency business processes and activities. This Privacy Assessment is a requirement of the *Initial Privacy and Civil Liberties Analysis* of the Suspicious Activity Reporting Functional Standard and Evaluation Environment (September 2008 - Version 1).

Site Visit information

Date: [Date and Time of Call, Eastern Standard Time]
 Method of Visit: Conference Call
 Personnel: [Names and Titles of Site Personnel]

DEVELOPING AND IMPLEMENTING AGENCY PRIVACY POLICIES

- 1) During the ISE-SAR EE, did your agency develop and implement either a comprehensive information and intelligence privacy policy using the Fusion Center Privacy Policy Development Template or an ISE-SAR specific Privacy Policy?
 - a) If so, has the Privacy Policy been promulgated agency wide?
- 2) Has your agency communicated its Privacy Policy to the public, community organizations, and other groups as appropriate?
- 3) Have you conducted a Privacy Impact Assessment for your ISE-SAR activity?
- 4) Did your agency utilize legal/privacy advisors when developing the agency's privacy policy?
- 5) Does the jurisdiction where your agency is located (regional, state, urban) have specific privacy laws or regulations that you incorporated into your privacy policy?
 - a) If yes, please describe these laws or regulations.
 - b) Did any of these laws or regulations impact the development of your agency's privacy and civil liberties policies?
- 6) Does your agency have a plan for regular review of your privacy policy, i.e. biannual review?

IMPLEMENTING AGENCY PRIVACY POLICIES INTO ISE-SAR BUSINESS PROCESSES

- 1) In what ways, if at all, did privacy and civil liberties considerations affect your agency's ability to integrate ISE-SAR activities pre-existing business processes? Describe.
- 2) How does your agency ensure that an ISE-SAR meets the criteria established by the ISE-SAR Functional Standard?
- 3) Does your agency have a mechanism for timely informing the original submitter of SAR information that the SAR has been determined to be an ISE-SAR?
- 4) If an ISE-SAR is determined to be erroneous in content or designation after being posted to the ISE Shared Space, what processes have you implemented to remedy the situation (correction, notice, etc.)?
- 5) What is your procedure for handling SARs that do not meet the criteria of an ISE-SAR? Do you retain and use those SARs and, if so, how do you ensure the privacy and civil liberties protection of those SARs?
- 6) How does your agency ensure that appropriate quality controls are in place for SARs and ISE-SARs (example of controls may include use of labels and markings to indicate questionable accuracy of SAR or ISE-SAR)?
- 7) Are periodic audits of SAR and ISE-SAR data conducted by command-level staff or agency designees?
 - a) If yes, describe your audit process.

ISE-SAR PRIVACY AND CIVIL LIBERTIES PROTECTIONS

- 1) What procedures, both internally and with SAR source agencies, has your agency established to ensure against “profiling” on the basis of race, ethnicity, national origin, religion, or other suspect classifications?
- 2) What procedures, both internally and with SAR source agencies, has your agency established to ensure that individuals’ other Constitutional rights are not violated in the gathering of SAR information?
- 3) Have you received any privacy or civil liberties complaints arising from your SAR or ISE-SAR activities?
 - a) How does your agency handle privacy or civil liberties complaints?
 - b) Do you track complaints? Do you track resolution of complaints?
 - c) Are complaints shared with any external organizations (for example, Attorney General’s office, Inspector General, Internal Affairs, etc.)?
- 4) Has your agency experienced any inadvertent sharing of ISE-SARs (such as a technical or personnel glitch that inadvertently caused a release)?
 - a) Did the inadvertent sharing come to light as sources?
 - b) What procedures does your agency follow to correct an incident where an ISE-SAR is inadvertently shared? Internal fixes? External notification? Other?
 - c) Are cases of inadvertent sharing reported external to your agency? If so, to whom (for example, Attorney General’s office, Inspector General, Internal Affairs, etc.)?

TRAINING AGENCY PERSONNEL ON PRIVACY AND CIVIL LIBERTIES PROTECTIONS AS PART OF THE SAR PROCESS

- 1) Have you trained personnel with ISE-SAR responsibilities on privacy and civil liberties protections applicable to the gathering, processing, analyzing, and sharing of SARs and ISE-SARs?
 - a) Provide examples of training provided to your staff to support the ISE-SAR EE.
- 2) Has your agency identified privacy and civil liberties issues for which additional training is needed?
 - a) If so, what types of additional training would your agency need?

CHALLENGES AND LESSONS LEARNED DURING ISE-SAR EE

- 1) What is the most significant change you have made to business processes as a result of the privacy and civil liberties considerations implicated by the ISE-SAR EE?
 - a) Describe other privacy and civil liberties considerations and resulting process changes.
- 2) Were privacy and civil liberties issues identified in any "lessons learned?"
 - a) If yes, please describe the lessons learned and the relationship to privacy and civil liberties concerns or protections.
 - b) Have you modified your privacy policy or business processes as a result of the lessons learned?

Appendix B – Observations of EE Participating Sites During the ISE-SAR EE

A. Overview of Results

All EE participating sites adopted the recommendations in the *Initial Privacy and Civil Liberties Analysis* and implemented the NSI Privacy Framework. This Appendix will address the methodology used during the EE to evaluate implementation policies and procedures and will highlight common themes that emerged during the assessment. This Appendix will also show that each EE participating site had unique experiences in implementing this framework.

B. Methodology

The PM-ISE and DOJ/BJA conducted follow-up assessments of EE implementation through conference calls with each EE participating site in the Fall of 2009. For the purpose of assessing privacy, civil rights, and civil liberties protections, a survey questionnaire²⁹ was developed by the PM-ISE, with input from the PGC Legal Issues Working Group. During conference calls with the EE participating sites, PM-ISE staff used the questionnaire to frame the discussion and then documented the responses from each site in a draft privacy, civil rights, and civil liberties assessment. The draft assessments were electronically submitted to each participating site for formal review and vetting.

Each site was requested to formally review and vet the draft response and to return it to the PGC Executive Director. Four of the twelve sites returned their assessment questionnaires using this process. Given the limited number of corrections to the draft responses made by these four sites, the PM-ISE determined that the draft privacy and civil liberties assessments would suffice for the purposes of analyzing the protection of privacy, civil rights, and civil liberties during the EE.

C. Results of Follow-up Assessments

The experiences of the EE participating sites in implementing the SAR process and the NSI Privacy Framework are summarized as follows:

1. Developing Privacy Policies Consistent with ISE Privacy Guidelines

With respect to policy alignment, a number of sites had privacy policies in place prior to participating in the ISE-SAR EE consistent with their State and local requirements. However, all of the EE participating sites noted that they devoted additional effort and resources to ensuring

²⁹ See ISE-SAR EE Privacy and Civil Liberties Assessment Survey Questionnaire contained in Appendix A of this Analysis.

that their existing privacy policies and procedures were fully compliant with the privacy, civil rights, and civil liberties requirements for ISE-SAR participation.

The development and implementation of the elements of the privacy policy framework generally took longer than anticipated at most EE participating sites. Most sites reported an average length of about six months to develop, review, approve, and implement the policy for the following reasons:

- 1) A number of sites experienced delays in coordinating the review of draft privacy policies with internal and external stakeholders; and
- 2) Coordinating the review and approval of policies between multiple State and local parties, including legal counsels, required several iterations of draft policy documents and extended the length of time before which the EE participating site was authorized to “go live” in sharing and receiving Privacy Field information.

These delays resulted in an inability to participate in information sharing activities for several sites. A few sites found that assigning a staff member as the single point of contact for development and coordination was a key factor in getting privacy policies completed faster.

The designation of privacy officials proved to be another area for improvement. There has been nominal progress in putting privacy officers in place at EE participating sites. Many sites noted that they were in the process of hiring a privacy officer or privacy and civil liberties subject matter expert.

To address this issue, most sites relied upon internal or departmental legal staff to determine the applicable SLT legal and regulatory requirements to be incorporated into ISE-SAR privacy policies. Some sites relied upon the expertise of records managers and compliance officers in the development and review of ISE-SAR policies. One site sought an extensive policy review from a variety of external stakeholders, including review by the state's advisory board on privacy and civil liberties, citizen advisory groups, and site partner agency legal counsels. Another site noted that while it did not involve the state's homeland security privacy officer in the development of its privacy policy, the site does coordinate with this privacy officer in planning other operational initiatives.

Some states have both a state fusion center and one or more Urban Area Security Initiative (UASI) fusion center sites in the state. None of the UASI sites coordinated with its designated state fusion center on the development of its privacy policy.

2. Privacy Policy Adoption and Community Outreach

Implementation strategies for adopting privacy, civil rights, and civil liberties policies and processes varied across the twelve EE participating sites. Every site with a privacy policy in place during the EE required personnel³⁰ involved in the SAR process to review and certify

³⁰ This included personnel assigned to the center from other organizations.

acceptance of the site's privacy, civil rights, and civil liberties policy. A number of sites plan to or are in the process of developing in-house training modules.

The majority of outreach efforts to the public and to privacy, civil rights, and civil liberties advocacy groups occurred after the site completed development of its privacy policy. Sites pursued varying approaches to informing the public. A number of sites posted privacy policies to a public websites, either a fusion center-specific or Departmental website. Other sites chose to include information on the ISE-SAR process in agency command and staff presentations. Finally, one site organized community training sessions on the SAR process, to include training on privacy, civil rights, and civil liberties, as part of its larger community outreach efforts.

A few sites focused on outreach to local advocacy groups as part of their commitment to transparency throughout the development and implementation of the SAR process. All of these sites confirmed the critical role of transparency in addressing concerns of citizens and watchdog groups. One site walked staff from the local ACLU through the site's Special Orders and Process steps; now, the ACLU is a partner that regularly compliments this site's efforts to protect privacy, civil rights, and civil liberties. A few sites also discussed holding open house events and providing facility tours. Another means of outreach involved the "Building Communities of Trust" initiative, where EE participating sites invited local privacy, civil rights, and civil liberties advocacy groups to participate in planning meetings and subsequent outreach events.

With respect to the use of Privacy Impact Assessments (PIAs) as a tool for ensuring transparency, very few sites were familiar with the concept of PIA. Only one of the EE participating sites has conducted a PIA. Two sites indicated that command staff was considering conducting a PIA sometime in the future. A brief description of a PIA was provided to the remaining sites, after which several sites noted that it sounded useful and recommended that guidance and templates for use of PIAs be made available to NSI sites.

3. Integrating Privacy, Civil Rights, and Civil Liberties Protections into Business Processes

The *Initial Privacy and Civil Liberties Analysis* recommended that sites "integrate the management of [SAR] processes with existing processes and systems . . . thereby leveraging existing policies and protocols that protect privacy, civil rights, and civil liberties." All EE participating sites confirmed their full compliance with the SAR Functional Standard. However, some sites found that they needed to update their existing business processes and procedures to comply with requirements of their privacy policies. For example, one site specifically described how it had changed existing business processes to comply with privacy policy requirements for redress, labeling, data quality, retention, and purging.

As for the sites' SAR submission status, most sites described business processes that included a requirement to provide feedback status to SAR originators. Those still engaged in developing an implementation strategy reported plans to include a process for providing feedback to source agencies (the agency documenting/submitted the SAR) that the SAR has been

designated as an ISE-SAR. Finally, in cases where EE participating sites referred ISE-SARs to the local FBI Joint Terrorism Task Force (JTTF), most of the sites have policies for notifying the source agency of the referral to the JTTF.

With respect to monitoring the status of ISE-SARs submitted to JTTFs, a number of sites reported terminating tracking/final outcomes upon submission of the ISE-SAR to the JTTF.

The sites were also assessed in terms of whether and to what extent they provided feedback on erroneous SAR information. Most sites indicating that feedback would be provided to the original submitter when SARs contained erroneous information. Several sites also indicated that SARs would be updated to correct the erroneous information. Few sites reported using labels to indicate when a SAR contained erroneous information. The majority of participants, however, confirmed that quality controls built into the SAR vetting process, especially multiple levels of analysis and review, would minimize the possibility of posting an ISE-SAR with erroneous information to the ISE Shared Space. Additionally, several sites emphasized the need to ensure that all NSI participating sites strictly adhere to the vetting and feedback processes to assure information quality and integrity.

With respect to inadvertent sharing, the *Initial Privacy and Civil Liberties Analysis* acknowledged the concerns of some advocates that the privacy, civil rights, and civil liberties of individuals could be placed at risk in the event that an ISE-SAR containing personal information was inadvertently shared. However, it is significant to note that none of the participants reported any instances where ISE-SARs were inadvertently shared. Moreover, all sites had established departmental policies and processes in place to address an inappropriate use of information or data breaches, should such a breach occur.

As for quality control and auditing, the majority of EE participating sites reported that they are subject to regular audits by Internal Affairs or Inspectors General offices. Quality control and audit functions were also performed through daily reviews of new SARs and ISE-SARs by senior level and/or experienced staff. This process served to address quality control and auditing needs.

4. Profiling Protections and Constitutional Rights

All EE participating sites reported strong emphasis within their departments and agencies on upholding constitutional rights of individuals and avoidance of any actions that could be interpreted as profiling. All sites cited training programs for site personnel and partners that focused on the importance of behavior-based SAR collection, i.e. gathering information associated with suspicious behavior rather than suspicious persons.

The supporting departments or agencies of a number of EE participating sites have previous experience with mitigating the risk of “profiling” based upon race, ethnicity, national origin, religion, etc. At least two sites noted that their departments were subject to tracking and auditing requirements for “profiling” activities at vehicle traffic stops as a result of earlier lawsuits or Federal consent decrees. Several sites reported rejecting or avoiding the use of any SAR that included information which could create the appearance of profiling or could impact

an individual's civil rights or civil liberties, even if that information came from a partner agency or the site's supporting department or agency. Moreover, in cases where a SAR meets the criteria of an ISE-SAR, any formats containing race or ethnicity information that are not deemed critical to the ISE-SAR are not uploaded to the ISE Shared Space.

Many sites were subject to mandates for regular training of all personnel (e.g. sworn officers or State employees) on civil rights and civil liberties issues, including the First and Fourth Amendments. Additionally, many sites provide follow-up feedback and training to front-line officers or partner agencies if these sources submit SARs that contain information that indicates profiling based on factors such as race or ethnicity.

Finally, there were no reports or complaints of privacy, civil rights, or civil liberties violations at any participating sites. All sites reported the existence of a formal process within their supporting departments or agencies to review, investigate, and address such complaints.

5. Training and Documentation

Most sites indicated a reliance upon existing privacy, civil rights, and civil liberties training offerings from Federal partners. All sites reported that their site personnel have achieved Federal 28 CFR Part 23 training certification and participated in SAR training (chief executive, analyst, and front-line officer training). Some sites have sent personnel to attend training conducted by DOJ BJA and DHS at regional fusion center conferences and meetings. Some of the sites had sent personnel to attend civil rights and civil liberties training sessions conducted by the DHS Office of Civil Rights and Civil Liberties. A number of EE participating sites also reported supplementing this training through the use of local civil liberties training which also covered First and Fourth Amendment issues and state privacy, civil rights, and civil liberties laws.

As for the development of in-house and academy training, many sites reported ongoing efforts or plans to develop in-house training for site personnel and partners on privacy, civil rights, and civil liberties requirements for the ISE-SAR process and are working with police academies to develop a curriculum for new cadets and in-service [continuing officer] training. The majority of sites specified that training curricula would include a focus on training front-line officers to establish clear expectations of the information gathering requirements for SARs given that front line officers generate the largest number of incoming reports. A number of sites also reported that their police academies have already integrated information on the SAR process, including information on privacy policies, into current cadet training and in-service training offerings.

Several EE participating sites remarked upon the differences in perspective and understanding between law enforcement and non-law enforcement personnel with respect to the SAR process. All of these sites confirmed that training is critical to bridging these perspective differences and that training should be provided at regular opportunities.

Finally, the assessment covered the training of citizenry. Citizens are a source of reporting SAR information that is documented by law enforcement agencies and a few sites have devoted time and attention to the training of citizens as a way to improve the relevancy of incoming

information pertaining to suspicious behavior from the public. One site noted that information on the SAR process has been incorporated into the curriculum of the city's citizen academy. Another reported providing feedback directly to citizens who have called in to report tips, particularly when those reports don't contain information indicative of suspicious behavior. One site commander provided suspicious behavior training to an individual citizen who called to report that several men of Middle Eastern origin had moved into the house next to her property; the site noted that training of citizens to identify suspicious behaviors is part of the site's ongoing commitment to ensuring a focus on the recognition and reporting of suspicious behaviors and not on personal attributes, such as national origin, race, ethnicity, religion, or other personal attributions.

Appendix C – Organizations That Participated in Outreach Efforts

Privacy and Civil Liberties Advocates

American-Arab Anti-Discrimination Committee

American Civil Liberties Union of Southern California

American Civil Liberties Union - Washington Legislative Office

Bill of Rights Defense Committee

Center for Democracy and Technology

Electronic Information Privacy Center

Freedom and Justice Foundation

Islamic Shura Council of Southern California

Muslim Advocates

Muslim Public Affairs Council

Rights Working Group

State, Local, and Tribal Law Enforcement Agencies

Georgia Bureau of Investigation

Intelligence Fusion Center
Iowa Department of Public Safety

Los Angeles Police Department

Los Angeles City Attorney's Office
New Jersey State Police

Pennsylvania State Police

Washington State Fusion Center
Seattle Police Department

Law Enforcement Professional Organizations

American Probation and Parole Association

International Association of Chiefs of Police

National Fusion Center Association

Federal Agencies

Civil Liberties and Privacy Office
Office of the Director of National
Intelligence

Community Oriented Policing
Services Office
U.S. Department of Justice

Privacy and Civil Liberties Office
Office of the Deputy Attorney General
U.S. Department of Justice

Chief Privacy Office
U.S. Department of Homeland Security

Office of the Chief Information Officer
U.S. Department of Justice

Office for Civil Rights and Civil
Liberties
U.S. Department of Homeland Security

Bureau of Justice Assistance
Office of Justice Programs
U.S. Department of Justice

Information Sharing and Collaboration
U.S. Department of Homeland Security

Privacy and Civil Liberties Unit
Office of the General Counsel
Federal Bureau of Investigation
U.S. Department of Justice

State and Local Program Office
U.S. Department of Homeland Security

National Threat Center Section
Counterterrorism Division
Federal Bureau of Investigation
U.S. Department of Justice

Office of Counterterrorism and Security
Preparedness
Protection and National Preparedness
Division
Federal Emergency Management
Agency
U.S. Department of Homeland Security

Office of the Program Manager,
Information Sharing Environment

Appendix D – Acronyms and Abbreviations

ACLU	American Civil Liberties Union
BJA	Bureau of Justice Assistance
CR/CL	Civil Rights/Civil Liberties
DHS	Department of Homeland Security
DoD	Department of Defense
DOJ	Department of Justice
EE	Evaluation Environment
FBI	Federal Bureau of Investigation
ISE	Information Sharing Environment
JTTF	Joint Terrorism Task Force
NSI	Nationwide Suspicious Activity Reporting Initiative
ODNI	Office of the Director of National Intelligence
PIA	Privacy Impact Assessment
PGC	Privacy Guidelines Committee
PM-ISE	Program Manager, Information Sharing Environment
SAR	Suspicious Activity Reporting
SLT	State, local, and tribal
UASI	Urban Area Security Initiative

Appendix E – Referenced Documents and Resources

This appendix provides a comprehensive listing of the documents referenced in this Analysis.

The Nationwide Suspicious Activity Reporting Initiative Program Management Office, <http://nsi.ncir.gov/>

Baseline Capabilities for State and Major Urban Area Fusion Centers: A Supplement to the Fusion Center Guidelines (September 2008)
<http://it.oip.gov/documents/baselinecapabilities.pdf>

The 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 ("ISE Privacy Guidelines") (December 2006),
<http://www.ise.gov/docs/privacy/PrivacyGuidelines20061204.pdf>

Fusion Center Privacy Policy Development – Privacy Civil Rights and Civil Liberties Policy Template (April 2010),
<http://it.oip.gov/docdownloader.aspx?ddid=1269>

The ISE-SAR Functional Standard, Version 1.5 (May 2009),
http://www.ise.gov/docs/ctiss/ISE-FS-200_ISE-SAR_Functional_Standard_V1.5_Issued_2009.pdf

National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing (October 2007),
http://www.ise.gov/docs/trsis/trsis_book.pdf

The Initial Privacy and Civil Liberties Analysis of the Information Sharing Environment - Suspicious Activity Reporting (ISE-SAR) Functional Standard and Evaluation Environment (September 2008),
http://www.ise.gov/docs/sar/ISE_SAR_Initial_Privacy_and_Civil_Liberties_Analysis.pdf

If you need assistance with this document, please contact the Clerk of the Court at (202) 544-2400. For more information, please visit the website at www.uscourts.gov.
If you have a question about this document, please contact the Clerk of the Court at (202) 544-2400. For more information, please visit the website at www.uscourts.gov.
This document is the property of the United States District Court for the District of Columbia. It is loaned to you for your use only and is not to be distributed outside your organization. If you have any questions, please contact the Clerk of the Court at (202) 544-2400. For more information, please visit the website at www.uscourts.gov.

Office of the Director of National Intelligence
Attention: Program Manager, Information Sharing Environment
Washington, DC 20511

(202) 331-2490

For more information, go to:

<http://www.ise.gov>

From: [German, Michael](#)
To: [REDACTED]
Cc: [REDACTED] [Jennifer Skinner](#); [REDACTED]
Subject: RE: Scheduling meeting with Kshemendra Paul for next week
Date: Monday, July 09, 2012 3:23:01 PM

Yes, it does. I look forward to talking with you.
Thanks,
Mike

From: [REDACTED] [mailto:[REDACTED]]
Sent: Monday, July 09, 2012 3:20 PM
To: German, Michael
Cc: [REDACTED]
Subject: RE: Scheduling meeting with Kshemendra Paul for next week

Does 2pm on Wed, July 18th work for you?

Thank you,
[REDACTED]

From: German, Michael [REDACTED]
Sent: Monday, July 09, 2012 3:09 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Scheduling meeting with Kshemendra Paul for next week

Hi [REDACTED]

I am available anytime on the 17, the afternoon of the 18th or anytime on the 20th. Let me know what works for you.

Best,
Mike

From: [REDACTED]
Sent: Monday, July 09, 2012 3:04 PM
To: German, Michael
Cc: [REDACTED]
Subject: Scheduling meeting with Kshemendra Paul for next week

Good afternoon, Mike,

I am following up on Kshemendra Paul's request for a meeting. Kshemendra is generally available next week with the exception of Thursday, July 19th. Please provide your availability for next week, July 16th-July 20th, for an in-person meeting at the PM-ISE office [REDACTED]
[REDACTED]

Thank you,

[REDACTED]

[REDACTED]

Privacy Coordinator

Office of the Program Manager, Information Sharing Environment (PM-ISE)

<http://www.ise.gov/>

[REDACTED]

[REDACTED]

From: Kshemendra N Paul

Sent: Friday, June 29, 2012 11:57 AM

To: [REDACTED]

Cc: [REDACTED]

Subject: Re: Meeting

Hello, Mike,

Yes, it was good to see you also.

Next week I am away. If you are available, perhaps sometime in the second half of the next week?

[REDACTED], can you please follow-up with a few times that work for me, you, and [REDACTED] to meet with Mike?

Mike, I am interested in listening to you, getting your take on challenges and opportunities around our efforts.

Warm Regards,

-Kshemendra

From: German, Michael [[mailto:\[REDACTED\]](mailto:[REDACTED])]

Sent: Friday, June 29, 2012 10:29 AM

To: Kshemendra N Paul

Subject: Meeting

Hi Kshemendra-

It was good seeing you again at CSIS this week. Thanks for your kind words, and I look forward to meeting with you again in the next few weeks to continue a dialogue. Let me know what works for you.

Best,

Mike

Michael German

Policy Counsel

American Civil Liberties Union

Washington Legislative Office

[REDACTED]

[REDACTED]

[REDACTED]

Subject: Kshemendra Paul and Mike German meeting
Location: [REDACTED]

Start: Wed 7/18/2012 2:00 PM
End: Wed 7/18/2012 3:00 PM

Recurrence: (none)

Meeting Status: Meeting organizer

Organizer: [REDACTED]

Required Attendees: Kshemendra N Paul; German, [REDACTED] Jennifer Skinner; [REDACTED]

From: Kshemendra N Paul
Sent: Friday, June 29, 2012 11:57 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: Re: Meeting

Hello, Mike,

Yes, it was good to see you also.

Next week I am away. If you are available, perhaps sometime in the second half of the next week?

[REDACTED] can you please follow-up with a few times that work for me, you, and [REDACTED] to meet with Mike?

Mike, I am interested in listening to you, getting your take on challenges and opportunities around our efforts.

Warm Regards,
-Kshemendra

From: German, Michael [mailto:[REDACTED]]
Sent: Friday, June 29, 2012 10:29 AM
To: Kshemendra N Paul
Subject: Meeting

Hi Kshemendra-
 It was good seeing you again at CSIS this week. Thanks for your kind words, and I look forward to meeting with you again in the next few weeks to continue a dialogue. Let me know what works for you.
 Best,
 Mike

Michael German
 Policy Counsel
 American Civil Liberties Union
 Washington Legislative Office

From: [Greg Nojeim](#)
To: [REDACTED]
Subject: Re: Availability to meet with the Program Manager for the Information Sharing Environment in October
Date: Monday, October 01, 2012 12:07:32 PM

confirmed.

On Oct 1, 2012, at 11:35 AM, [REDACTED] wrote:

Greg, Kshemendra is available at 3pm on Monday, Oct 22nd – please confirm if this time works for your schedule.

Thanks,
[REDACTED]

From: Greg Nojeim [mailto:[REDACTED]]
Sent: Monday, October 01, 2012 11:05 AM
To: [REDACTED]
Subject: Re: Availability to meet with the Program Manager for the Information Sharing Environment in October

10/22 works best, at any time except 12:00-2:00
10/23 am also works.
I leave for Seattle the next day.

-- Greg

On Oct 1, 2012, at 9:40 AM, [REDACTED] wrote:

Greg, unfortunately, I just learned that Kshemendra will be out of the office on travel between 10/15-10/18. Would the week of Oct 22nd-Oct 26th work for your schedule?

Thank you,
[REDACTED]

From: Greg Nojeim [mailto:[REDACTED]]
Sent: Friday, September 28, 2012 6:02 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: Re: Availability to meet with the Program Manager for the Information Sharing Environment in October

Great, [REDACTED] I'd like to get together with Mr. Paul. The following dates/times work for me:

10/15 and 10/16: 3:30-5:30
10/17: at any time whatsoever
10/18: at any time except for 12:30-2:30.

-- Greg

On Sep 28, 2012, at 11:24 AM, [REDACTED] >
[REDACTED] wrote:

Hi Greg, I am following up on our earlier request to schedule an informal, one-on-one meeting between yourself and Kshemendra Paul during the first two weeks of October.

Please let me know if you have any questions about this request.

Thank you,

[REDACTED]

[REDACTED]

Privacy Coordinator

Office of the Program Manager, Information Sharing Environment (PM-ISE)

www.ISE.gov

[REDACTED]

Email: [REDACTED]

[Blog](#) | [Twitter](#) | [Facebook](#) | [YouTube](#) | [LinkedIn](#)

[Get ISE Email Updates](#)

From: Greg Nojeim [[mailto:\[REDACTED\]](mailto:[REDACTED])]
Sent: Friday, July 20, 2012 6:01 PM
To: jskinner
Cc: [REDACTED]; [REDACTED]; Jim Dempsey
Subject: Re: Availability to meet with the Program Manager for the Information Sharing Environment

Ms. Skinner: I'm happy to get together with Mr. Paul and have pretty good availability the week of August 6 and the week after that. Greg
On Jul 20, 2012, at 5:34 PM, Jim Dempsey wrote:

Jennifer,

I would like to propose that my colleague, Greg Nojeim, meet with Mr Paul sometime in August, if that is possible.

live in San Francisco and work there most of the time. I am back to DC often, and I am coming back next week, but that trip will be very short.

Meanwhile, Mr. Nojeim is very busy while Congress is in session. He would be more likely to have time available in August - would any weeks be best then for

Mr. Paul?

I will certainly be back to DC in the Fall, and I would like to meet with Mr. Paul then.

Please convey my best regards to Mr. Paul.

Jim Dempsey
Vice President for Public Policy
Center for Democracy & Technology



Keeping the Internet Open, Innovative and Free

On Jul 20, 2012, at 3:56 PM, Jennifer Skinner wrote:

Mr. Dempsey,

I have been asked by the Program Manager for the Information Sharing Environment to contact you to see if you would be available to meet with him next week. Mr. Paul is engaging in a series of informal, one-on-one meetings with representatives of privacy and open government groups to share ISE successes. He is also seeking their feedback on ISE privacy, civil rights, and civil liberties protections and the implementation of protections by ISE mission partners.

If you are available to meet with Mr. Paul next week, would you please let us know what dates and times work for you? I look forward to hearing from you. Thank you.

Regards,

Jen

Jennifer Skinner, J.D.

Senior Research Associate
Institute for Intergovernmental Research



Gregory T. Nojeim
Senior Counsel and

Director, Project on Freedom, Security & Technology
Center for Democracy & Technology
1634 Eye St., NW Ste 1100
Washington, DC 20006



Follow our Security and surveillance work on Twitter at [@CenDemTech](#).

Gregory T. Nojeim
Senior Counsel and
Director, Project on Freedom, Security & Technology
Center for Democracy & Technology
1634 Eye St., NW Ste 1100
Washington, DC 20006



Follow our Security and surveillance work on Twitter at [@CenDemTech](#).

Gregory T. Nojeim
Senior Counsel and
Director, Project on Freedom, Security & Technology
Center for Democracy & Technology
1634 Eye St., NW Ste 1100

Washington, DC 20006

[REDACTED]
gnojeim@cdt.org

Follow our Security and surveillance work on Twitter at [@CenDemTech](https://twitter.com/CenDemTech).

Gregory T. Nojeim
Senior Counsel and
Director, Project on Freedom, Security & Technology
Center for Democracy & Technology
1634 Eye St., NW Ste 1100
Washington, DC 20006

[REDACTED]

Follow our Security and surveillance work on Twitter at [@CenDemTech](https://twitter.com/CenDemTech).



Subject: Meeting between Kshemendra Paul, PM-ISE, and Greg Nojeim of the Center for Democracy and Technology (CDT)

Location: PM-ISE Offices, [Redacted]

Start: Mon 10/22/2012 3:00 PM

End: Mon 10/22/2012 4:00 PM

Recurrence: (none)

Meeting Status: Meeting organizer

Organizer: [Redacted]

Required Attendees: Greg Nojeim; Kshemendra N Paul; [Redacted] Arecia A Grayton; [Redacted] 'Richard Ward'; 'Jennifer Skinner'; Michael J. Howell; [Redacted]

The Program Manager for the Information Sharing Environment, Kshemendra Paul, is engaging in a series of informal, one-on-one meetings to introduce himself to the privacy, civil rights, and civil liberties advocacy community and to expand his understanding of each organization's position on the work of the development and implementation of the Information Sharing Environment (ISE). For more information on the work of the ISE, please see our most recent ISE Annual Report to Congress, which is posted here:

[http://ise.gov/sites/default/files/ISE Annual Report to Congress 2012.pdf](http://ise.gov/sites/default/files/ISE%20Annual%20Report%20to%20Congress%202012.pdf)

Please contact [Redacted] if you have any questions regarding this meeting.

From: DNI-PM-ISE-EXECSEC
To: [REDACTED]
Cc: [REDACTED]
Subject: Invitation to Participate in ISE Privacy, Civil Rights, and Civil Liberties Roundtable - May 30, 2013, from 1-4 p.m. in downtown Washington, D.C.
Date: Wednesday, May 15, 2013 5:39:55 AM

THIS MESSAGE IS SENT ON BEHALF OF KSHEMENDRA PAUL, THE PROGRAM MANAGER FOR THE INFORMATION SHARING ENVIRONMENT (PM-ISE)

I am contacting you to formally invite you to attend an Information Sharing Environment (ISE) Privacy, Civil Rights, and Civil Liberties (P/CRCL) Roundtable on **Thursday, May 30, 2013, from 1:00 p.m. – 4:00 p.m., in room 430B of the Eisenhower Executive Office Building (EEOB)**. The EEOB is located at the intersection of 17th Street and State Place, N.W. in downtown Washington, D.C. (Note: the visitors entrance is located on State Place, NW, at the southern end of the building).

The purpose of this roundtable is to bring federal, state, and local ISE mission partners and members of the P/CRCL advocacy community together to discuss ISE issues. This forum will encourage open discussion to foster dialogue between and among roundtable participants about the way forward. Please note that a conference line is not available for those who are unable to attend the roundtable in person.

Please RSVP to the PM-ISE Executive Secretariat at DNI-PM-ISE-EXECSEC@dni.gov no later than the close of business of Wednesday, May 22nd. A Microsoft Outlook meeting invitation will also be sent from PM-ISE to assist you in managing this event on your calendars.

I also want to make you aware that in order to enter the EEOB building, PM-ISE must collect personally identifiable information (PII) from confirmed roundtable attendees. The required PII will include: full name, date of birth, social security number, and current city of residence. This information will be collected for the purpose of providing entry into the EEOB and will be deleted immediately after the roundtable event. PM-ISE will send an email to roundtable attendees who have RSVPed for this event approximately one week prior to the roundtable (on Thursday, May 23rd) with instructions on how to submit this requested information.

Attendees will have the option of submitting this requested PII to a PM-ISE staffer via phone. Additional information and read-ahead materials will be provided prior to the roundtable. If you have any questions about this roundtable event, please feel free to contact the PM-ISE Executive Secretariat at DNI-PM-ISE-EXECSEC@dni.gov or via phone at (202) 331-4060.

Thank you,
 PM-ISE Executive Secretariat
 202-331-4060
www.ise.gov

From: [DNI-PM-ISE-EXECSEC](#)

To: [Redacted]

Cc: [Redacted]

Subject: Read aheads for May 30th ISE Privacy, Civil Rights, and Civil Liberties Roundtable

Date: Friday, May 24, 2013 11:52:57 AM

Attachments: [ISE Privacy Roundtable Background and Resources.pdf](#)
[WAVE Request System Template for PCRCL Meeting.xlsx](#)
[Agenda ISE PCRCL Roundtable May 30 2013 final.pdf](#)

THIS MESSAGE IS SENT ON BEHALF OF **KSHEMENDRA PAUL**, THE **PROGRAM MANAGER** FOR THE **INFORMATION SHARING ENVIRONMENT (PM-ISE)**

We are looking forward to seeing you at the Information Sharing Environment (ISE) Privacy, Civil Rights, and Civil Liberties (P/CRCL) Roundtable on **Thursday, May 30, 2013, from 1:00 p.m. – 4:00 p.m., in room 430B of the Eisenhower Executive Office Building (EEOB)**. The EEOB is located at the intersection of 17th Street and State Place, N.W. in downtown Washington, D.C. (Note: the visitors entrance is located on State Place, NW, at the southern end of the building).

Attached for your information are the roundtable agenda and background information. The background material provides hyperlinks to the National Strategy for Information Sharing and Safeguarding and several other resources to assist you in preparing for the roundtable discussions. Thank you to everyone who has already RSVPed. For those who are still interested in attending this roundtable but who have not yet RSVPed, please submit the requested personal information for access into the EEOB to DNI-PM-ISE-EXECSEC@dni.gov today. Entry to the EEOB is tied to the individual's information, and invitees and/or substitute attendees will not be able to enter the EEOB if his or her personal information is not submitted and processed in advance.

If you have any questions about this roundtable event or need to submit your RSVP and WAVES form, please feel free to contact the PM-ISE Executive Secretariat at DNI-PM-ISE-EXECSEC@dni.gov or via phone at [Redacted].

Thank you,

PM-ISE Executive Secretariat

[Redacted]

www.ise.gov



ISE PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES ROUNDTABLE

EISENHOWER EXECUTIVE OFFICE BUILDING (EEOB), ROOM 430B,
WASHINGTON D.C.

THURSDAY, MAY 30, 2013 • 1:00 P.M. – 4:00 P.M.

1:00 p.m. – 1:15 p.m.	Introduction and Opening Remarks
1:15 p.m. – 1:45 p.m.	Update on the National Strategy for Information Sharing and Safeguarding (NSISS)
1:45 p.m. – 2:30 p.m.	Update on the Information Sharing Environment (ISE)
2:30 p.m. – 2:45 p.m.	Break
2:45 p.m. – 3:30 p.m.	Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) Functional Standard
3:30 p.m. – 4:00 p.m.	Roundtable and Wrap Up

UNCLASSIFIED



ISE PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES ROUNDTABLE

BACKGROUND ON THE INFORMATION SHARING ENVIRONMENT (ISE)

The Intelligence Reform and Terrorism Prevention Act of 2004 called for the creation of the Information Sharing Environment (ISE). In order to fix the information sharing gaps identified by the 9/11 Commission, we are working to build the ISE across federal, state, local, and tribal government, foreign partners, and the private sector.

The goal of the ISE is not to build a massive new information system, but to find common ground, align and build upon information sharing agreements, and promote a culture of information sharing—all while upholding the privacy, civil rights, and civil liberties (P/CR/CL) of Americans.

The Act also established the position of a Program Manager for the ISE (PM-ISE) to “plan for and oversee the implementation of, and manage the ISE,” and be “responsible for information sharing across the Federal Government.” In that capacity, the PM-ISE serves as:

- An “honest broker” and facilitator for improved private sector and federal, state, and local government terrorism-related information sharing; and
- The authority for issuing common ISE standards and related guidance for federal, state, and local government participants.

PURPOSE OF TODAY’S DISCUSSION

The PM-ISE has hosted several roundtable discussions in 2008, 2009, and 2010 with P/CR/CL advocacy groups and federal, state, and local government partners to promote transparency and receive feedback on key ISE initiatives, such as the National Network of Fusion Centers and the Nationwide Suspicious Activity Reporting Initiative. In addition, in 2012, the PM-ISE engaged in one-on-one sessions with P/CR/CL advocates to identify the topics of discussion for this meeting.

This roundtable builds upon these previous discussions with the same purpose of promoting transparency and feedback. It is intended as an open dialogue and consultation between P/CR/CL advocacy groups and government entities, with the intended outcome of: 1) informing participants about ISE initiatives and 2) soliciting feedback and inputs related to the protections and safeguards that are required and essential elements of the ISE.

1 BINGHAM MCCUTCHEN LLP
Jonathan Loeb (#162758) jonathan.loeb@bingham.com
2 Jeffrey Rosenfeld (#221625) jeffreyrosenfeld@bingham.com
Edward Andrews (#268479) edward.andrews@bingham.com
3 The Water Garden, Suite 2050 North
1601 Cloverfield Boulevard
4 Santa Monica, CA 90404-4082
Telephone: 310-907-1000
5 Facsimile: 310-907-2000

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

10 ASIAN AMERICANS ADVANCING
JUSTICE - ASIAN LAW CAUCUS
Nasrina Bargzie (#238917) nasrinab@advancingjustice-alc.org
11 Yaman Salahi (#288752) yamans@advancingjustice-alc.org
55 Columbus Avenue
12 San Francisco, CA 94111
Telephone: 415-848-7711
13 Facsimile: 415-896-1702

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

15 Additional counsel listed on signature page

16 UNITED STATES DISTRICT COURT
17 NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO-OAKLAND DIVISION

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

20 Plaintiffs,

21 v.

22 DEPARTMENT OF JUSTICE; ERIC H.
23 HOLDER, Jr., in his official capacity as the
Attorney General of the United States;
24 PROGRAM MANAGER - INFORMATION
SHARING ENVIRONMENT; KSHEMENDRA
25 PAUL, in his official capacity as the Program
Manager of the Information Sharing
Environment,

26 Defendants.
27
28

No. _____

**COMPLAINT FOR DECLARATORY
AND INJUNCTIVE RELIEF**

Administrative Procedure Act Case

INTRODUCTION

1
2 1. This complaint challenges a widespread domestic surveillance program that
3 targets constitutionally protected conduct and encourages racial and religious profiling.
4 Plaintiffs are five United States citizens – two photographers, one white man who is a devout
5 Muslim, and two men of Middle Eastern and South Asian descent. They engaged in innocuous,
6 lawful, and in some cases First Amendment protected activity. Two were photographing sites of
7 aesthetic interest, one was likely viewing a website about video games inside his home, one was
8 buying computers at Best Buy, and another was standing outside a restroom at a train station
9 while waiting for his mother. Due to the standards issued by Defendants that govern the
10 reporting of information about people supposedly involved in terrorism, Plaintiffs were reported
11 as having engaged in “suspicious activities,” reports about them were entered into
12 counterterrorism databases, and they were subjected to unwelcome and unwarranted law
13 enforcement scrutiny and interrogation. Defendants’ unlawful standards for maintaining a
14 federal law enforcement database regarding such supposedly “suspicious” activities have not
15 yielded any demonstrable benefit in the fight against terrorism, but they have swept up innocent
16 Americans in violation of federal law.

17 2. Through the National Suspicious Activity Reporting Initiative (“NSI”), the federal
18 government encourages state and local law enforcement agencies as well as private actors to
19 collect and report information that has a potential nexus to terrorism in the form of so-called
20 Suspicious Activity Reports (“SARs”). SARs are collected and maintained in various
21 counterterrorism databases and disseminated to law enforcement agencies across the country.
22 An individual who is reported in a SAR is flagged as a person with a potential nexus to terrorism
23 and automatically falls under law enforcement scrutiny, which may include intrusive questioning
24 by local or federal law enforcement agents. Even when the Federal Bureau of Investigation
25 concludes that the person did not have any nexus to terrorism, a SAR can haunt that individual
26 for decades, as SARs remain in federal databases for up to 30 years.

27 3. Defendants Department of Justice (“DOJ”) and Program Manager of the
28 Information Sharing Environment (“PM-ISE”) have issued standards governing the types of

1 information that should be reported in a SAR. Both standards authorize the collection,
2 maintenance, and dissemination of information, in the absence of any reasonable suspicion of
3 criminal activity. Defendants have also identified specific categories of behavior that they claim
4 satisfy each agency's standard and should be reported as suspicious. These behavioral categories
5 range from the constitutionally protected (photographing infrastructure) to the absurd ("acting
6 suspiciously").

7 4. Defendants' standards conflict with a duly promulgated regulation of Defendant
8 DOJ that prohibits the collection, maintenance, and dissemination of criminal intelligence
9 information, unless there is reasonable suspicion of criminal activity. *See* 28 C.F.R. § 23 (1993).
10 The regulation's reasonable suspicion requirement reflects the constitutional principle that law
11 enforcement should not take action against someone, unless there is good reason to believe
12 criminal activity is afoot. Neither of Defendants' standards for reporting suspicious activity was
13 promulgated in accordance with the notice and comment requirements of the Administrative
14 Procedure Act ("APA"), 5 U.S.C. § 551 *et seq.* (2012). As a result, Defendants' issuance and
15 implementation of standards for suspicious activity reporting violate federal statutory
16 requirements that agencies not act in an arbitrary and capricious manner and observe the
17 procedures required by law. Through this action for declaratory and injunctive relief, Plaintiffs
18 seek to set aside as unlawful Defendants' standards for suspicious activity reporting.

19 **PARTIES**

20 5. Plaintiff Wiley Gill is a United States citizen and a custodian at California State
21 University, Chico ("Chico State"). Mr. Gill converted to Islam while he was a student at Chico
22 State. He resides in Chico, California. He is the subject of a SAR, attached as Appendix A to
23 this Complaint. The SAR was uploaded to eGuardian, a law enforcement database maintained
24 by the FBI. The SAR identifies Mr. Gill as a "Suspicious Male Subject in Possession of Flight
25 Simulator Game." Mr. Gill was likely viewing a website about video games on his computer at
26 home, when two officers of the Chico Police Department entered and searched his home without
27 voluntary consent or a warrant based on probable cause.
28

1 6. Plaintiff James Prigoff is a United States citizen and an internationally renowned
2 photographer of public art. Mr. Prigoff resides in Sacramento, California. Private security
3 guards warned Mr. Prigoff not to photograph a piece of public art called the “Rainbow Swash” in
4 Boston, Massachusetts. As a result of that encounter, an agent of the Federal Bureau of
5 Investigation (“FBI”) went to Mr. Prigoff’s home in Sacramento several months later and
6 questioned at least one neighbor about him. Upon information and belief, Mr. Prigoff is the
7 subject of a SAR or SAR precursor report.

8 7. Plaintiff Khaled Ibrahim is a United States citizen of Egyptian descent who works
9 as an accountant for Nordix Computer Corporation, a computer network consulting and service
10 company. He formerly worked as a purchasing agent for Nordix. Mr. Ibrahim resides in San
11 Jose, California. Mr. Ibrahim is the subject of a SAR, attached as Appendix B to the Complaint.
12 The SAR describes a “[s]uspicious attempt to purchase large number of computers.” Mr.
13 Ibrahim attempted to make a bulk purchase of computers from a Best Buy retail store in Dublin,
14 California, in his capacity as a purchasing agent for Nordix. The SAR was uploaded to
15 eGuardian, a law enforcement database maintained by the FBI. Dublin is located in Alameda
16 County, California.

17 8. Plaintiff Tariq Razak is a United States citizen of Pakistani descent. A graduate
18 of the University of California at Irvine, he works in the bio-tech industry. Mr. Razak resides in
19 Placentia, California. Mr. Razak is the subject of a SAR, attached as Appendix C to this
20 Complaint. The SAR identifies Mr. Razak as a “Male of Middle Eastern decent [sic] observed
21 surveying entry/exit points” at the Santa Ana Train Depot and describes him as exiting the
22 facility with “a female wearing a white burka head dress.” Mr. Razak had never been to the
23 Depot before and was finding his way to the county employment resource center, which is
24 located inside the Depot and where he had an appointment. The woman accompanying him was
25 his mother.

26 9. Plaintiff Aaron Conklin is a graphic design student and amateur photographer.
27 He resides in Vallejo, California. Private security guards have twice prevented Mr. Conklin
28 from taking photographs of industrial architecture from public locations. One such incident

1 occurred outside the Shell refinery in Martinez, California, and resulted in Mr. Conklin being
2 detained and having his camera and car searched by Contra Costa County Sheriff’s Deputies,
3 who told Mr. Conklin that he would be placed on an “NSA watchlist.” Upon information and
4 belief, Mr. Conklin is the subject of a SAR. Martinez is located in Contra Costa County,
5 California.

6 10. Defendant DOJ is a federal agency within the meaning of the APA, 5 U.S.C. §
7 551(1). DOJ, through its components, has issued a standard governing SAR reporting, conducts
8 trainings on that standard, and plays a major role in implementing the NSI.

9 11. The FBI is a component of DOJ with both intelligence and law enforcement
10 responsibilities. The FBI has issued a standard governing the reporting of SARs, and trains law
11 enforcement and private sector personnel on its SAR reporting standard. The FBI oversees and
12 maintains the eGuardian system, which serves as a repository for SARs and allows thousands of
13 law enforcement personnel and analysts across the country to access SARs in the eGuardian
14 system. The FBI is one of the primary entities responsible for the NSI.

15 12. The Office of Justice Programs (“OJP”) was created pursuant to 42 U.S.C. § 3711
16 (2012) and is a component of Defendant DOJ. OJP administers grants to state and local law
17 enforcement entities. Upon information and belief, OJP funding supports, among other things,
18 entities that engage in the collection, maintenance, and dissemination of SARs, and systems that
19 collect, maintain, and disseminate SARs.

20 13. The Bureau of Justice Assistance (“BJA”), within OJP, provides assistance to
21 local criminal justice programs through policy, programming, and planning. BJA served as the
22 executive agent of the NSI until October 2013. BJA has issued a standard governing the
23 reporting of SARs, and conducts trainings on its SAR reporting standard.

24 14. The Program Management Office (“PMO”), also a component of DOJ, has played
25 a key role in implementing the NSI. On December 17, 2009, DOJ was named the executive
26 agent to establish and operate the PMO for the NSI. In March 2010, DOJ established the NSI
27 PMO within BJA to support nationwide implementation of the SAR process.
28

INTRADISTRICT ASSIGNMENT

21. Pursuant to Local Rule 3-2(c) and (d), assignment to the San Francisco-Oakland Division is proper because a substantial part of the events giving rise to this action occurred in Alameda and Contra Costa Counties.

FACTUAL ALLEGATIONS

A. The Nationwide Suspicious Activity Reporting Initiative

22. The federal government created the NSI to facilitate the sharing of information potentially related to terrorism across federal, state, local, and tribal law enforcement agencies. In particular, the NSI creates the capability to share reports of information with a potential nexus to terrorism, which have been dubbed Suspicious Activity Reports.

23. Fusion centers are focal points of the system for sharing SARs. There are currently 78 fusion centers nationwide. They are generally, though not always, owned and operated by state or local government entities. Fusion centers receive federal financial support, including from OJP.

24. Defendants PM-ISE and DOJ train state, local, and tribal law enforcement agencies as well as private entities to collect information about activities with a potential nexus to terrorism based on the standard each agency has adopted, and to submit the information in the form of a SAR, either to a fusion center or the FBI.

25. Fusion centers gather, receive, store, analyze, and share terrorism and other threat-related information, including SARs. On information and belief, fusion centers collect, maintain, and disseminate SARs through databases that receive financial support from OJP.

26. Defendants train fusion center analysts in their respective standards for SAR reporting. Fusion center analysts review submitted SARs. If a SAR meets Defendants' standards, it is uploaded to one or more national databases, such as the FBI's eGuardian system, where it can be accessed by the FBI and law enforcement agencies across the country. The federal government maintains SARs sent to the FBI's eGuardian system for 30 years. This is done even when the FBI determines that the SAR has no nexus to terrorism. *See* Functional Standard 1.5 at 34, 53; United States Government Accountability Office, "Information Sharing:

1 Additional Actions Could Help Ensure That Efforts to Share Terrorism-Related Suspicious
2 Activity Reports Are Effective” at 7 (March 2013) (“GAO SAR Report”).

3 27. Pursuant to the process created by Defendants PM-ISE and DOJ for suspicious
4 activity reporting, individuals who are the subject of a SAR are automatically subjected to law
5 enforcement scrutiny at multiple levels of government. That scrutiny may include, but is not
6 limited to, follow-up interviews and other forms of investigation by law enforcement. For
7 example:

8 (a) At the initial response and investigation stage, and even before a SAR is
9 submitted to a fusion center or the FBI, Defendant PM-ISE instructs the federal,
10 state, local, or tribal law enforcement agency with jurisdiction to respond to the
11 reported observation by “gather[ing] additional facts through personal
12 observations, interviews, and other investigative activities. This may, at the
13 discretion of the [responding] official, require further observation or engaging the
14 suspect in conversation.” Functional Standard 1.5 at 32.

15 (b) Fusion center personnel “tak[e] steps to investigate SARs – such as
16 interviewing the individual engaged in suspicious activity or who witnessed
17 suspicious activity – before providing the SARs to the FBI.” GAO SAR Report at
18 16. Officials from fusion centers do investigative work as part of their vetting
19 process. *Id.* at 17.

20 (c) The FBI reviews all SARs that it receives from fusion centers for follow-up.
21 That follow-up can take the form of an interview with the subject of the SAR, and
22 includes, but is not limited to, engaging in a threat assessment of or opening an
23 investigation into the subject.

24 (d) FBI agents have admitted that they are required to follow-up on SARs, even
25 when they know the individual does not pose a threat. For example, a
26 professional freelance photographer in Los Angeles, California who specializes in
27 industrial photography, has twice been interviewed by the FBI after
28 photographing industrial sites. After security guards instructed him not to

1 photograph certain industrial sites in the area of the Port of Long Beach in April
2 2008, FBI agents visited him at his home to question him about the incident. The
3 FBI contacted him again, after Los Angeles Sheriff's Department personnel
4 interfered with his efforts to photograph another industrial site in approximately
5 December 2009. The FBI agent told the photographer that he knew the
6 photographer did not pose a threat but that because a report had been opened, he
7 was required to follow-up on it.

8 (e) As explained above, SARs that have been uploaded to a national database can
9 be accessed by law enforcement agencies nationwide. Once uploaded to a
10 national database, the subject of a SAR faces scrutiny and potential investigation
11 by one or more of the law enforcement agencies across the country that has access
12 to the database. That scrutiny is only increasing, as queries of national SAR
13 databases have dramatically jumped in recent years. The number of queries of
14 national SAR databases such as eGuardian has risen from about 2,800 queries as
15 of July 2010 to more than 71,000 queries as of February 2013. *See* GAO SAR
16 Report at 36.

17 28. This surveillance program has not proven effective in the fight against terrorism.
18 The United States Government Accountability Office ("GAO") has faulted the program for
19 failing to demonstrate *any* results-oriented outcomes, such as arrests, convictions, or thwarted
20 threats, even though tens of thousands of SARs had been deemed sufficiently significant to be
21 uploaded to national SAR databases as of October 2012. *See* GAO SAR Report at 33, 36-38. In
22 2012, a Senate Subcommittee reviewed a year of similar intelligence reporting from state and
23 local authorities, and identified "dozens of problematic or useless" reports "potentially violating
24 civil liberties protections." United States Senate, Permanent Subcommittee on Investigations,
25 Committee on Homeland Security and Governmental Affairs, "Federal Support for and
26 Involvement in State and Local Fusion Centers," October 3, 2012 at 27. Another report, co-
27 authored by Los Angeles Police Department Deputy Chief Michael Downing, found that SARs
28 have "flooded fusion centers, law enforcement, and other security entities with white noise."

1 The George Washington University Homeland Security Policy Institute, “Counterterrorism
2 Intelligence: Fusion Center Perspectives,” June 26, 2012 at 31.

3 29. While the SARs process has not proven effective in combating terrorism, it has
4 been extremely effective in sweeping up innocent Americans and recording their lawful activity
5 in federal counterterrorism databases. Over 1,800 SARs from fusion centers in California show
6 that the program targets First Amendment protected activity such as photography and encourages
7 racial and religious profiling. Examples of SARs that met Defendants’ standards for SAR
8 reporting and have been uploaded to the FBI’s eGuardian database include:

- 9 • “Suspicious ME [Middle Eastern] Males Buy Several Large Pallets of Water”
- 10 • A sergeant from the Elk Grove Police Department reported “on a suspicious
11 individual in his neighborhood”; the sergeant had “long been concerned about a
12 residence in his neighborhood occupied by a Middle Eastern male adult physician
13 who is very unfriendly”
- 14 • “Female Subject taking photos of Folsom Post Office”
- 15 • “an identified subject was reported to be taking photographs of a bridge crossing
16 the American River Bike trail”
- 17 • “I was called out to the above address regarding a male who was taking
18 photographs of the [name of facility blacked out] [in Commerce, California]. The
19 male stated, he is an artist and enjoys photographing building[s] in industrial
20 areas ... [and] stated he is a professor at San Diego State private college, and
21 takes the photos for his art class.”
- 22 • “I observed a male nonchalantly taking numerous pictures inside a purple line
23 train [in Los Angeles County] ... The male said he was taking pictures because
24 they were going to film the television show ‘24’ on the train next week.”
- 25 • “two middle eastern looking males taking photographs of Folsom Dam. One of
26 the ME males appeared to be in his 50’s”
- 27 • “Suspicious photography of the Federal Courthouse in Sacramento”: an “AUSA
28 [Assistant United States Attorney] reported to the Court Security Officer (CSO) a

1 suspicious vehicle occupied by what [name blacked out] described as two Middle
2 Eastern males, the passenger being between 40-50 years of age.”

- 3 • “Suspicious photography of Folsom Dam by Chinese Nationals”: “a Sac County
4 Sheriff’s Deputy contacted 3 adult Asian males who were taking photos of
5 Folsom Dam. They were evasive when the deputy asked them for identification
6 and said their passports were in their vehicle.”

7 **B. Conflicting Federal Rules for Collection of Intelligence Information**

8 30. Defendants have issued three separate rules governing the collection of
9 intelligence information, in particular, suspicious activity reports. Only one of these rules,
10 however, requires reasonable suspicion of criminal activity for the information to be collected,
11 maintained, and disseminated, and only that rule was duly promulgated under the APA.

12 **1. 28 C.F.R. Part 23**

13 31. On June 19, 1968, President Lyndon B. Johnson signed into law the Omnibus
14 Crime Control and Safe Streets Act of 1968 (“Omnibus Act”). The Act created the Law
15 Enforcement Administration Agency (“LEAA”), a forerunner to OJP and a component of DOJ,
16 and authorized it to oversee the distribution of federal grants to state and local law enforcement
17 programs.

18 32. In 1978, after observing the notice and comment process set forth in the APA,
19 Defendant DOJ, through its component the LEAA, published a final rule establishing operating
20 principles for “Criminal Intelligence Systems.” *See* 28 C.F.R. § 23 (1993). The regulation was
21 promulgated pursuant to the LEAA’s statutory mandate to ensure that criminal intelligence is not
22 collected, maintained, or disseminated “in violation of the privacy and constitutional rights of
23 individuals.” 42 U.S.C. § 3789g(c) (2012).

24 33. Several commenters on the then-proposed regulation “were concerned that the
25 collection and maintenance of intelligence information should only be triggered by a reasonable
26 suspicion that an individual is involved in criminal activity.” *See* 43 Fed. Reg. 28,572 (June 30,
27 1978). The agency concurred, and the proposed operating principles were “revised to require
28 this criteria as a basis for collection and maintenance of intelligence information.” *Id.*

1 34. Among other requirements, the final rule provides that a “project shall collect and
2 maintain criminal intelligence information concerning an individual only if there is reasonable
3 suspicion that the individual is involved in criminal conduct or activity and the information is
4 relevant to that criminal conduct or activity.” 28 CFR § 23.20(a).

5 35. In addition, the regulation states that while “pooling of information about” various
6 kinds of criminal activities such as drug trafficking, smuggling, and public corruption can be
7 helpful in “expos[ing] ... ongoing networks of criminal activity,” “the collection and exchange
8 of intelligence data necessary to support control of serious criminal activity may represent
9 potential threats to the privacy of individuals to whom such data relates,” and the privacy
10 guidelines set forth in 28 CFR Part 23 are therefore necessary. 28 CFR § 23.2.

11 36. In 1980, DOJ amended the rule, following the public notice and comment process
12 set forth in the APA, to extend the reach of 28 C.F.R. Part 23 to criminal intelligence systems
13 funded by both discretionary and formula grants. 45 Fed. Reg. 61,612 (Sep. 17, 1980).

14 37. DOJ amended the rule again in 1993 to include a definition of “reasonable
15 suspicion”:

16 Reasonable Suspicion . . . is established when information exists which establishes
17 sufficient facts to give a trained law enforcement or criminal investigative agency officer,
18 investigator, or employee a basis to believe that there is a reasonable possibility that an
individual or organization is involved in a definable criminal activity or enterprise.

19 See 28 C.F.R. § 23.20.

20 38. “Reasonable suspicion” is the time-tested, constitutional standard that limits law
21 enforcement from taking action against someone, unless there is good reason to believe criminal
22 activity is afoot.

23 39. One commenter argued that “reasonable suspicion . . . is not necessary to the
24 protection of individual privacy and Constitutional rights, [and suggested] instead that
25 information in a funded intelligence system need only be ‘necessary and relevant to an agency’s
26 lawful purposes.’” 58 Fed. Reg. 178, 48451 (Sept. 16, 1993). The agency disagreed, replying:

27 the potential for national dissemination of information in intelligence information
28 systems, coupled with the lack of access by subjects to challenge the information,
justifies the reasonable suspicion standard as well as other operating principle restrictions
set forth in this regulation. Also, the quality and utility of ‘hits’ in an information system

1 is enhanced by the reasonable suspicion requirement. Scarce resources are not wasted by
 2 agencies in coordinating information on subjects for whom information is vague,
 incomplete and conjectural.

3 *Id.*

4 40. DOJ made an attempt in 2008 to amend the regulation to weaken its privacy
 5 protections. In particular, the proposed rule would have (1) permitted information to be stored
 6 regarding organizations as well as individuals; (2) allowed information to be stored based on
 7 reasonable suspicion related to “domestic and international terrorism, including material support
 8 thereof,” and (3) eliminated the requirement that law enforcement agencies receiving information
 9 from a Criminal Intelligence System agree to comply with 28 C.F.R. Part 23, so that recipients
 10 would merely need to have procedures “consistent with” Section 23. *See* 73 Fed. Reg. 44,674
 11 (July 31, 2008). This attempted rulemaking, however, met with criticism and DOJ withdrew its
 12 proposed rule. The regulation has remained unchanged since its last amendment in 1993.

13 41. In short, in initially adopting the regulation, DOJ emphasized the importance of
 14 the reasonable suspicion requirement and since then has expanded the scope of the regulation,
 15 reiterated the importance of the reasonable suspicion requirement, and withdrawn efforts to
 16 weaken the regulation’s privacy protections.

17 **2. PM-ISE Standard for Suspicious Activity Reporting**

18 42. Defendant PM-ISE subsequently issued a standard for SAR reporting that –
 19 unlike 28 CFR Part 23 – does not require reasonable suspicion of criminal activity before a
 20 suspicious activity report is collected, maintained, or disseminated and was not issued through
 21 the notice and comment procedure required by the APA, thus dodging public review.

22 43. Pursuant to the exercise of its statutory authority to “exercise governmentwide
 23 authority over the sharing of [terrorism and homeland security] information,” 6 U.S.C. §
 24 485(f)(1) (2012), PM-ISE has issued “Functional Standards” governing suspicious activity
 25 reporting.

26 44. In or about May 2009, PM-ISE released Information Sharing Environment (ISE) -
 27 Functional Standard (FS) - Suspicious Activity Reporting (SAR) Version 1.5 (“Functional
 28 Standard 1.5”), which remains currently in effect. It sets forth the following standard for

1 suspicious activity reporting: “[o]bserved behavior *reasonably indicative* of pre-operational
2 planning related to terrorism or other criminal activity.” Functional Standard 1.5 at 2 (emphasis
3 added).

4 45. The agency has expressly acknowledged that Functional Standard 1.5 requires
5 “less than the ‘reasonable suspicion’ standard.” PM-ISE, Privacy, Civil Rights, and Civil
6 Liberties Analysis and Recommendations–Nationwide Suspicious Activity Reporting Initiative
7 at 12 (draft May 2010).

8 46. The document also identifies sixteen categories of activity that fall under the
9 standard and provide a guide to law enforcement in determining what amounts to a suspicious
10 activity. These categories include photography, observation/surveillance, and acquisition of
11 materials or expertise. Functional Standard 1.5 at 29-30.

12 47. Functional Standard 1.5 applies to, *inter alia*, “all departments or agencies that
13 possess or use terrorism or homeland security information.” Functional Standard 1.5 at 1.
14 Functional Standard 1.5 applies to state, local, and tribal law enforcement agencies and fusion
15 centers that participate in the NSI. Agencies participating in the NSI follow Functional Standard
16 1.5 in reporting suspicious activity.

17 48. Functional Standard 1.5 purports to define the scope of suspicious activity that
18 should be reported for agencies participating in the NSI. The purpose of Functional Standard 1.5
19 is to standardize SAR reporting at the federal, state, and local levels.

20 49. PM-ISE trains participants in the NSI about, among other things, how to follow
21 Functional Standard 1.5.

22 50. In promulgating Functional Standard 1.5, PM-ISE expressly cited its legislative
23 authority under, *inter alia*, the IRTPA over governmentwide standards for information sharing.
24 Functional Standard 1.5 at 1.

25 51. Functional Standard 1.5 constitutes final agency action and a legislative rule
26 within the meaning of the APA.
27
28

1 52. PM-ISE issued Functional Standard 1.5 without observing the process set forth in
2 the APA for public notice and comment. Functional Standard 1.5 went into immediate effect
3 upon its publication on May 1, 2009 and remains currently in effect.

4 **3. DOJ Standard for Suspicious Activity Reporting**

5 53. Defendant DOJ, through its components, has issued a standard for SAR reporting
6 (“DOJ’s SAR Standard”) that – unlike 28 CFR § 23 – does not require reasonable suspicion of
7 criminal activity before a suspicious activity report is collected, maintained, or disseminated and
8 was not issued through the notice and comment procedure required by the APA, thus dodging
9 public review.

10 54. DOJ, through its component the FBI, has set forth the following standard for
11 suspicious activity reporting: “observed behavior that *may be indicative* of intelligence gathering
12 or pre-operational planning related to terrorism, criminal or other illicit intention.” FBI, Privacy
13 Impact Assessment for the eGuardian Threat Tracking System at § 1.1 (emphasis added). This
14 standard is set forth in the FBI’s 2008 eGuardian Privacy Impact Assessment (“2008 eGuardian
15 PIA”), which is attached as Appendix E to this Complaint. “[T]he FBI uses the criteria in the
16 eGuardian Privacy Impact Assessment (dated November 25, 2008) ... to determine if SARs have
17 a potential nexus to terrorism.” GAO SAR Report at 6 n.10.

18 55. DOJ’s “may be indicative” SAR Standard is even broader than PM-ISE’s
19 “reasonably indicative” Functional Standard 1.5. *See* GAO SAR Report at 15-16. But like
20 Functional Standard 1.5, DOJ’s SAR Standard encourages reporting even in the absence of
21 reasonable suspicion of criminal activity.

22 56. Just as Defendant PM-ISE has enumerated categories of behavior that fall under
23 its “reasonably indicative” reporting standard, DOJ through its components has also enumerated
24 categories of behavior that fall under its “may be indicative” reporting standard. These
25 categories of behavior are broader than the categories set forth in Functional Standard 1.5 and
26 include but are not limited to:

1 (a) “Possible indicators of terrorist behaviors at hotels:...” FBI and United States
2 Department of Homeland Security, “Roll Call Release,” July 26, 2010, attached as
3 Appendix F to this Complaint.

4 (1) “Using payphones for outgoing calls or making front desk requests in
5 person to avoid using the room telephone.” *Id.*

6 (2) “Interest in using Internet cafes, despite hotel Internet availability....”
7 *Id.*

8 (3) “Requests for specific rooms, floors, or other locations in the
9 hotel....” *Id.*

10 (4) “Multiple visitors or deliveries to one individual or room.” *Id.*

11 (b) “No obvious signs of employment.” FBI, “Quick Reference Terrorism Card,”
12 attached as Appendix G to this Complaint.

13 (c) “Possess student visa but not English Proficient.” *Id.*

14 (d) “Persons not fitting into the surrounding environment, such as wearing
15 improper attire for the location.” *Id.*

16 (e) “Persons exhibiting unusual behavior such as staring or quickly looking away
17 from individuals or vehicles as they enter or leave designated facilities or
18 parking areas.” *Id.*

19 (f) “A blank facial expression in an individual may be indicative of someone
20 concentrating on something not related to what they appear to be doing.” *Id.*

21 (g) “[P]eople in places where they do not belong.” Bureau of Justice Assistance,
22 “Communities Against Terrorism: Potential Indicators of Terrorist Activities
23 Related to the General Public,” attached as Appendix H to this Complaint.

24 57. One category of behavior identified by DOJ as “suspicious” activity that should
25 be reported is a “catch-all”:

26 (a) “[P]eople acting suspiciously.” *Id.*

27 58. DOJ through its components has also issued “Potential Indicators of Terrorist
28 Activities Related to Electronic Stores” (attached as Appendix I to this Complaint) and

1 “Potential Indicators of Terrorist Activities Related to Mass Transportation” (attached as
2 Appendix J to this Complaint). Activities identified as suspicious in connection with mass
3 transportation include “[a]cting nervous or suspicious,” and “[u]nusual or prolonged interest in
4 ... entry points and access controls.”

5 59. DOJ through its components trains participants in the NSI about DOJ’s SAR
6 Standard. For example, as of 2013, the PMO had provided training for 290,000 line officers (law
7 enforcement officers whose routine duties put them in a position to observe “suspicious”
8 activity), 2,000 analytical personnel, and executives from 77 fusion centers. *See* GAO SAR
9 Report at 29. DOJ components teach participants in the NSI, including frontline officers and
10 fusion center analysts to submit to the FBI “all potentially terrorism-related information and not
11 just ISE-SARs that met the [PM-ISE’s] Functional Standard [1.5].” GAO SAR Report at 16.

12 60. DOJ’s SAR Standard applies to state, local, and tribal law enforcement agencies
13 and fusion centers that participate in the NSI. Agencies participating in the NSI follow DOJ’s
14 SAR Standard in reporting suspicious activity.

15 61. DOJ’s SAR Standard purports to define the scope of suspicious activity that
16 should be reported for agencies participating in the NSI. The purpose of DOJ’s SAR Standard is
17 to standardize SAR reporting at the federal, state, and local levels.

18 62. Because DOJ’s SAR Standard is broader than PM-ISE’s Functional Standard 1.5
19 and DOJ’s behavioral categories include the catch-all “people acting suspiciously,” any activity
20 that falls under PM-ISE’s Functional Standard also falls under DOJ’s SAR Standard.

21 63. Fusion centers that follow DOJ’s SAR Standard instead of PM-ISE’s Functional
22 Standard 1.5 send many SARs to the FBI for review. For example, of the SARs uploaded by one
23 state’s fusion center to a national SAR database from June 2011 to October 2012, only 10% met
24 PM-ISE’s Functional Standard 1.5. *See* GAO SAR Report at 16.

25 64. DOJ establishes an even broader standard than the already overbroad Functional
26 Standard 1.5, and the DOJ reinforces its broader standard through the trainings it provides to NSI
27 participants and through other mechanisms. For example, when fusion center personnel are
28 uncertain whether to share a SAR, DOJ encourages them to err on the side of overreporting. *See*

1 GAO SAR Report at 16. In addition, the only feedback mechanism participants in the NSI
2 currently receive on whether they are reporting SARs appropriately is provided by the FBI
3 through its eGuardian system. *See* GAO SAR Report at 13-14. The feedback the FBI provides
4 reinforces the DOJ SAR Standard to NSI participants.

5 65. DOJ's 2008 eGuardian PIA, which sets forth the agency's standard for reporting
6 suspicious activity, was signed by four "Responsible Officials," two "Reviewing Officials," and
7 one "Approving Official." It reflects the consummation of the agency's decision making
8 process.

9 66. DOJ's 2008 eGuardian PIA contains a set of mandatory, non-discretionary rules
10 and obligations. It lays out clear instructions for the use of the eGuardian system to collect and
11 share SARs and the standard for defining "suspicious activity." For example, the 2008
12 eGuardian PIA states that the eGuardian system will "ensure consistency of process and of
13 handling protocols" and mandates that all users "will be required to complete robust system
14 training that will incorporate eGuardian policies and procedures." 2008 eGuardian PIA at 4. In
15 addition, the eGuardian User Agreement, attached to the 2008 eGuardian PIA, states that
16 "[i]ncidents not meeting the criteria of suspicious activity or with a potential nexus to terrorism
17 and that, further, do not comply with the above-stated rules, will be immediately deleted from
18 eGuardian." 2008 eGuardian PIA at 25.

19 67. DOJ has consistently reinforced its standard for SAR reporting, set forth in the
20 2008 eGuardian PIA, through training materials and other publications that identify categories of
21 behavior that the agency contends are suspicious and should be reported.

22 68. In promulgating DOJ's SAR Standard, DOJ expressly invoked its statutory
23 "mandate" under IRTPA and "other statutes ... to share terrorism information with other federal,
24 and state, local and tribal (SLT) law enforcement partners." 2008 eGuardian PIA at 2.

25 69. DOJ's SAR Standard constitutes final agency action and a legislative rule within
26 the meaning of the APA.
27
28

1 70. Defendant DOJ issued the DOJ SAR Standard without observing the process set
2 forth in the APA for public notice and comment. It is the DOJ Standard for SAR reporting
3 currently in effect.

4 **4. PM-ISE’s Functional Standard 1.5 and DOJ’s SAR Standard Conflict with**
5 **28 CFR Part 23**

6 71. As a report of “[o]bserved behavior reasonably indicative of pre-operational
7 planning related to terrorism or other criminal activity” (Functional Standard 1.5) or a report of
8 “observed behavior that may be indicative of intelligence gathering or pre-operational planning
9 related to terrorism, criminal or other illicit intention” (DOJ’s SAR Standard), a SAR contains
10 data relevant to the identification of an individual who is suspected in some fashion of being
11 involved in criminal, in particular, terrorist activity.

12 72. A SAR constitutes “criminal intelligence” within the meaning of 28 CFR Part 23.

13 73. State, local, and tribal law enforcement agencies and fusion centers that
14 participate in the NSI and observe PM-ISE’s Functional Standard 1.5 and/or DOJ’s SAR
15 Standard collect, review, analyze, and disseminate SARs. These entities operate arrangements,
16 equipment, facilities, and procedures, used for the receipt, storage, interagency exchange or
17 dissemination, and analysis of SARs. Upon information and belief, these entities and the
18 systems they operate for receiving, storing, exchanging, disseminating, and analyzing SARs
19 operate through support from Defendant DOJ’s component OJP.

20 74. State, local, and tribal law enforcement agencies and fusion centers that
21 participate in the NSI and observe PM-ISE’s Functional Standard 1.5 and/or DOJ’s SAR
22 Standard are “projects” within the meaning of 28 CFR Part 23. The systems or databases on
23 which SARs are maintained and through which they are collected and disseminated are “criminal
24 intelligence systems” within the meaning of 28 CFR Part 23.

25 75. PM-ISE’s Functional Standard 1.5 and DOJ’s SAR Standard set forth operating
26 principles for the collection, maintenance, and dissemination of data relevant to the identification
27 of an individual who is suspected in some fashion of being involved in criminal, in particular,
28 terrorist activity. Both standards, however, encourage or purport to authorize collection,

1 maintenance, and dissemination of such data even in the absence of reasonable suspicion of
2 criminal activity. Both standards encourage or purport to authorize collection, maintenance, and
3 dissemination of much more data than that permitted under 28 CFR Part 23. Both standards
4 therefore conflict with 28 CFR Part 23.

5 76. Through PM-ISE's promulgation of Functional Standard 1.5 and DOJ's
6 promulgation of its SAR Standard, and through each agency's training of entities participating in
7 the NSI in their respective standards for reporting suspicious activity, Defendants PM-ISE, Paul,
8 DOJ, and Holder have undermined and thereby violated 28 CFR Part 23.

9 77. Neither DOJ nor PM-ISE has offered any reasoned basis for departing from the
10 reasonable suspicion standard set forth in 28 CFR Part 23 for the collection, maintenance, and
11 dissemination of SARs.

12 78. DOJ could rescind its SAR reporting standard. If DOJ rescinded its SAR
13 reporting standard, participants in the NSI would cease collecting, maintaining, reviewing,
14 analyzing and disseminating SARs based on DOJ's SAR Standard, and it would be clear that the
15 governing standard for suspicious activity reporting is 28 CFR Part 23. As a result, individuals
16 who are currently the subject of SARs but whose conduct did not give rise to a reasonable
17 suspicion of criminal activity would no longer have their information collected, maintained, and
18 disseminated in SAR databases. DOJ could cease collecting, maintaining, reviewing, analyzing,
19 and disseminating SARs about individuals whose conduct did not give rise to a reasonable
20 suspicion of criminal activity.

21 79. PM-ISE could rescind Functional Standard 1.5. If PM-ISE rescinded Functional
22 Standard 1.5, participants in the NSI would cease collecting, maintaining, reviewing, analyzing
23 and disseminating SARs based on Functional Standard 1.5, and it would be clear that the
24 governing standard for suspicious activity reporting is 28 CFR Part 23. As a result, individuals
25 who are currently the subject of SARs but whose conduct did not give rise to a reasonable
26 suspicion of criminal activity would no longer have their information collected, maintained, and
27 disseminated in SAR databases.
28

1 **C. Plaintiff's Allegations**

2 **1. Wiley Gill**

3 80. Wiley Gill is a United States citizen living in Chico, California. He works as a
4 custodian at Chico State, which he attended as an undergraduate. Mr. Gill converted to Islam in
5 2009, after learning about the religion in a course he took while a student at Chico State.

6 81. Mr. Gill is the subject of a SAR that identifies him as a "Suspicious Male Subject
7 in Possession of Flight Simulator Game." This SAR falls into one or more of the behavioral
8 categories identified in Functional Standard 1.5, in particular, "[a]cquisition of [e]xpertise" and
9 potentially "[a]viation [a]ctivity." Functional Standard 1.5 at 29-30. It also falls under one or
10 more behavioral categories identified by Defendant DOJ, such as the catch-all behavioral
11 category of "acting suspiciously."

12 82. Mr. Gill's SAR was collected, maintained, and disseminated through a fusion
13 center SAR database, and uploaded to eGuardian and/or another national SAR database. As a
14 result, the FBI has scrutinized Mr. Gill, conducted extensive background checks on him, and
15 created a file about him.

16 83. The SAR was created on or about May 23, 2012, and purports to document an
17 encounter between Mr. Gill and the Chico Police Department ("CPD") on or about May 20,
18 2012. The SAR states that a CPD officer was investigating a domestic violence incident and
19 believed the suspect may have fled into Mr. Gill's residence. The SAR states that this was later
20 discovered to be unfounded. It acknowledges that the CPD officer searched Mr. Gill's home.
21 The SAR asserts that Mr. Gill's computer displayed a screen titled something to the effect of
22 "Games that fly under the radar," which appeared to be a "flight simulator type of game." The
23 SAR concludes by describing Mr. Gill's "full conversion to Islam as a young WMA [white, male
24 adult]," "pious demeanor," and "potential access to flight simulators via the internet" as "worthy
25 of note."

26 84. CPD's search of Mr. Gill's residence on or about May 20, 2012 did in fact occur.
27 But the SAR contains numerous misstatements and omits several crucial facts, including that two
28 CPD officers banged on Mr. Gill's door and after when he went to open it, they came around the

1 corner of the house with their guns drawn and pointed at Mr. Gill. Mr. Gill was thrown off
2 guard. The officers eventually lowered their guns, and then asked to search Mr. Gill's home,
3 based on the alleged domestic violence incident involving two individuals that they claimed to
4 have received. Mr. Gill informed the officers that he was home alone. Despite that, the officers
5 continued to ask to search his home. Mr. Gill was reluctant to grant permission, but felt that he
6 had no choice under the circumstances. One officer remained with Mr. Gill outside, while the
7 other searched his home. Mr. Gill did not feel free to leave. Mr. Gill cooperated with the
8 officers' request for identification. Mr. Gill believes that he was likely viewing a website about
9 video games at the time of the May 20, 2012, incident.

10 85. On information and belief, the officers' contention that they were investigating a
11 domestic violence call was a pretext for searching Mr. Gill's home because CPD had already
12 decided to investigate Mr. Gill because of his religion.

13 86. The SAR also describes two earlier encounters between CPD and Mr. Gill, one at
14 the Mosque that Mr. Gill attends and another while Mr. Gill was walking through downtown
15 Chico "with elders." The SAR describes Mr. Gill in these instances as "avoid[ing] eye contact"
16 and "hesitant to answer questions."

17 87. Mr. Gill recalls CPD officers visiting the Mosque he attends, paying what they
18 described as a courtesy visit in an attempt to build good relations with the Muslim community.
19 Mr. Gill listened to the presentation. When it was over, CPD officers asked Mr. Gill his name,
20 whether he went to school, and if he was employed. Mr. Gill answered all of their questions.
21 His understanding is that the officers did not question anyone else in this manner.

22 88. Mr. Gill also recalls encountering CPD officers while he was walking through
23 downtown Chico with two older Muslim men who are friends from the Mosque. A CPD officer
24 called out Mr. Gill's name and asked Mr. Gill if he had found a job yet. Mr. Gill answered the
25 question, but was caught off guard by the encounter because he did not recognize the officer and
26 was surprised that the officer knew his name and employment status.

27 89. At no point during any of the encounters with CPD recounted in the SAR did Mr.
28 Gill engage in conduct that gave rise to a reasonable suspicion of criminal activity.

1 90. The CPD also targeted Mr. Gill in two other encounters that are not described in
2 the SAR, and that do not involve any conduct by Mr. Gill that gave rise to a reasonable suspicion
3 of criminal activity, but instead reflect CPD’s suspicion of Mr. Gill because of his religion. One
4 of the incidents occurred before CPD filed the SAR about Mr. Gill on or about May 23, 2012;
5 the other occurred after. This religious harassment is attributable to the training of local law
6 enforcement on the SARs standards and process.

7 91. In approximately September 2010, after Mr. Gill had converted to Islam, two
8 CPD officers visited him at his apartment and requested to speak to him about supposedly “anti-
9 American statements” that he had made. One of the officers referred to having a file on Mr. Gill,
10 refused to explain what “anti-American statements” Mr. Gill had purportedly made or the source
11 of the information, and stated that he wished to ensure Mr. Gill would not turn into another
12 Mohammed Atta, one of the individuals identified as a September 11 hijacker. Mr. Gill still does
13 not know how he came to the attention of the CPD.

14 92. Around or after July 2012, Mr. Gill also received a telephone call from a CPD
15 officer. Over the phone, the CPD officer said Mr. Gill should shut down his Facebook page
16 because of the video games Mr. Gill played. At the time, Mr. Gill had a picture of the Shahada,
17 the Muslim statement of faith, on his Facebook page. Mr. Gill told the CPD officer he would not
18 take down his Facebook page and Mr. Gill also told the CPD officer that he believed the CPD
19 wanted Mr. Gill to take down his Facebook page because of its references to Islam. The CPD
20 officer refused to comment on Mr. Gill’s observation, but stated that he had a report on Mr. Gill
21 and indicated that Mr. Gill was on some kind of watch list.

22 93. By describing Mr. Gill’s conversion to Islam and “pious demeanor” in the SAR as
23 “worthy of note,” CPD implicitly acknowledges that it found him “suspicious” because he is a
24 devout Muslim.

25 94. Defendants’ issuance of overly broad definitions of “suspicious activity” and the
26 categories of behavior they have identified as “suspicious” include, among other things,
27 “[a]cquisition of expertise” (PM-ISE) and “[n]o obvious signs of employment” (DOJ). On
28 information and belief, CPD officers are trained in Defendants’ standards for SAR reporting.

1 95. Defendants’ overly broad standards for reporting suspicious activity opens the
2 door to and encourages religious profiling. These standards opened the door to and encouraged
3 the religious profiling of Mr. Gill by CPD, CPD’s repeated questioning and ongoing scrutiny of
4 Mr. Gill, and CPD’s identification of Mr. Gill in a SAR as someone engaged in activity with a
5 potential nexus to terrorism.

6 96. In addition, Functional Standard 1.5 instructs law enforcement agencies at the
7 “[i]nitial [r]esponse and [i]nvestigation stage” to respond to the observation reported in a SAR,
8 and “gather[] additional facts,” by, *inter alia*, “engaging the suspect in conversation” and “other
9 investigative activities.” Functional Standard 1.5 at 32. The CPD was implementing the
10 protocols set forth in Functional Standard 1.5 when it harassed Mr. Gill on or about May 2012,
11 before, and after.

12 97. Because Mr. Gill is the subject of a SAR that falls under Defendants’ standards
13 for suspicious activity reporting, Mr. Gill has been automatically subjected to law enforcement
14 scrutiny. That scrutiny has included, among other things, CPD’s telephone call to him around or
15 after July 2012 and the FBI’s creation of a file about and investigation of Mr. Gill.

16 98. Given the repeated harassment Mr. Gill has already suffered by CPD, he fears
17 further action may be taken against him by CPD and other investigative agencies as the result of
18 this SAR. He also fears further investigative harassment at the hands of the CPD and other
19 agencies caused by the existence of the SAR.

20 99. Mr. Gill also has experienced frustration and stress resulting from the creation of
21 the SAR based on innocent conduct. He is also deeply troubled by what may result from the
22 collection, maintenance, and dissemination in a national database of a report describing him as
23 engaging in suspicious activity with a potential nexus to terrorism.

24 100. The SAR about Mr. Gill is maintained and will continue to be maintained in one
25 or more national SAR databases, where it can be accessed by law enforcement agencies across
26 the country.

27 //

28 //

1 **2. James Prigoff**

2 101. James Prigoff is a United States citizen who resides in Sacramento, California.
3 He is an internationally renowned photographer. The focus of his work is public art, such as
4 murals and graffiti art. He has amassed over 80,000 photographic slides and published several
5 books containing his photography. Mr. Prigoff is also a former business executive, having
6 served as a Senior Vice President of the Sara Lee Corporation and a President of a division of
7 Levi Strauss.

8 102. In or around the spring of 2004, Mr. Prigoff was in Boston, Massachusetts. While
9 there, he sought to photograph a famous piece of public art known as the “Rainbow Swash,”
10 located in the Dorchester neighborhood of Boston. The artwork is painted on a natural gas
11 storage tank, which is surrounded by a chain link fence. It is highly visible to commuters from
12 the local expressway.

13 103. Mr. Prigoff drove a rental car to a public area outside the fence surrounding the
14 Rainbow Swash, and set up to take photographs. He chose the location in part because of
15 favorable lighting conditions. From this location, the sun was behind him and casting its light on
16 the Rainbow Swash. Before Mr. Prigoff could take any photographs, two private security guards
17 came out from inside the fenced area and told him that he was not allowed to photograph,
18 claiming the area was private property. Mr. Prigoff pointed out to the security guards that he
19 was not, in fact, on private property. The guards still insisted that Mr. Prigoff could not
20 photograph.

21 104. To avoid a confrontation with the guards, Mr. Prigoff departed. He left without
22 giving the security guards any identifying information.

23 105. He drove further down the road to another public location outside the fenced
24 perimeter and attempted to take photographs from this second location. But the guards began to
25 follow him.

26 106. To avoid further harassment by the guards, he drove to a third location on the
27 other side of the Rainbow Swash. The guards did not follow him to this third location, and he
28 was finally able to take photographs of the Rainbow Swash unmolested. But the lighting

1 conditions were significantly inferior to those at the first two locations; from this third location,
2 he had to photograph into the sunlight.

3 107. At no point while he was attempting to photograph the Rainbow Swash did Mr.
4 Prigoff engage in conduct that gave rise to a reasonable suspicion of criminal activity.

5 108. Mr. Prigoff subsequently discovered photographs online, including on the
6 Rainbow Swash's Wikipedia webpage. These widely available photographs were taken from
7 vantage points closer than the three locations from which Mr. Prigoff attempted to and actually
8 took photographs.

9 109. Mr. Prigoff returned to his home in Sacramento, California after his trip to
10 Boston. A few months later, on or about August 19, 2004, he came home one day to find a
11 business card affixed to his door from Agent A. Ayaz of the Joint Terrorism Task Force, which,
12 as noted above, is a partnership between the FBI and other law enforcement agencies. On the
13 back was a handwritten note stating, "Mr. Prigoff, please call me. Thanks." Mr. Prigoff later
14 learned from a neighbor across the street that two agents had knocked on her door and asked for
15 information about Mr. Prigoff.

16 110. Mr. Prigoff called Mr. Ayaz, who asked if Mr. Prigoff had been to Boston.
17 Realizing that Mr. Ayaz was referring to his efforts to photograph a piece of public art, Mr.
18 Prigoff explained what had occurred. On information and belief, security guards at the site of the
19 Rainbow Swash had submitted a SAR or SAR precursor report regarding Mr. Prigoff that
20 included his rental car information, after which authorities traced him from Boston,
21 Massachusetts, to his home in Sacramento, California.

22 111. Mr. Prigoff is very upset that he was tracked cross-country from Boston to
23 Sacramento, and contacted by law enforcement agents at his home over his effort to engage in
24 photography from a public location. Mr. Prigoff is also very upset that law enforcement agents
25 questioned at least one of his neighbors about him, as such questioning casts the negative and
26 strong implication that Mr. Prigoff had somehow engaged in misconduct.

27 112. Taking photographs of infrastructure falls under one or more of the behavioral
28 categories identified by Defendant PM-ISE under Functional Standard 1.5 as "suspicious," and

1 also falls under one or more behavioral categories identified by Defendant DOJ, such as the
2 catch-all behavioral category of “acting suspiciously.” After attempting to photograph a piece of
3 public art painted on a natural gas storage tank in Boston, Mr. Prigoff was tracked to his home in
4 Sacramento and questioned about his trip to Boston, even though he never provided the security
5 guards with identifying information. On information and belief, Mr. Prigoff is the subject of a
6 SAR or SAR precursor report, which was filed by security guards at the Rainbow Swash. On
7 information and belief, the report about him was collected, maintained, and disseminated through
8 a fusion center database, and uploaded to eGuardian and/or another national SAR or similar
9 counterterrorism database. On information and belief, the report about him was collected,
10 maintained, and disseminated under standards that authorized collection, maintenance and
11 dissemination of information even in the absence of reasonable suspicion of criminal activity;
12 Defendants’ standards for SAR reporting ratify that conduct.

13 113. On information and belief, security guards at the Rainbow Swash were trained in
14 standards that encourage reporting of activity deemed connected to terrorism, even in the
15 absence of reasonable suspicion of criminal activity; Defendants’ standards for SAR reporting
16 ratify that conduct. Because of that training, they interfered with Mr. Prigoff’s lawful efforts to
17 take photographs of the Rainbow Swash.

18 114. Because Mr. Prigoff is the subject of a report that falls under Defendants’
19 standards for suspicious activity reporting, Mr. Prigoff has been automatically subjected to law
20 enforcement scrutiny. That scrutiny has included but may not be limited to a follow-up visit by
21 an agent of the Joint Terrorism Task Force to his home, a telephone call with that agent, and
22 inquiries by that agent of at least one of his neighbors about him.

23 115. Upon information and belief, the report about Mr. Prigoff is maintained and will
24 continue to be maintained in one or more national SAR or similar counterterrorism databases,
25 where it can be accessed by law enforcement agencies across the country.

26 116. Mr. Prigoff continues to be an active photographer and often takes pictures of
27 architectural structures and post offices, among other sites that could be described as
28 “infrastructure.” Because taking photographs of infrastructure falls under one or more of the

1 behavioral categories identified by Defendant PM-ISE under Functional Standard 1.5 as
2 “suspicious,” and also falls under one or more behavioral categories identified by Defendant
3 DOJ, such as the catch-all behavioral category of “acting suspiciously,” he is likely to be the
4 subject of another SAR in the future. He fears that his efforts to take photographs of such areas
5 will be hindered again in the future.

6 117. Mr. Prigoff is also deeply troubled by what may result from the collection,
7 maintenance, and dissemination in a national database of a report describing him as engaging in
8 suspicious activity with a potential nexus to terrorism.

9 **3. Khaled Ibrahim**

10 118. Khaled Ibrahim is a United States citizen of Egyptian descent living in San Jose,
11 California. He works in accounting for Nordix Computer Corporation, a computer network
12 consulting and service company. He formerly worked as a purchasing agent for Nordix. As part
13 of his job as purchasing agent, Mr. Ibrahim bought computers in bulk from retail stores, where
14 the stores allowed such transactions.

15 119. On several occasions in 2011, Mr. Ibrahim went to the Best Buy in Dublin,
16 California in order to attempt to purchase computers in bulk for Nordix. On one such occasion,
17 he was told that management did not allow such bulk purchases and, with that, Mr. Ibrahim left.

18 120. At no point while he was attempting to purchase computers from Best Buy did
19 Mr. Ibrahim engage in conduct that gave rise to a reasonable suspicion of criminal activity.

20 121. Mr. Ibrahim is the subject of a SAR, created on November 14, 2011, regarding
21 Mr. Ibrahim’s attempts to purchase “a large amount of computers.” The SAR about him was
22 collected, maintained, and disseminated through a fusion center SAR database, and uploaded to
23 the FBI’s eGuardian database. Upon information and belief, the personnel at the fusion center
24 who uploaded Mr. Ibrahim’s SAR to eGuardian were trained in Defendants’ standards for SAR
25 reporting.

26 122. The SAR pertaining to Mr. Ibrahim falls into one or more of the behavioral
27 categories identified in Functional Standard 1.5, in particular, “[a]cquisition ... of unusual
28 quantities of materials.” Functional Standard 1.5 at 30. It also falls under one or more

1 behavioral categories identified by Defendant DOJ, such as the catch-all behavioral category of
2 “acting suspiciously” and DOJ’s “Potential Indicators of Terrorist Activities Related to
3 Electronic Stores.”

4 123. Because Mr. Ibrahim is the subject of a SAR that falls under Defendants’
5 standards for suspicious activity reporting, Mr. Ibrahim has been automatically subjected to law
6 enforcement scrutiny. That scrutiny may include but is not limited to scrutiny or interviews by
7 any of the law enforcement agencies across the country that have access to the FBI’s eGuardian
8 system, to which his SAR was uploaded.

9 124. Mr. Ibrahim is particularly disturbed that trained law enforcement personnel at a
10 fusion center uploaded the SAR about him to eGuardian, thereby flagging him as an individual
11 with a potential nexus to terrorism. He is also troubled by what may result from the collection,
12 maintenance, and dissemination in a national database of a report describing him as engaging in
13 suspicious activity with a potential nexus to terrorism. Mr. Ibrahim is upset that a SAR was
14 entered about him potentially because of his Middle Eastern descent, and believes that this
15 system of racial profiling diminishes the rights of Middle Eastern communities.

16 125. The SAR about Mr. Ibrahim is maintained and will continue to be maintained in
17 one or more national SAR databases, where it can be accessed by law enforcement agencies
18 across the country.

19 **4. Tariq Razak**

20 126. Tariq Razak is a United States citizen of Pakistani descent. He resides in
21 Placentia, California. A graduate of the University of California at Irvine, he works in the bio-
22 tech industry.

23 127. Mr. Razak is the subject of a SAR pertaining to a “Male of Middle Eastern decent
24 [sic] observed surveying entry/exit points” at the Santa Ana Train Depot.

25 128. On May 16, 2011, Santa Ana Police Officer J. Gallardo filed a SAR regarding Mr.
26 Razak. According to the SAR, Officer Gallardo responded to a call at the Santa Ana Train
27 Depot from Security Officer Karina De La Rosa. Ms. De La Rosa explained that her “suspicion
28 became aroused because the male appeared to be observant of his surroundings and was

1 constantly surveying all areas of the facility. The male's appearance was neat and clean with a
2 closely cropped beard, short hair wearing blue jeans and a blue plaid shirt." The SAR goes on to
3 describe how Mr. Razak, after studying entry/exit points moved to a part of the train station
4 where the restrooms are located and eventually departed the train station with "a female wearing
5 a white burka head dress" who had emerged from the restrooms. Office Gallardo concludes the
6 SAR by requesting that it be forwarded to the fusion center in Orange County "for review and
7 possible follow-up."

8 129. According to the SAR, Security Officer De La Rosa stated that "she received
9 'suspicious activity as related to terrorism training'" and that "the behavior depicted by the male
10 was similar to examples shown in her training raising her suspicion and making the decision to
11 notify the police." Mr. Razak is the subject of the SAR because of Defendants' trainings on their
12 SAR reporting standards to state and local law enforcement and the private sector.

13 130. Mr. Razak was, indeed, at the Santa Ana Train Depot on May 16, 2011. The
14 woman he was with was his mother. He had an appointment at the county employment resource
15 center, which is located in the station building. He had not been to the station before and spent
16 some time locating the office before meeting up with his mother by the restrooms and leaving.
17 His mother was wearing a hijab (head scarf), and not a burka.

18 131. Mr. Razak did not talk to any security officers at the Santa Ana Train Depot that
19 day. The SAR notes the make and model of Mr. Razak's vehicle, and his license plate number.
20 On information and belief, Security Officer De La Rosa followed Mr. Razak to his vehicle and
21 wrote down his license plate number to identify him.

22 132. At no point while he was waiting in the Train Depot did Mr. Razak engage in
23 conduct that gave rise to a reasonable suspicion of criminal activity.

24 133. This SAR falls into one or more of the behavioral categories identified in
25 Functional Standard 1.5, in particular, "Observation/Surveillance." Functional Standard 1.5 at
26 30. It also falls under DOJ's "Potential Indicators of Terrorist Activities Related to Mass
27 Transportation," which includes, among other things, "[u]nusual or prolonged interest in ...
28 [e]ntry points and access controls." It also falls under one or more behavioral categories

1 identified by Defendant DOJ, such as the catch-all behavioral category of “acting suspiciously.”
2 The SAR about Mr. Razak was collected, maintained, and disseminated through a fusion center
3 SAR database, and on information and belief has been uploaded to eGuardian and/or another
4 national SAR database.

5 134. Because Mr. Razak is the subject of a SAR that falls under Defendants’ standards
6 for suspicious activity reporting, Mr. Razak has been automatically subjected to law enforcement
7 scrutiny. That scrutiny may include but is not limited to scrutiny or interviews by any of the law
8 enforcement agencies across the country that have access to the SAR about him.

9 135. Mr. Razak is deeply troubled by what may result from the collection,
10 maintenance, and dissemination in a national database of a report describing him as engaging in
11 suspicious activity with a potential nexus to terrorism.

12 136. Upon information and belief, the SAR about Mr. Razak is maintained and will
13 continue to be maintained in one or more national SAR databases, where it can be accessed by
14 law enforcement agencies across the country.

15 **5. Aaron Conklin**

16 137. Aaron Conklin resides in Vallejo, California. Mr. Conklin is a student at Diablo
17 Valley College, studying graphic design. He is also an amateur photographer who posts his
18 work online. Mr. Conklin has a strong aesthetic interest in photographing industrial architecture,
19 including refineries.

20 138. In either 2011 or 2012, Mr. Conklin was photographing the Valero Refinery
21 located in Benicia, California at around 10:00 p.m. He chose to photograph at night for aesthetic
22 reasons, to capture the refinery illuminated against the dark night sky. Mr. Conklin set up in an
23 empty lot where a food truck parks during the day, near a publicly accessible sidewalk and a bus
24 stop. Mr. Conklin was positioned outside the refinery’s fenced perimeter.

25 139. Despite Mr. Conklin’s location outside the refinery’s perimeter in a publicly
26 accessible location, a private security guard from the refinery came out to tell Mr. Conklin that
27 he could not photograph the refinery and issued stern warnings. Mr. Conklin felt threatened and
28 feared that the situation would escalate if he remained, so he left. Because he fears further

1 harassment, he has not returned to photograph the refinery, despite his desire to develop his
2 portfolio with photographs of industrial sites.

3 140. Mr. Conklin later discovered that images of the refinery, taken from a similar
4 location, were viewable on the internet through Google Maps, using the site's "street view"
5 feature.

6 141. In or about November 2013, Mr. Conklin was attempting to photograph the Shell
7 Refinery located in Martinez, California at approximately 9:30 or 10:00 pm. He wished to
8 photograph the refinery at night for artistic reasons.

9 142. Mr. Conklin set up in the parking lot of a strip mall containing a smog testing
10 center and a dance studio, across the street from the Shell Refinery's fenced perimeter.

11 143. As Mr. Conklin was preparing to photograph, a private security guard came out
12 from the refinery and stopped him. At least one other guard from the refinery soon joined the
13 first security guard. The security guards told Mr. Conklin that he was prohibited from
14 photographing the refinery and that photographing the refinery was illegal and somehow
15 connected to terrorism.

16 144. Despite Mr. Conklin's complete cooperation with the security guards, they called
17 the Contra Costa County Sheriff's department, and at least two deputies arrived on the scene.
18 The deputies searched through the pictures on Mr. Conklin's camera and searched his car. They
19 also took pictures of Mr. Conklin, his camera equipment, and his vehicle. Mr. Conklin was
20 afraid and felt as though he did not have the option to object to the searches without making
21 matters worse for himself.

22 145. The deputies concluded by telling Mr. Conklin that he would have to be placed on
23 an "NSA watch list." Only then was Mr. Conklin allowed to leave. The entire encounter lasted
24 between forty-five minutes and an hour.

25 146. At no point while he was attempting to photograph the Valero or Shell refineries
26 did Mr. Conklin engage in conduct that gave rise to a reasonable suspicion of criminal activity.

27 147. Taking photographs of infrastructure falls under one or more of the behavioral
28 categories identified by Defendant PM-ISE as "suspicious," and also falls under one or more

1 behavioral categories identified by Defendant DOJ, such as the catch-all behavioral category of
2 “acting suspiciously.” A Contra Costa deputy sheriff expressly told Mr. Conklin that he had to
3 be put on an “NSA watchlist.” On information and belief, Mr. Conklin is the subject of a SAR,
4 which was collected, maintained, and disseminated through a fusion center SAR database, and
5 uploaded to eGuardian and/or another national SAR database.

6 148. On information and belief, security guards at oil refineries are trained in
7 Defendants’ standards for SAR reporting. As a result, security guards at the Valero and Shell oil
8 refineries prevented Mr. Conklin from taking photographs of sites of aesthetic interest to him.
9 On information and belief, the Contra Costa deputy sheriffs are trained in Defendants’ standards
10 for SAR reporting. As a result, they detained and searched Mr. Conklin for doing nothing more
11 than attempting to photograph a site of aesthetic interest from a public location, told Mr. Conklin
12 that he had to be placed on a watchlist, and reported Mr. Conklin in a SAR.

13 149. Because Mr. Conklin is the subject of a SAR that falls under Defendants’
14 standards for suspicious activity reporting, Mr. Conklin has been automatically subjected to law
15 enforcement scrutiny. That scrutiny may include but is not limited to scrutiny or interviews by
16 any of the law enforcement agencies across the country that have access to the SAR about him.

17 150. Mr. Conklin was very upset by the encounter with private security and Contra
18 Costa deputy sheriffs at the Shell refinery. He wants to continue taking photographs of
19 industrial architecture in the future. But because of this event and the earlier incident at the
20 Valero refinery, he is afraid to continue photographing industrial sites for fear of being stopped
21 and questioned or, worse, arrested. Mr. Conklin has been chilled and has refrained from
22 engaging in certain forms of photography, despite his desire to develop his photography
23 portfolio. His inability to develop his photography portfolio limits his ability to apply
24 successfully for jobs in his chosen field.

25 151. Mr. Conklin is also deeply troubled by what may result from the collection,
26 maintenance, and dissemination in a national database of a report describing him as engaging in
27 suspicious activity with a potential nexus to terrorism.
28

1 152. Mr. Conklin currently worries about being on a watchlist because he fears it will
2 adversely impact him in the future. For example, he is concerned about his employment
3 prospects if employers conduct background checks and he is flagged as someone with a potential
4 connection to terrorism. Mr. Conklin also currently worries about being on a watchlist because
5 he fears it will adversely impact his family. His father has worked and is seeking employment in
6 the aviation industry and as a result must undergo rigorous background checks; Mr. Conklin is
7 afraid about jeopardizing his father’s career based on his own innocent efforts to take
8 photographs of aesthetically interesting sites.

9 **FIRST CLAIM FOR RELIEF**

10 **Violation of APA by Defendants DOJ and Eric Holder for**
11 **Agency Action that is Arbitrary and Capricious and Not in Accordance with Law**
12 **5 U.S.C. §§ 702, 706(2)(A)**

13 153. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth
14 herein.

15 154. DOJ’s promulgation of DOJ’s SAR Standard constitutes final agency action.

16 155. DOJ and Eric Holder have issued a SAR Standard that sets forth operating
17 principles for the collection, maintenance, and dissemination of “criminal intelligence
18 information” within the meaning of 28 CFR Part 23. It applies to entities that operate
19 arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency
20 exchange or dissemination and analysis of criminal intelligence information. These entities and
21 the systems they operate receive support from OJP and constitute “projects” and “criminal
22 intelligence systems” within the meaning of 28 CFR Part 23.

23 156. Because DOJ’s SAR standard is broader than 28 CFR Part 23 and authorizes the
24 collection, maintenance, and dissemination of information even in the absence of reasonable
25 suspicion of criminal activity, it conflicts with 28 CFR Part 23. DOJ has also undermined 28
26 CFR Part 23 by training participants in the NSI on DOJ’s SAR Standard.

27 157. Defendants DOJ and Eric Holder have not provided a reasoned basis for adopting
28 a conflicting standard.

158. Defendants’ actions described herein were and are arbitrary, capricious, an

1 abuse of discretion, and otherwise not in accordance with law, and should be set aside as
2 unlawful pursuant to 5 U.S.C. § 706 (2012).

3 **SECOND CLAIM FOR RELIEF**

4 **Violation of APA by Defendants PM-ISE and Kshemendra Paul for**
5 **Agency Action that is Arbitrary and Capricious and Not in Accordance with Law**
6 **5 U.S.C. §§ 702, 706(2)(A)**

7 159. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth
8 herein.

9 160. PM-ISE’s promulgation of Functional Standard 1.5 constitutes final agency
10 action.

11 161. PM-ISE and Kshemendra Paul have issued a SAR Standard that sets forth
12 operating principles for the collection, maintenance, and dissemination of “criminal intelligence
13 information” within the meaning of 28 CFR Part 23. It applies to entities that operate
14 arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency
15 exchange or dissemination and analysis of criminal intelligence information. These entities and
16 the systems they operate receive support from OJP and constitute “projects” and “criminal
17 intelligence systems” within the meaning of 28 CFR Part 23.

18 162. Because Functional Standard 1.5 is broader than 28 CFR Part 23 and authorizes
19 the collection, maintenance, and dissemination of information even in the absence of reasonable
20 suspicion of criminal activity, it conflicts with 28 CFR Part 23. PM-ISE has also undermined 28
21 CFR Part 23 by training participants in the NSI on Functional Standard 1.5.

22 163. Defendants PM-ISE and Kshemendra Paul have not provided a reasoned basis for
23 adopting a conflicting standard.

24 164. Defendants’ actions described herein were and are arbitrary, capricious, an
25 abuse of discretion, otherwise not in accordance with law and should be set aside as unlawful
26 pursuant to 5 U.S.C. § 706 (2012).

27 //
28 //

THIRD CLAIM FOR RELIEF

**Violation of APA by Defendants DOJ and Eric Holder
for Issuance of a Legislative Rule Without Notice and Comment
5 U.S.C. §§ 553, 706(2)(A), (D)**

165. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

166. DOJ’s SAR’s Standard is a legislative rule but was adopted without observing the notice and comment procedure required under 5 U.S.C. § 553 (2012). Because DOJ’s SAR Standard was adopted without observing the required notice and comment procedure, Defendants’ actions described herein were and are also arbitrary, capricious, an abuse of discretion, otherwise not in accordance with law, and without observance of procedure required by law. Defendants’ actions should be set aside as unlawful pursuant to 5 U.S.C. § 706 (2012).

FOURTH CLAIM FOR RELIEF

**Violation of APA by Defendants PM-ISE and Kshemendra Paul
for Issuance of a Legislative Rule Without Notice and Comment
5 U.S.C. §§ 553, 706(2)(A), (D)**

167. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

168. PM-ISE’s Functional Standard 1.5 is a legislative rule but was adopted without observing the notice and comment procedure required under 5 U.S.C. § 553 (2012). Because PM-ISE’s Functional Standard 1.5 was adopted without observing the required notice and comment procedure, Defendants’ actions described herein were and are also arbitrary, capricious, an abuse of discretion, otherwise not in accordance with law, and without observance of procedure required by law. Defendants’ actions should be set aside as unlawful pursuant to 5 U.S.C. § 706 (2012).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray that the Court:

1. Enter a declaratory judgment that DOJ’s standard for SAR reporting is invalid and issue a permanent injunction requiring Defendants DOJ and Eric Holder to rescind DOJ’s SAR Standard and cease and desist from training participants in the NSI in DOJ’s SAR Standard.

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 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
Nasrina Bargzie (SBN 238917)
nasrinab@advancingjustice-alc.org
Yaman Salahi (SBN 288752)
yamans@advancingjustice-alc.org
55 Columbus Avenue
San Francisco, CA 94111
Telephone: 415-848-7711
Facsimile: 415-896-1702

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

AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF SAN DIEGO AND IMPERIAL
COUNTIES
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

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

By: _____ /s/ Jonathan Loeb _____

Jonathan Loeb

BINGHAM MCCUTCHEN LLP

By: _____ /s/ Linda Lye _____

Linda Lye

AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN CALIFORNIA

By: _____ /s/ Nasrina Bargzie _____

Nasrina Bargzie

ASIAN AMERICANS ADVANCING JUSTICE –
ASIAN LAW CAUCUS

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

CERTIFICATE OF SERVICE

I hereby certify that on February 16, 2018, I caused the foregoing supplemental excerpts of record to be electronically filed with the United States Court of Appeals for the Ninth Circuit, and served to counsel, via the ECF system.

/s/ Daniel Aguilar
Daniel Aguilar