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

SUPLLEMENTAL EXCERPTS OF RECORD — VOLUME 1 OF 2
(Pages 1-297)

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

Volume 2

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

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

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

Attorneys for Plaintiffs
Additional counsel listed on signature page

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

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

Plaintiffs,

v.

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

Defendants.

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

PLAINTIFFS' OPPOSITION TO DEFENDANTS' MOTION FOR SUMMARY JUDGMENT AND CROSS-MOTION FOR SUMMARY JUDGMENT; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT

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

Notably, the legislative rule inquiry is similar to the test for whether a rule is final agency action under the APA; both ask whether the agency pronouncement imposes a binding legal norm. *See Bennett v. Spear*, 520 U.S. 154, 177-78 (1997). This Court has already ruled that the Functional Standard meets this test for the simple reason that "if a state or local law enforcement agency does participate in the NSI and submits SARs, it is to do so consistent with the Defendants' Standards." Order at 9. For the same reasons that the Functional Standard establishes a "binding legal norm" for final agency action purposes, it does so for purposes of the legislative-rule inquiry. Indeed, as Defendants previously acknowledged, the legislative rule and final agency action inquiries "largely coalesce." Def. Reply ISO Mot. to Dismiss at 7:16 (Dkt. No. 28 at 12).[12]

Because the Functional Standard is a legislative rule and not a general statement of policy, Defendants violated the APA by failing to provide public notice and comment.

3. Defendants' Wholesale Failure to Provide Notice and Comment Prejudiced Plaintiffs and Undermined the Quality of the Agency's Decisionmaking.

According to Defendants, any failure to observe the "technical requirements of the APA's rulemaking procedures" is of no concern because doing so was harmless error. Def. Br. at 18. This is so, Defendants contend, because its process did not prejudice Plaintiffs, and the substantive outcome would have been the same in any event. *Id.* at 18-22. The first part of Defendants' argument is simply wrong, and the second part requires either clairvoyance or a predetermined indifference to public comment.

(a) Plaintiffs and the Public Suffered Prejudice.

Defendants assert that "the development of the Functional Standard was a collaborative

[12] Defendants incorporate by reference the argument in their motion to dismiss that the Functional Standard does not constitute final agency action. Def. Br. at 17-18. The contention is meritless for the reasons stated in the Court's order on the motion to dismiss and set forth in Plaintiffs' opposition to that motion, which Plaintiffs hereby incorporate. *See* Pltfs.' Opp. Mot. to Dismiss at 22-25 (Dkt. No. 26 at 29-32). Like the biological opinion found by the Supreme Court in *Bennett* to constitute final agency action, the Functional Standard establishes a condition on participation in the Initiative. *See Bennett*, 520 U.S. at 178 ("Biological Opinion . . . alter[ed] the legal regime" because the Bureau was "[authorized] to take endangered species if (but only if) it complie[d] with the prescribed conditions").

process that allowed for significant participation by interested parties—including NSI participants and advocacy organizations representing the privacy and civil liberty interests of individuals." Def. Br. at 20. Advocacy organizations may have commented, but the public at large and the Plaintiffs to this lawsuit did not. Section 553 is not satisfied when proxies for the public are given an opportunity to comment; it requires that the public be given that opportunity. *See Riverbend Farms, Inc. v. Madigan*, 958 F.2d 1479, 1485 (9th Cir. 1992) ("[T]he notice and comment requirements . . . are designed to ensure public participation in rulemaking."). There is a vast difference between providing a select group of insiders the opportunity to comment, and providing that opportunity to the public. *Sequoia Orange*, 973 F.2d at 758 ("[T]he appearance and integrity of the decision-making process would have benefited from a more formal procedure."); *Nat'l Ski Areas Ass'n, Inc. v. U.S. Forest Serv.*, 910 F. Supp. 2d 1269, 1278 (D. Colo. 2012) ("[T]he ability to communicate informally with an agency does not lawfully substitute for what the APA requires.").

In *Paulsen v. Daniels*, 413 F.3d 999, 1006-07 (9th Cir. 2005), the Ninth Circuit examined cases where the courts ruled the error harmless:

- In *Idaho Farm Bureau Federation v. Babbitt*, 58 F.3d 1392, 1405 (9th Cir. 1995), the agency failed to provide the required individual notice to affected counties, but it held a public hearing and the county commissioner "was aware of the proposed regulation, as demonstrated by his presenting" written and oral comments. *Paulsen*, 413 F.3d at 1006 (citing *Idaho Farm*, 58 F.3d at 1405).[13]
- In *Riverbend*, the agency failed to publish notice in the *Federal Register*, but provided individual notice to all regulated entities and the public by placing "advertisements in the newspaper before holding a public meeting." 958 F.2d at 1483, 1486. The process had existed for 35 years and was well known to plaintiffs, who did not complain until they "ran into trouble with the Department of Agriculture." *Id.* at 1488.
- In *Sagebrush Rebellion, Inc. v. Hodel*, 790 F.2d 760 (9th Cir. 1986), the agency published notice in the *Federal Register*, but the notice failed to comply with technical provisions of the Federal Land Policy and Management Act, for example, by failing to "state that the Secretary, rather than Congress, might create" a conservation area. *Id.* at 762 & n.5, 764. The court concluded that the "same public would have responded to a notice of administrative [action] as responded to the noticed congressional [action]." *Id.* at 765.

[13] Similarly, in *Nat'l Ass'n of Home Builders v. Defs. of Wildlife*, 551 U.S. 644 (2007), cited by Defendants (Def. Br. at 18-19), the Supreme Court found harmless error where the agency made an incorrect statement in the *Federal Register* regarding whether a consultation was required or voluntary *after* the consultation had taken place. 551 U.S. at 659.

The court in *Paulsen* contrasted these cases with *Buschmann v. Schweiker*, 676 F.2d 352, 356-58 (9th Cir. 1982), in which the agency did not provide the public with advance notice or an opportunity to comment on a regulation that affected Social Security Income eligibility. *Paulsen*, 413 F.3d at 1007-08. After surveying these cases, the court concluded that the error is harmless where "interested parties received some notice that sufficiently enabled them to participate in the rulemaking process before the relevant agency adopted the rule," but is prejudicial where "petitioners were given no such opportunity." *Id.* at 1007. Applying this rule, the *Paulsen* court found not harmless an agency's "fail[ure] to provide the required notice-and-comment period before effectuating [a rule]" because the error "preclud[ed] public participation in the rulemaking." *Id.* at 1006, 1008.

Three related themes emerge. First, "harmless error doctrine . . . is narrow" and "applies to technical or minor procedural violations, not total failures to comply with important rule-making processes." *Nat'l Ski Areas Ass'n*, 910 F. Supp. 2d at 1277. Second, it applies where the agency provided some kind of notice, even if technically imperfect, to affected parties and the public. Third, the error is harmless where affected parties and the public, notwithstanding a technical defect in notice, were aware of and participated in the proceedings. None is true here.

Defendants' error was not a technical defect, such as the failure to include particular language in an otherwise public notice, *see, e.g.*, *Sagebrush Rebellion*, 790 F.2d at 762 & n.5, 764, but a wholesale failure to provide public notice and comment. Under these circumstances, courts find the error prejudicial. *See, e.g.*, *Paulsen*, 413 F.3d at 1008; *Buschmann*, 676 F.2d at 356-57; *Nat'l Ski Areas Ass'n*, 910 F. Supp. 2d at 1279; *W.C. v. Heckler*, 629 F. Supp. 791, 808, 812-13 (W.D. Wash. 1985), *aff'd sub nom. W.C. v. Bowen*, 807 F.2d 1502 (9th Cir. 1987), *opinion amended on denial of reh'g*, 819 F.2d 237 (9th Cir. 1987).

Although certain advocacy organizations were invited to participate (the Record leaves unanswered how these groups were selected), AR 116-19, Defendants published no notice in the Federal Register or otherwise notified the public. In Defendants' cases, moreover, the courts found harmless error where the plaintiffs had actual notice of the challenged agency action. *See Riverbend*, 958 F.2d at 1482-83 (plaintiffs were "domestic 'handlers' of navel oranges" and the agency "notifie[d] all handlers by letter"); *Safari Aviation Inc. v. Garvey*, 300 F.3d 1144, 1149 (9th Cir. 2002) (agency issued notice of proposed rulemaking and plaintiff submitted comment). None of the Plaintiffs to this lawsuit was aware that Defendants sought input on the Functional Standard. Gill Decl. ¶ 22; Razak Decl. ¶ 24; Ibrahim Decl. ¶ 9; Prigoff Decl. ¶ 27; Conklin Decl. ¶ 14.

Finally, because Plaintiffs lacked any notice, they were "denied . . . the opportunity to comment on a new policy which directly affected" them. *See Heckler*, 629 F. Supp. at 813 (failure to provide notice was prejudicial). Each of the Plaintiffs here would have appreciated the opportunity to provide his views and would have relayed, based on his personal experience, the factual basis for his concerns about a loose standard. Gill Decl. ¶ 22; Razak Decl. ¶ 24; Ibrahim Decl. ¶ 9; Prigoff Decl. ¶ 27; Conklin Decl. ¶ 14.

(b) Defendants Cannot Know the Result of a Correct Process.

In defense of their deficient process, Defendants say "[t]he substantive outcome would have been the same." Def. Br. at 21. But this is unknowable, given that Defendants have not had an opportunity to examine the comments of the public or the Plaintiffs.

In *Safari Aviation*, on which Defendants rely, the plaintiff, who had submitted a comment that had been "overlooked" by the agency, raised the same concerns as other comments considered by the agency. 300 F.3d at 1151-52. Defendants assume that Plaintiffs' comments would similarly duplicate comments submitted by advocacy organizations. Def. Br. at 20-21. But Plaintiffs' perspective cannot be conflated with that of the advocacy organizations, which presented general *legal* arguments. The agency was not presented with, and thus did not consider, concrete *factual* evidence—such as Plaintiffs' individual stories—about harms that result from a standard that does not require reasonable suspicion. The experiences of Gill and Razak, for example, provide a concrete illustration of how the Functional Standard encourages religious profiling. *See* Gill Decl. ¶ 11 & Exh. 1 (SAR describes his "pious demeanor" as "worthy of note"); Razak Decl. ¶ 9 & Exh. 1 (SAR describes Razak, who is Pakistani, as "Middle Eastern" and "Arab," and also his mother, who was wearing a head scarf, as wearing a "burka"). As Defendants themselves observe, their decision turned on a balancing of law enforcement and privacy interests. *See* Def. Br. at 29-30 (citing AR 281-82). Factual information about the impact of their standard is precisely the kind of topic about which the agency should have educated itself in striking that balance. *See Alcaraz*, 746 F.2d at 611 (notice and comment requirement "creates a pre-publication dialogue which allows the agency to educate itself on the full range of interests the rule affects").

Defendants cite *PDK Laboratories Inc. v. DEA*, 362 F.3d 786 (D.C. Cir. 2004), but that case rejected the very argument Defendants make here—that "the result of the agency proceedings would not have changed" if it had considered a particular issue. *See id.* at 799.

Riverbend Farms states the other obvious problem with taking Defendants' position: "if the harmless error rule were to look solely to result, an agency could always claim that it would have adopted the same rule even if it had complied with the APA procedures." 958 F.2d at 1487.

*   *   *

The error here was not harmless. Indeed, it undermined the twin goals of the APA's procedural requirements by precluding the public and these Plaintiffs from participating and depriving agency decisionmakers of important factual information. *See Alcaraz*, 746 F.2d at 611 (discussing purposes of APA procedural requirements).

D. Vacatur Is the Only Appropriate Remedy.

The Court should vacate the Functional Standard. Defendants' violations of the APA were serious, and they have not met their burden of demonstrating disruptive consequences.

The APA states in mandatory terms that a "reviewing court shall . . . hold unlawful and set aside agency action" that is arbitrary and capricious or adopted "without observance of procedure required by law." 5 U.S.C. § 706(2). As some appellate judges have observed, "'[s]hall' means 'must'" and there is "no play in the joints." *Comcast Corp. v. FCC*, 579 F.3d 1, 10 (D.C. Cir. 2009) (Randolph, J., concurring). Nevertheless, the Ninth Circuit has permitted remand without vacatur, but "only in 'limited circumstances.'" *See Pollinator Stewardship Council v. EPA*, 806 F.3d 520, 532 (9th Cir. 2015); *Klamath-Siskiyou Wildlands Ctr. v. Nat'l Oceanic & Atmospheric Admin. Nat'l Marine Fisheries Serv.*, 109 F. Supp. 3d 1238, 1239 (N.D. Cal. 2015) ("[C]ourts within this circuit rarely remand without vacatur."). In determining whether to vacate an invalid

BENJAMIN C. MIZER
Principal Deputy Attorney General
ANTHONY J. COPPOLINO
Deputy Branch Director
KIERAN G. GOSTIN
Trial Attorney
D.C. Bar No. 1019779

Civil Division, Federal Programs Branch
U.S. Department of Justice
P.O. Box 883
Washington, D.C. 20044
Telephone: (202) 353-4556
Facsimile: (202) 616-8460
E-mail: kieran.g.gostin@usdoj.gov

Attorneys for Federal Defendants

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

WILEY GILL; JAMES PRIGOFF; TARIQ RAZAK; KHALID IBRAHIM; and AARON CONKLIN, Plaintiffs, v. DEPARTMENT OF JUSTICE, *et al.*, Defendants.	No. 3:14-cv-03120 (RS) (KAW) **DECLARATION OF BASIL N. HARRIS**

challenges, framed appropriate mission processes, and put in place protections appropriate for a coordinated approach to information sharing and safeguarding.

6. PM-ISE issued Functional Standard 1.0 on January 25, 2008. A.R. at 75–106. It was provided to the heads of all federal departments and agencies by memorandum, A.R. at 71–106, and made available to the public via the internet at www.ise.gov. As a matter of practice, PM-ISE posted documents of this type on or shortly after the issuance of the document, in order to ensure transparency. Functional Standard 1.0 also indicated that PM-ISE would periodically issue new or modified versions of the Functional Standard. A.R. at 77.

7. Following the issuance of Functional Standard 1.0, PM-ISE informed numerous groups that it intended to update this standard. To ensure that the public interest was represented in the updating process, PM-ISE solicited inputs and commentary from those groups.

8. PM-ISE held meetings with representatives of NSI participants at all levels of government, as well as with representatives of numerous privacy and civil liberties organizations. Among others, these organizations included the American Civil Liberties Union (ACLU), the Muslim Public Affairs Council; the Muslim Advocates, the Center for Democracy and Technology (CDT), the American-Arab Anti-Discrimination Committee, the Islamic Shura Council of Southern California, American Probation and Parole Association, state and local law enforcement agencies from various states (Pennsylvania, Minnesota, Georgia, New Jersey, Seattle, Iowa), the Department of Homeland Security, the Office of the Director for National Intelligence, and the Department of Justice. *See, e.g.*, A.R. at 116–119. On September 3, 2008, for example, the Office of PM-ISE hosted a Dialogue on Privacy and Civil Liberties that provided numerous groups, including those named above, the opportunity to discuss their privacy and civil liberties perspectives on the SAR process and to offer recommendations regarding the policies and safeguards that should be implemented. A.R. at 114–115, 120.

9. An additional "feedback session" with privacy and civil liberties advocates was held on February 18, 2009 and included representatives from many of the same organizations as those in

SUPPLEMENTAL ADMINISTRATIVE RECORD INDEX

	DOCUMENT INFORMATION	BATES NUMBER	REDACTION[1]
1	ISE Privacy Guidelines (December 4, 2006)	**001-009**	None
2	May 22, 2007 Review 2: Agenda May 22, 2007 Review 2: Agenda (May, 22, 2007)	**010**	None
3	National Strategy for Information Sharing (October 2007)	**011-058**	None
4	December 2007 SAR WG Meeting Agenda (December 13, 2007)	**059**	01
5	Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project (October 1, 2008)	**060-097**	01
6	ISE Suspicious Activity Reporting Evaluation Environment Segment Architecture (December 2008)	**098-188**	None
7	ISE SAR Evaluation Environment Implementation Guide, Version 1.0 (January 9, 2009)	**189-218**	01 & 03
8	Final Report: Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Evaluation Environment (January 2010)	**219-381**	01 & 03
9	Review of Advocate Websites for Concerns and Issues on ISE-Related Activities (2012)	**382-388**	None
10	Meeting Agenda for May 20, 2013DOJ/FBI Functional Standard Stakeholders Meeting (May 13, 2013)	**389**	None
11	Sign-in sheet for May 2013 DOJ/FBI Functional Standard Stakeholders Meeting (May 20, 2013)	**390**	01, 02 & 03
12	Sign-in sheet for May 2013 DHS Functional Standard Stakeholders Meeting (May 24, 2013)	**391**	01 & 03
13	Attendee list for November 2014 NSI Functional Standard Meeting (November 18, 2014)	**392**	01, 02 & 03

[1] The nature of each of the redactions is explained in Defendants' Notice of Filing of Administrative Record. Dkt. No. 52.

14	Email from Mike Sena re: Proposed Final ISE-SAR Functional Standard Version 1.5.5 (November 21, 2014)	**393-394**	01, 02, & 03
15	Email from Vernon Keenan re: Proposed Final ISE-SAR Functional Standard Version 1.5.5 (November 24, 2014)	**395-396**	01, 02, & 03

NATIONAL STRATEGY FOR

INFORMATION SHARING

Successes and Challenges In Improving Terrorism-Related Information Sharing

OCTOBER 2007

NATIONAL STRATEGY FOR INFORMATION SHARING

Successes and Challenges
In Improving
Terrorism-Related
Information Sharing

OCTOBER 2007

Contents

Introduction and Overview

Our success in preventing future terrorist attacks depends upon our ability to gather, analyze, and share information and intelligence regarding those who want to attack us, the tactics that they use, and the targets that they intend to attack. Our *National Strategy for Combating Terrorism*, issued in September 2006, recognizes that the War on Terror is a different kind of war, which requires a paradigm shift and the application of all elements of our national power and influence. The intelligence and information sharing structures that once enabled the winning of the Cold War now require greater flexibility and resilience to confront the threats facing our Nation from a transnational terrorist movement determined to destroy our people, our freedoms, and our way of life.

For the past six years, this Administration has worked within the Federal Government, and with our State, local, tribal, private sector, and foreign partners to transform our policies, processes, procedures, and—most importantly—our workplace cultures to reinforce the imperative of improved information sharing. The exchange of information should be the rule, not the exception, in our efforts to combat the terrorist threat. Substantial improvements have occurred within individual agencies and disciplines, but there is still more to be done. Improving information sharing in the post–September 11 world requires an environment that supports the sharing of information across all levels of government, disciplines, and security domains. As with our achievements to date, an improved information sharing environment will not be constructed overnight, but rather will evolve over time and will be the fruit of careful cultivation. An improved information sharing environment also will be constructed upon a foundation of trusted partnerships among all levels of government, the private sector, and our foreign allies—partnerships based on a shared commitment to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism. This *Strategy* sets forth the Administration's vision of what improvements are needed and how they can be achieved.

The *Strategy* was developed with the understanding that homeland security information, terrorism information, and law enforcement information related to terrorism can come from multiple sources, all levels of government, as well as from private sector organizations and foreign sources. Federal, State, local, and tribal government organizations use such information for multiple purposes. In addition to traditional law enforcement uses, such information is used to (1) support efforts to prevent terrorist attacks, (2) develop critical infrastructure protection and resilience plans, (3) prioritize emergency management, response, and recovery planning activities, (4) devise training and exercise programs, and (5) determine the allocation of funding and other resources for homeland security-related purposes.

The Need for a National Strategy

While improved information sharing has been an Administration priority since the September 11 attacks, this *Strategy* reflects the first time the Administration has articulated the full contours of its vision in a single document. Memorializing the *Strategy* in a single document not only provides information to others about the Administration's plans and outlook, but also guides our efforts as we continue to implement many programs and initiatives designed to advance and facilitate the sharing of terrorism-related information.

This *Strategy* will assist the Administration in ensuring that Federal, State, local and tribal government employees responsible for protecting our Nation from future attacks or responding should an attack occur understand the Administration's expectations and plans for achieving improvements in the gathering and sharing of information related to terrorism.

Accordingly, while this *Strategy* describes the vision that has guided the Administration for the past six years, it also sets forth our plan to build upon progress and establish a more integrated information sharing capability to ensure that those who need information to protect our Nation from terrorism will receive it and those who have that information will share it. We will improve interagency information sharing at the Federal level, while building information sharing bridges between the Federal Government and our non-Federal partners.

Guiding Principles

Those responsible for combating terrorism must have access to timely and accurate information regarding those who want to attack us, their plans and activities, and the targets that they intend to attack. That information guides our efforts to:

- Identify rapidly both immediate and long-term threats;
- Identify persons involved in terrorism-related activities; and
- Implement information-driven and risk-based detection, prevention, deterrence, response, protection, and emergency management efforts.

Experience has shown that there is no single source for information related to terrorism. It is derived by gathering, fusing, analyzing, and evaluating relevant information from a broad array of sources on a continual basis. Important information can come through the efforts of the Intelligence Community, Federal, State, tribal, and local law enforcement and homeland security authorities, other government agencies (e.g., the Department of Transportation, the Department of Health and Human Services), and the private sector (e.g., the transportation, healthcare, financial, and information technology sectors). Commonly referred to as homeland security information, terrorism information, or law enforcement information, this wide-ranging information can be found across all levels of government as well as in the private sector.

This *Strategy* provides the vision for how our Nation will best use and build upon the information sharing innovations which have emerged post-September 11 in order to develop a fully coordinated and integrated information sharing capability that supports our efforts to combat terrorism. The *Strategy* is founded on the following core principles and understandings:

- Effective information sharing comes through strong partnerships among Federal, State, local, and tribal authorities, private sector organizations, and our foreign partners and allies;
- Information acquired for one purpose, or under one set of authorities, might provide unique insights when combined, in accordance with applicable law, with seemingly

unrelated information from other sources, and therefore we must foster a culture of awareness in which people at all levels of government remain cognizant of the functions and needs of others and use knowledge and information from all sources to support counterterrorism efforts;

- Information sharing must be woven into all aspects of counterterrorism activity, including preventive and protective actions, actionable responses, criminal and counterterrorism investigative activities, event preparedness, and response to and recovery from catastrophic events;
- The procedures, processes, and systems that support information sharing must draw upon and integrate existing technical capabilities and must respect established authorities and responsibilities; and
- State and major urban area fusion centers represent a valuable information sharing resource and should be incorporated into the national information sharing framework, which will require that fusion centers achieve a baseline level of capability to gather, process, share, and utilize information and operate in a manner that respects individuals' privacy rights and other legal rights protected by U.S. laws.

Foundational Elements

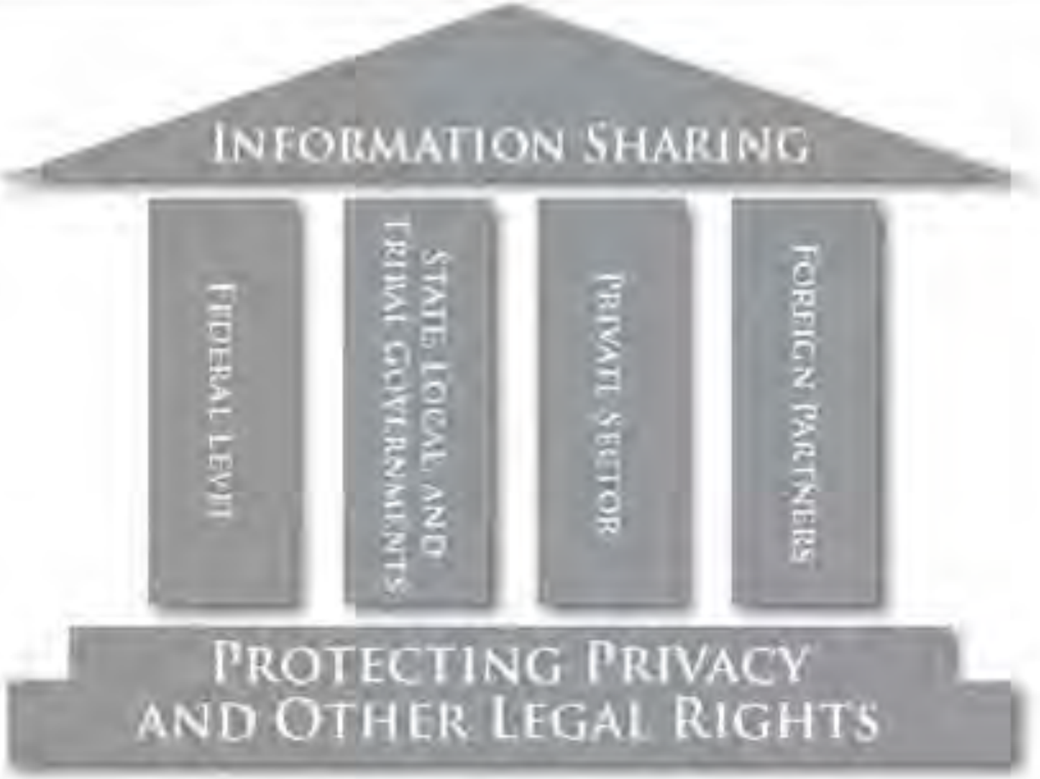
This *Strategy* is focused on improving the sharing of homeland security, terrorism, and law enforcement information related to terrorism within and among all levels of governments and the private sector.

- **Information Sharing at the Federal Level.** The instruments of our national power have long depended on the capabilities of the Intelligence Community to collect, process, analyze, and disseminate intelligence regarding our adversaries and enemies. Our efforts to combat terrorism depend on enhancing those intelligence capabilities, while enabling other Federal departments and agencies responsible for protecting the United States and its interests to regularly share information and intelligence with other public and private entities in support of mission critical activities. Information sharing at the Federal level has improved significantly since September 11, but challenges still remain that must be addressed before our strategic vision is realized.
- **Information Sharing with State, Local, and Tribal Entities.** As our Nation's first "preventers and responders," State, local, and tribal governments are critical to our efforts to prevent future terrorist attacks and to respond if an attack occurs. They must have access to the information that enables them to protect our local communities. In addition, these State, local, and tribal officials are often best able to identify potential threats that exist within their jurisdictions. They are full and trusted partners with the Federal Government in our Nation's efforts to combat terrorism, and therefore they must be a part of an information sharing framework that supports an effective and efficient two-way flow of information enabling officials at all levels of government to counter and respond to threats.

- **Information Sharing with the Private Sector.** Private sector information represents a crucial element in both understanding the current threat environment and protecting our nation's critical infrastructure from targeted attacks. The private sector owns and operates over 85% of the nation's critical infrastructure and is therefore a primary source of important vulnerability and other potentially relevant consequence information. Some private sector entities have cultivated effective information sharing partnerships with the State and local authorities that regulate their activities in the localities in which they operate. Important elements of the private sector have made significant investments to develop mechanisms and methodologies to evaluate, assess, and exchange information across regional, market, and security-related communities of interest; however still more can be done to improve those mechanisms and communication. We will use both sector-specific and geographic strategies to ensure effective information sharing with the private sector.

- **Sharing Information with Foreign Partners.** In the immediate wake of the September 11 attacks, many foreign governments joined the United States as partners in the Global War on Terrorism, and many have since contributed to the war in important ways. The events of the past six years have reaffirmed that risks and threats often emerge and take shape without regard to geographic borders. Intelligence provided by foreign partners often provides the first indications of terrorist plans and intentions. Accordingly, we are taking steps to evaluate and improve upon our sharing of information with foreign governments and encouraging them to share with us.

- **Protecting Information Privacy and Other Legal Rights.** It will remain essential to continue to protect the information privacy and other legal rights of Americans as we protect our Nation from terrorism. Accordingly, our efforts will remain relentless on two fronts -- protecting our people, communities, and infrastructure from attack and zealously protecting the information privacy and other legal rights of Americans. At the President's direction, the Attorney General and the Director of National Intelligence developed guidelines that describe how executive departments and agencies will protect the information privacy and other legal rights of Americans when sharing information related to terrorism. Consistent with the *Intelligence Reform and Terrorism Prevention Act of 2004*, the guidelines were developed in consultation with the Privacy and Civil Liberties Oversight Board.


INFORMATION SHARING
FEDERAL LEVEL
STATE, LOCAL, AND TRIBAL GOVERNMENTS
PRIVATE SECTOR
FOREIGN PARTNERS
PROTECTING PRIVACY AND OTHER LEGAL RIGHTS

Foundations of the National Strategy for Information Sharing

Linkage with Other National Strategies

The *National Strategy for Information Sharing* does not exist in a vacuum. It is a critical component of our Nation's comprehensive approach for combating terrorism. As such, it takes its lead from the President's *National Security Strategy*, which provides the broad vision and goals for confronting the national security challenges of the 21st century. In addition, it is closely aligned with the *National Strategy for Combating Terrorism* and the *National Strategy for Homeland Security*.

This *Strategy* also supports and supplements the National Implementation Plan, which is the foundational document guiding the efforts of the Directorate of Strategic Operational Planning in the National Counterterrorism Center, required by the *Intelligence Reform and Terrorism Prevention Act of 2004*. The National Implementation Plan integrates the activities of all elements of national power into our efforts to combat terrorism. Additionally, the *Strategy* supports and supplements other relevant planning efforts, such as those associated with the implementation of the National Response Plan and the establishment of a National Command and Coordination Capability.

Finally, this *Strategy* aligns with the *National Intelligence Strategy*, published at Presidential direction by the Director of National Intelligence in October 2005. An information sharing framework is recognized as a critical component of intelligence reform in the *National Intelligence Strategy*.

Background and the Current Environment

One clear lesson of September 11 was the need to improve the sharing of information. To prevent further attacks and to protect the homeland, we need to stay a step ahead of those individuals and organizations intent upon harming America. Key to preventing future attacks is the gathering of information about terrorist risks and threats and then ensuring that the information gets into the hands of those whose responsibility it is to protect our communities and critical infrastructure. In the past six years, we have achieved significant accomplishments in our efforts to improve information sharing, and we are well positioned in the current environment to build upon those past accomplishments as we move forward.

What has been accomplished since the September 11 attacks?

In the aftermath of the September 11 terrorist attacks, our Nation began a historic transformation aimed at preventing future attacks and improving our ability to protect and defend our people and institutions at home and abroad. As a result, we are now better informed of terrorist intentions and plans and better prepared to detect, prevent, and respond to their actions. Improved intelligence collection and analysis have helped paint a more complete picture of the threat, while more information sharing has provided us a greater capacity for coordinated and integrated action.

- We worked with the Congress to adopt, implement, and renew key reforms like the USA PATRIOT Act that remove barriers that once restricted the sharing of information between the law enforcement and intelligence communities, while at the same time protecting our fundamental liberties.
- We established the Department of Homeland Security (DHS) in part to improve the sharing of information among Federal, State, and local government agencies and the private sector, in order to enhance our Nation's ability to detect, identify, understand, and assess terrorist threats to and vulnerabilities of the homeland to better protect our Nation's critical infrastructure, integrate our emergency response networks, and link State and Federal governments.
- We reorganized the Intelligence Community. The position of Director of National Intelligence was created to serve as the President's chief intelligence advisor and the head of the Intelligence Community and to ensure closer coordination and integration of the 16 agencies that make up the Intelligence Community.
- We established the National Counterterrorism Center (NCTC) to serve as a multiagency center analyzing and integrating all intelligence pertaining to terrorism, including threats to U.S. interests at home and abroad.
- We worked to develop an Information Sharing Environment (ISE) to enhance the sharing of terrorism-related information among Federal, State, local, and tribal governments and the private sector. The President designated a Program Manager for the ISE to lead

these efforts. The President also issued guidelines to inform the continued development of the ISE.

- We have worked to achieve the objectives set out in the President's guidelines by devising and instituting various initiatives designed to improve information sharing both at the Federal level and with our partners at the State, local, and tribal level, as well as with our foreign partners, while simultaneously taking great care to ensure that mechanisms are in place to protect the information privacy and other legal rights of Americans.
- We established the Terrorist Screening Center to consolidate terrorist watch lists and provide around-the-clock operational support for Federal and other law enforcement personnel across the country.
- We have provided significant grant funding to support the establishment of State and major urban area information fusion centers. Fusion centers coordinate the gathering, analysis, and sharing of criminal intelligence, public safety information, and other information related to terrorism within specific States or localities. As of September 1, 2007, 58 fusion centers have either been established or are in the process of being established.
- We have brought about significant growth and maturation of the 101 Joint Terrorism Task Forces (JTTF) in major cities throughout the United States. The JTTFs have substantially contributed to improved information sharing and operational capabilities at the State and municipal levels.
- The Attorney General and the Director of the Federal Bureau of Investigation (FBI) have worked with the Director of National Intelligence to create the FBI National Security Branch by merging the FBI Counterterrorism and Counterintelligence Divisions with the newly established Directorates of Intelligence and Weapons of Mass Destruction. Establishment of the Directorate of Intelligence and of Field Intelligence Groups in every FBI field office exemplify the FBI's major steps to transform itself into a preeminent domestic counterterrorism agency.
- The Secretary of Homeland Security has appointed a Chief Intelligence Officer responsible for integrating the intelligence activities of all DHS components.
- We have established the U.S. Northern Command within the Department of Defense (DoD) to plan, organize, and execute military, homeland defense, and civil support missions in the continental United States, Alaska, and offshore waters.
- The National Guard Bureau has completed a major organizational transformation including establishment of the National Guard Bureau Joint Staff focused on Homeland Defense and Defense Support of Civil Authorities mission requirements and the creation of a single Joint Force Headquarters in each of the States and Territories.
- DHS has expanded the Homeland Security Information Network, a computer-based counterterrorism communications network, to all 50 States, five territories, the District of Columbia, and 50 other major urban areas to strengthen the two-way flow of

threat information among Federal, State, local, and tribal officials. Additionally, DHS is streamlining and merging its disparate classified networks into a single, integrated network called the Homeland Secure Data Network, to provide classified access to State, local, and tribal governments.

- The Department of State has initiated a Visa and Passport Security Program and Strategic Plan to target and disrupt individuals or organizations worldwide that are involved in the fraudulent production, distribution, or use of visas and passports, or other similar activities, intended to aid unlawful entry into the United States.
- The State Department's Bureau of Diplomatic Security has enhanced the Rewards for Justice Program to encourage reporting to authorities with tips, leads, and other information critical to preventing or favorably resolving acts of international terrorism against U.S. persons or property worldwide.
- The Department of Treasury has worked to upgrade and enhance its classified communications networks to be fully compatible with the Intelligence Community's in order to ensure that information related to terrorist financing and other national security threats related to financial crime are safely and efficiently communicated to and coordinated with the Intelligence Community.

Through these and other efforts, the United States and its coalition partners have made significant strides against al-Qaida, its affiliates, and others who threaten us. Collaboration and information sharing have helped limit the ability of al-Qaida and like-minded terrorist groups to operate successfully. We have uncovered and eliminated numerous threats to our citizens and to our friends and allies. We have disrupted terrorist plots, arrested operatives, captured or killed senior leaders, and strengthened the capacity of the Nation to confront and defeat our adversaries.

Continuing Challenges

We are engaged in what some have termed "a long war," or a "protracted conflict," and our enemy has proved to be adept at evolving and adapting his tactics. Internationally, al-Qaida remains the most serious threat to the Homeland as its central leaderships continues to plan high impact attacks while pushing others in extremist communities to mimic its efforts and supplement its capabilities. Its leadership is being reconstituted, and new jihadists are being recruited and trained daily. Additionally, the spread of radical internet sites, increasingly aggressive anti-U.S. rhetoric and actions, and the growing number of radical, self-generating cells in Western countries indicate that the radical and violent segment of the West's Muslim population is expanding. As a result, the Untied States will continue to face ideologically committed extremists determined to attack our interests at home and abroad.

Serious challenges lie ahead, including defeating the enemy, denying safe haven, combating violent extremist ideologies, and protecting the homeland. For the foreseeable future, those challenges will continue to be a top priority for the Federal Government on all fronts – intelligence, diplomatic, homeland security, law enforcement, and defense.

While these instruments of our national power are mighty, the nature of the global threat, as well as the emergence of homegrown extremists, require that State, local, and tribal governments incorporate counterterrorism activities as part of their daily efforts to provide emergency and non-emergency services to the public. These partners are now a critical component of our Nation's security capability as both "first preventers" and "first responders," and their efforts have achieved concrete results within their communities, as the following examples illustrate:

- A narcotics investigation – conducted by Federal, State, and local law enforcement officials and resulting in multiple arrests – revealed that a Canadian-based organization supplying precursor chemicals to Mexican methamphetamine producers was in fact a Hezbollah support cell.
- A local police detective investigating a gas station robbery uncovered a homegrown jihadist cell planning a series of attacks.
- An investigation into cigarette smuggling initiated by a county sheriff's department uncovered a Hezbollah support cell operating in several States.

To combat and prevent terrorist actions effectively we must first acquire knowledge about their organizations' plans, intentions, and tactics, and then ensure that such knowledge is available to those responsible for preventing and responding to attacks. The Intelligence Community will continue to be a primary source for this information; however, the Intelligence Community must modify its processes and procedures to encompass non-traditional customers at all levels of government with roles in prevention and response. In addition, important information regarding possible attack planning may come from organizations outside the Intelligence Community. Our challenge is to ensure that information from all sources is brought to bear on our efforts to protect our people and infrastructure from terrorist attacks.

Today, the sharing of terrorism-related information takes place within multiple independent sharing environments that serve five communities—intelligence, law enforcement, defense, homeland security, and foreign affairs. Historically, each community developed its own policies, rules, standards, architectures, and systems to channel information to meet mission requirements. These environments were insulated from one another, which resulted in gaps and seams in the sharing of information across all levels of government.

Recognizing these significant challenges, the Congress passed and the President signed the *Intelligence Reform and Terrorism Prevention Act of 2004*. Among other things, the law called for the creation of the ISE to enable trusted partnerships among all levels of government, the private sector, and our foreign partners, in order to more effectively detect, prevent, disrupt, preempt, and mitigate the effects of terrorism against the territory, people, and interests of the United States. This partnership will enable the trusted, secure, and appropriate exchange of terrorism-related information across the Federal Government, to and from State, local, and tribal governments, foreign allies, and the private sector, and at all levels of security classifications.

Through this *Strategy* and the use of the ISE we will:

- Enable greater coordination at the Federal level, so that strategic and time-sensitive threat information gets into the hands of those who need it to protect our local communities and our Nation's interests at home and abroad;
- Facilitate the exchange of coordinated sets of requirements and information needs across the Federal and non-Federal domains to help guide the targeting, selection, and reporting of terrorism-related information;
- Make certain that intelligence products can be easily shared, as appropriate, with those outside the Intelligence Community, such as other Federal entities, State, local, tribal, and foreign governments, and the private sector;
- Enable State, local, and tribal government efforts to gather, process, analyze, and share information and intelligence;
- Establish a network of State and local information fusion centers operating in a manner that safeguards information privacy rights and other legal rights of Americans;
- Ensure our efforts to prevent future terrorist attacks are risk-based, information-driven, and supported by a greater understanding of our adversaries' motivations, intentions, and plans; and
- Change government culture to one in which information is regularly and responsibly shared and only withheld by exception.

Although the effort to implement the ISE is well underway, it is essential for implementation activities to take place within a broader strategic context. The sections that follow describe in more detail the current environment, the key elements of our National *Strategy*, and the actions we will take to achieve our vision.

Legislative and Regulatory Background

On August 27, 2004, the President issued two Executive Orders pertinent to this *Strategy*. Executive Order 13354 established the NCTC as "the primary organization in the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism [with the exception of] purely domestic counterterrorism information." Executive Order 13356 was aimed directly at strengthening the sharing of terrorism information to protect Americans. Specifically, the President directed agencies to give the "highest priority" to the prevention of terrorism and the "interchange of terrorism information [both] among agencies" and "between agencies and appropriate authorities of States and local governments." The President further directed that this improved information sharing be accomplished in ways that "protect the freedom, information privacy, and other legal rights of Americans."

The *Intelligence Reform and Terrorism Prevention Act*, enacted in December 2004, placed NCTC within the newly created Office of the Director of National Intelligence. The law directed NCTC to "serve as the primary organization in the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism." In addition, NCTC serves as "the central and shared knowledge bank on known and suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contacts and support." The NCTC strives to ensure that agencies, as appropriate, receive and have access to the intelligence necessary to perform their counterterrorism missions.

Section 1016 of the *Intelligence Reform and Terrorism Prevention Act of 2004* directed the establishment of the ISE, which it defined as "an approach that facilitates the sharing of terrorism information." The President was charged to create the ISE, designate its organization and management structure, and determine and enforce the policies and rules to govern the ISE's content and usage. The law further required the ISE be "a decentralized, distributed, and coordinated environment" that "to the greatest extent practicable, … connects existing systems … ; builds upon existing systems capabilities currently in use across the Government; … facilitates the sharing of information at and across all levels of security; … and incorporates protections for individuals' privacy and civil liberties."

In addition, the law required the President designate a Program Manager for the ISE. The role of the Program Manager is to manage the ISE, oversee its implementation, assist in the development of ISE standards and practices, and monitor and assess its implementation by Federal departments and agencies. The law also established an Information Sharing Council to advise the President and the Program Manager on the development of ISE policies, procedures, guidelines, and standards, and to ensure proper coordination among Federal departments and agencies participating in the ISE.

Accordingly, the President designated the Program Manager and directed that the Program Manager and his staff be located in the Office of the Director of National Intelligence. On October 25, 2005, the President issued Executive Order 13388, superseding Executive Order 13356, to facilitate the work of the Program Manager, expedite the establishment of the ISE, and restructure the Information Sharing Council.

On December 16, 2005, in accordance with section 1016 of the *Intelligence Reform and Terrorism Prevention Act of 2004*, the President issued a Memorandum to Heads of Executive Departments and Agencies prescribing the guidelines and requirements in support of the creation and implementation of the ISE. In the December Memorandum, the President directed that the ISE be established by building upon "existing Federal Government policies, standards, procedures, programs, systems, and architectures (collectively "resources") used for the sharing and integration of and access to terrorism-related information, and … leverage those resources to the maximum extent practicable, with the objective of establishing a decentralized, comprehensive, and coordinated environment for the sharing and integration of such information." He also directed the heads of executive departments and agencies to "actively work to create a culture of information sharing within their respective departments or agencies by assigning personnel and dedicating resources to terrorism-related information sharing, by reducing disincentives to such sharing, and by holding their senior managers accountable for improved and increased sharing of such information."

The President's Memorandum also included five specific guidelines designed to advance the development and implementation of the ISE.

- ***Guideline One:*** the President directed that common standards be developed "to maximize the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE, consistent with the protection of intelligence, law enforcement, protective, and military sources, methods, and activities." These common standards, the President further directed, must accommodate and account for the need to improve upon the sharing of terrorism-related information with State, local, and tribal governments and the private sector.
- ***Guideline Two:*** the President stressed that "war on terror must be a national effort" and therefore one in which State, local, and tribal governments and the private sector are afforded appropriate opportunities to participate as full partners in the ISE. Accordingly, he directed that a common framework be developed governing the roles and responsibilities of Federal departments and agencies relating to the sharing of terrorism information, homeland security information, and law enforcement information among Federal departments and agencies, State, local, and tribal governments, and private sector entities.
- ***Guideline Three:*** the President directed a series of actions be undertaken to improve upon the sharing of Sensitive but Unclassified (SBU) information. Specifically, he directed the heads of particular departments and agencies to submit recommendations for the standardization of SBU procedures for marking and handling terrorism information, homeland security information, and law enforcement information, and eventually all other types of information shared within the ISE.
- ***Guideline Four:*** the President recognized the imperative for the ISE to facilitate and support the appropriate exchange of terrorism information with our foreign partners and allies and, toward that end, directed the development of recommendations to achieve improved sharing in this area.
- ***Guideline Five:*** the President directed, as he did earlier in Executive Order 13353, that the information privacy rights and other legal rights of Americans must be protected. Accordingly, he required guidelines be developed and submitted for approval to ensure such rights are protected in the implementation and operation of the ISE.

On November 16, 2006, pursuant to the President's delegation of authority, the Director of National Intelligence submitted to the Congress a report containing the *Implementation Plan for the Information Sharing Environment.* The ISE Implementation Plan, among other things, delineates how the President's guidelines and requirements will be implemented by drawing upon recommendations developed pursuant to those guidelines. The plan contains descriptions of the functions, capabilities, resources, and conceptual design of the ISE, a plan for deploying and operating the ISE, and a process for measuring implementation progress and performance. The plan, which is available on the Program Manager's website (www.ise.gov), was developed through a collaborative effort among the Program Manager and the member organizations of the Information Sharing Council. It also incorporates the perspectives of representatives from State, local, and tribal governments who reviewed the ISE Implementation Plan Report during its development. Since the Plan's submission to the Congress, many of its action items have been implemented.

Most recently, the *Implementing Recommendations of the 9/11 Commission Act of 2007*, enacted in August of this year, included amendments to section 1016 of the *Intelligence Reform and Terrorism Prevention Act of 2004* and to the *Homeland Security Act of 2002*. The new law expands the scope of the ISE to explicitly include homeland security information and weapons of mass destruction information. It also endorses and formalizes many of the recommendations developed in response to the President's information sharing guidelines, such as the creation of the Interagency Threat Assessment and Coordination Group, and the development of a national network of State and major urban area fusion centers.

Sharing Information at the Federal Level

Today's ISE consists of multiple sharing environments designed to serve five communities: intelligence, law enforcement, defense, homeland security, and foreign affairs. Our objective is to establish a framework for Federal agencies in the fulfillment of their individual roles and responsibilities and forge a coordinated and trusted interagency partnership and process across all five communities. This collaborative approach at the Federal level will in turn drive the manner in which terrorism-related information is shared with non-Federal partners. Those efforts support and build upon the success of ongoing initiatives at each level of government, offer practical guidance for addressing challenges that emerge, and provide the multi-agency perspective necessary to achieve the objectives of information sharing. In addition, as our information sharing efforts mature, policy and technology will lead to the introduction of additional information sources not currently included or available within those Federal communities.

NCTC has the primary responsibility within the Federal Government for analysis of all intelligence and information pertaining to terrorism, and supports the Department of Justice (DOJ), DHS, and other appropriate agencies in the fulfillment of their responsibilities to disseminate terrorism-related information. To carry out this responsibility, NCTC is staffed by personnel from many Federal departments and agencies, thus allowing the development of coordinated and integrated assessments of terrorist threats, plans, intentions, and capabilities.

NCTC also serves as the central and shared knowledge bank on known and suspected terrorists and international terror groups and ensures that agencies have access to and receive all-source intelligence support needed to execute their counterterrorism plans or perform independent, alternative and mission-oriented analysis. Authorized agencies may request information from NCTC to assist in the agency's activities, consistent with applicable law and guidelines governing access to intelligence. NCTC enables the sharing of a wide spectrum of terrorism intelligence and related information among thousands of users in the Federal counterterrorism community through its production of comprehensive, "federally coordinated," analytical products and its secure web site, NCTC Online.

All Federal departments and agencies that possess or acquire terrorism-related intelligence and information provide access to such information to NCTC for analysis and integration unless prohibited by law or otherwise directed by the President. As the "Federal Fusion Center" responsible "for analyzing and integrating all intelligence pertaining to terrorism and counterterrorism," NCTC works with appropriate Federal departments and agencies to enable the development of "federally coordinated," terrorism-related information products tailored to the needs of Federal entities. Within the NCTC, the new Interagency Threat Assessment and Coordination Group will facilitate the production of "federally coordinated" terrorism-related information products intended for dissemination to State, local, and tribal officials and private sector partners.

Our efforts to improve the sharing of information related to terrorism acknowledge the interdependent and—in some respects—overlapping responsibilities of the elements of government charged with combating terrorism, securing the homeland, and enforcing laws. We will leverage the strength of each and challenge them to collaborate to build an informed, composite understanding of the nature of the threat, strengthening the United States' posture and making us a more productive and effective partner in the effort to combat terrorism.

Sharing Information with State, Local, and Tribal Governments

Guideline 2 of the President's December 16, 2006, Memorandum to Heads of Executive Departments and Agencies directed that a common framework be developed governing the roles and responsibilities of Federal departments and agencies relating to the sharing of terrorism information, homeland security information, and law enforcement information between and among Federal departments and agencies, State, local, and tribal governments, and private sector entities.

The President's guidelines recognized that State, local, and tribal authorities are critical to our Nation's efforts to prevent future terrorist attacks and are the first to respond if an attack occurs. The attacks of September 11 illustrated that foreign terrorists wanting to commit acts of terrorism might live in our local communities and be engaged in criminal or other suspicious activity as they plan attacks on targets within the United States or its territories. At the same time, there is increasing concern regarding the potential threat posed by homegrown terrorists. While lacking formal ties to al-Qaida, these disaffected, radicalized, violent extremists often draw inspiration from al-Qaida and other global terrorist organizations. Whether a plan for a terrorist attack is homegrown or originates overseas, important knowledge that may forewarn of a future attack may be derived from information gathered by State, local, and tribal government personnel in the course of routine law enforcement and other activities.

State, local, and tribal governments carry out their counterterrorism responsibilities within the broader context of their core mission to protect the public's health and safety and to provide emergency and non-emergency services. While State and local officials work to prevent future terrorist attacks, they still must arrest criminals, put out fires, respond to traffic accidents, and deal with a host of public health and safety issues. Success in these endeavors depends on a strong partnership with the public, built on a foundation of communication and trust between local officials and the members of their community. These same partnerships will be used to protect these communities from future attacks by terrorists.

Needs of State, Local, and Tribal Governments

The informational needs of State, local, and tribal entities continue to grow as they incorporate counterterrorism and homeland security activities into their day-to-day missions. Specifically, they require access to timely, credible, and actionable information and intelligence about individuals and groups intending to carry out attacks within the United States, their organizations and their financing, potential targets, pre-attack indicators, and major events or circumstances that might influence State, local, and tribal preventive and protective postures. To implement recommendations developed pursuant to Guideline 2 of the President's Guidelines, and as key participants in the information sharing mission, State, local, and tribal entities are encouraged to undertake the following activities, in appropriate consultation and coordination with Federal departments and agencies:

- Foster a culture that recognizes the importance of fusing information regarding all crimes with national security implications, with other security-related information (e.g., criminal investigations, terrorism, public health and safety, and natural hazard emergency response);

- Support efforts to detect and prevent terrorist attacks by maintaining situational awareness of threats, alerts, and warnings, and develop critical infrastructure protection plans to ensure the security and resilience of infrastructure operations (e.g., electric power, transportation, telecommunications) within a region, State, or locality; and
- Develop training, awareness, and exercise programs to ensure that State, local, and tribal personnel are prepared to deal with terrorist strategies, tactics, capabilities, and intentions, and to test plans for preventing, preparing for, mitigating the effects of, and responding to events.

Authorities at all levels of our federal system must share a common understanding of the information needed to prevent, deter, and respond to terrorist attacks. The common understanding will be achieved through a framework that enables:

- Federal entities to work together to provide information in ways that better meet the needs of State, local, and tribal partners; and
- Information gathered at the State and local level to be processed, analyzed, disseminated, and integrated with information gathered at the Federal level.

We will have an integrated approach that allows Federal agencies to work together to produce and disseminate a federally-validated perspective on available threat information and relies on the efforts of consolidated fusion environments at the State and regional levels.

Interagency Threat Assessment and Coordination Group

To improve the coordination of the sharing of terrorism-related information, as well as to implement recommendations developed in response to the President's December 16, 2005, Memorandum to the Heads of Executive Departments and Agencies, we have established an Interagency Threat Assessment and Coordination Group (ITACG) within the NCTC. Participants in this coordination group include DHS, FBI, members of the Intelligence Community, and State and local representatives. The coordination group will enable the development of "federally coordinated" perspectives on intelligence reports and analytical products regarding terrorist threats and related issues that address the needs of State, local, tribal, and, as appropriate, private sector entities.

The ITACG supports the efforts of NCTC to produce "federally coordinated" terrorism-related information products intended for dissemination to State, local, and tribal officials and private sector partners through existing channels established by Federal departments and agencies by:

1. Enabling the development of intelligence reports on terrorist threats and related issues that represent a "federally coordinated" perspective regarding those threats and issues and that satisfy the needs of State, local, tribal, and private sector entities until such time as the ISE matures organizationally and culturally to satisfy those needs as a normal part of doing business;

2. Providing advice, counsel, and subject matter expertise to the Intelligence Community regarding the operations of State, local, and tribal officials, including how such entities use terrorism-related information to fulfill their counterterrorism responsibilities as part of their core mission of protecting their communities;
3. Enabling the production of clear, relevant, official, "federally coordinated" threat information in a timely and consistent manner;
4. Facilitating the production of "federally coordinated" situation awareness reporting for State, local, tribal, and private sector entities on significant domestic and international terrorism or terrorism-related events that have the potential to have an impact on local or regional security conditions in the United States;
5. Ensuring terrorism-related information intended for State, local, tribal, and private sector entities is rendered in a usable format that is, to the extent possible, unclassified, to facilitate further dissemination;
6. Informing and helping to shape Intelligence Community products for State, local, tribal, and private sector entities by providing advice, counsel, and subject matter expertise; and
7. Facilitating the production and posting by NCTC of "federally coordinated" terrorism-related information intended for augmentation, as appropriate, and subsequent dissemination to State, local, tribal, and private sector entities by other Federal departments and agencies. Accordingly, the ITACG will advise the Intelligence Community on how to tailor its products to satisfy the needs of DHS, FBI, and other Federal entities so that they in turn can better serve their consumers.

The efforts of the ITACG complement and supplement existing analytic, production, and dissemination efforts by Federal entities. The location at NCTC affords the coordination group direct access to experts assigned to NCTC and other co-located organizations such as the National Joint Terrorism Task Force to effect decisions rapidly regarding sanitization and release of information to be shared with State, local, and tribal officials, and the private sector.

Specifically, the group will coordinate the production and timely issuance of the following interagency products intended for distribution to State, local, and tribal officials, the private sector, as well as the general public when appropriate:

- Alerts, warnings, and notifications of time-sensitive terrorism threats to locations within the United States;
- Situational awareness reporting regarding significant events or activities occurring at the international, national, State, or local levels; and
- Strategic assessments of terrorist risks and threats to the United States.

State and Major Urban Area Fusion Centers

Many State and major urban areas have established information fusion centers to coordinate the gathering, analysis, and dissemination of law enforcement, homeland security, public-safety, and terrorism information. As of September 1, 2007, over 58 of these centers are operating or are being established in States and localities across the country. A majority operate under national guidelines developed through the Global Justice Information Sharing Initiative and Homeland Security Advisory Council. (The full text of the Fusion center Guidelines can be found at www.ise.gov.)

State and major urban area fusion centers are vital assets critical to sharing information related to terrorism. They will serve as the primary focal points within the State and local environment for the receipt and sharing of terrorism-related information. As a part of this *Strategy*, the Federal Government is promoting that State and major urban area fusion centers achieve a baseline level of capability and become interconnected with the Federal government and each other, thereby creating a national, integrated, network of fusion centers to enable the effective sharing of terrorism-related information. The Federal Government will support the establishment of these centers and help sustain them through grant funding, technical assistance, and training to achieve a baseline level of capability and to help ensure compliance with all applicable privacy laws. This approach respects our system of federalism and strengthens our security posture.

Federal departments and agencies will provide terrorism-related information to State, local, and tribal authorities primarily through these fusion centers. Unless specifically prohibited by law, or subject to security classification restrictions, these fusion centers may further customize such information for dissemination to satisfy intra- or inter-State needs. Fusion centers will enable the effective communication of locally generated terrorism-related information to the Federal Government and other fusion centers through the ISE. Locally generated information that is not threat- or incident-related will be gathered, processed, analyzed, and interpreted by those same fusion centers—in coordination with locally based Federal officials—and disseminated to the national level via the DoD, DHS, FBI, or other appropriate Federal agency channels. Where practical, Federal organizations will assign personnel to fusion centers and, to the extent practicable, will strive to integrate and collocate resources.[1]

[1] Appendix 1 delineates the specific roles and responsibilities of Federal, State, local, and tribal governments as they relate to the establishment and continued operation of State and major urban area fusion centers and provides guidelines to support the performance of those roles and responsibilities.

Sharing Information with the Private Sector

As the terrorist attacks on transportation infrastructure in London and Madrid demonstrate, critical infrastructure can be a prime target for the transnational terrorist enemy we face today. The private sector owns and operates an estimated 85% of infrastructure and resources that are critical to our Nation's physical and economic security. It is, therefore, vital to ensure we develop effective and efficient information sharing partnerships with private sector entities. Important sectors of private industry have made significant investments in mechanisms and methodologies to evaluate, assess, and exchange information across regional, market, and security-related communities of interest. This *Strategy* builds on these efforts to adopt an effective framework that ensures a two-way flow of timely and actionable security information between public and private partners.

Efforts to improve information sharing with the private sector have initially focused on sharing with the owners and operators of our Nation's critical infrastructure and key resources. In accordance with the National Infrastructure Protection Plan, we are currently implementing a networked approach to information sharing that allows distribution and access to information both horizontally and vertically using secure networks and coordination mechanisms, allowing information sharing and collaboration within and among sectors. It also enables multidirectional information sharing between government and industry that focuses, streamlines, and reduces redundancy in reporting to the greatest extent possible.

These processes are enabling the integration of private sector security partners, as appropriate, into the intelligence cycle and National Common Operating Picture. Moreover, sector security partners are becoming more confident that the integrity and confidentiality of their sensitive information can and will be protected and that the information sharing process can produce actionable information regarding threats, incidents, vulnerabilities, and potential consequences to critical infrastructure and key resources. These efforts are being integrated into broader efforts to establish the ISE.

It is important to note that critical infrastructure and key resource owners and operators utilize a number of mechanisms that facilitate the flow of information, mitigate obstacles to voluntary information sharing, and provide feedback and continuous improvement regarding structure and process. These include the Sector Coordination Councils, Government Coordination Councils, National Infrastructure Coordinating Center, Sector-level Information Sharing and Analysis Centers (commonly referred to as ISACs), DHS Protective Security Advisors, the DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), and State and major urban area fusion centers. These mechanisms accommodate a broad range of sector cultures, operations, and risk management approaches and recognize the unique policy and legal challenges for full two-way sharing of information between private sector owners and operators and government, as well as the important requirements for efficient operational processes.

Our efforts to improve information sharing with the private sector have been guided by a number of important factors:

- Current, reliable, accurate, and actionable information is critical to private sector decisions to protect their business;
- Private sector entities gather, process, analyze, and share information in order to protect their companies' assets, employees, infrastructure, and ability to operate, so as to maintain a competitive advantage;
- In many cases, private sector entities have spent years establishing strong working relationships with Federal, State, and local law enforcement and other entities; this *Strategy* respects and encourages those established relationships;
- The private sector operates within multiple information sharing frameworks: industry executives often prefer to separately share threat-related information with Federal and State as well as local government officials and other business executives as they assess the threat environment in which they operate, implement protective measures, and engage in emergency response planning activities;
- As we incorporate the information sharing needs and capabilities of the private sector into our efforts to enable information sharing, we need to recognize that at times the environment in which homeland security, law enforcement, and terrorism-related information is shared mirrors the regulatory environment in which the sharing entity operates; and
- The private sector relies on multiple information sources including professional and local organizations, private information providers, news outlets, colleagues, open intelligence sources on the web, and company management in both domestic and foreign locations, in addition to the government at all levels (Federal, State, and local).

Accordingly, as we improve efforts to share terrorism-related information with the private sector we must continue to:

- Build a trusted relationship between Federal, State, local, and tribal officials and private sector representatives to facilitate information sharing;
- Improve the two-way sharing of terrorism-related information on incidents, threats, consequences, and vulnerabilities, including enhancing the quantity and quality of specific, timely, and actionable information provided by the Federal Government to critical infrastructure sectors and their State, local, and tribal partners;
- Ensure that Federal, State, local, and tribal authorities have policies in place that ensure the protection of private sector information that is shared with government entities;
- Integrate private sector analytical efforts into Federal, State, local, and tribal processes, as appropriate, for a more complete understanding of the terrorism risk; and
- Establish mechanisms and processes to ensure compliance with all relevant U.S. laws, including applicable information privacy laws.

We will continue to build upon existing successful information sharing partnerships in a variety of areas key to our national security. Those include programs such as the following:

- The Critical Infrastructure Partnership Advisory Council – provides the framework for owner and operator members of Sector Coordinating Councils and members of Government Coordinating Councils to engage in intra-government and public-private cooperation, information sharing, and engagement across the entire range of critical infrastructure protection activities;
- InfraGard – a partnership between the Federal Government, an association of businesses, academic institutions, State and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States;
- Protected Critical Infrastructure Information/Sensitive Security Information – an information-protection tool that facilitates information sharing between the government and the private sector, which is used by DHS and other Federal, State, and local analysts in pursuit of a more secure homeland, focusing primarily on analyzing and securing critical infrastructure and protected systems, identifying vulnerabilities and developing risk assessments, and enhancing recovery preparedness measures;
- The Overseas Security Advisory Council – a Federal advisory committee that promotes security cooperation between American business and private sector interests worldwide and currently encompasses the 34-member core Council, an Executive Office, over 100 Country Councils, and more than 3,500 constituent member organizations and 372 associates; and
- Existing collaborative information sharing relationships between private sector entities and State and local authorities to facilitate the sharing of time-sensitive threat and vulnerability information, which reflect the preference, in some cases, of private sector entities to coordinate the sharing of threat-related and other information with the government authorities responsible for regulating their activities.

The President also created the National Infrastructure Advisory Council (NIAC). The NIAC is charged to make recommendations on improving the cooperation and partnership between the Federal Government and industry, for the purpose of securing the critical infrastructures. The advice from the NIAC is meant to assist the President and the Secretary of Homeland Security in the development of policies and strategies that range from risk assessment and management to information sharing, protective measure, and clarification on roles and responsibilities between public and private sectors.

Finally, the needs and capabilities of the private sector, particularly those entities considered to be critical infrastructure or key resources, will be incorporated into efforts to establish a national, integrated network of State and major urban area fusion centers and to produce "federally coordinated" terrorism-related information products at NCTC.

Sharing Information with Foreign Partners

Strong and effective cooperation with our foreign partners is a vital component of the global war on terrorism. The President recognized the need to share information with foreign partners in his December 16, 2005, Memorandum to the Heads of Executive Departments and Agencies. Accordingly, the sharing of terrorism-related information between Federal departments and agencies and foreign partners and allies forms a critical component of our information sharing strategy.

The counterterrorism mission requires sharing many types of terrorism-related information, for example, the exchange of biographic and biometric information related to known or suspected terrorists. While such sharing often includes classified information and sensitive diplomatic, law enforcement, and homeland security information relating to terrorism, it also encompasses other information that, over time, may help reveal links to terrorist groups or individuals. Information regarding lost or stolen passports and suspect financial transactions, for example, might yield information on groups or persons who subsequently are linked to a specific terrorist threat. In addition to asking for such information from other countries, it is also essential that we appropriately share similar types of information with foreign governments or foreign law enforcement entities, such as INTERPOL, as long as the sharing of any records about American citizens and lawful permanent residents data is subject to the *Privacy Act of 1974* limitations, especially regarding personally identifiable information.

Information sharing with foreign partners is a key component of international outreach and cooperation to protect U.S. critical infrastructure. Given the often sensitive nature of the information shared, we will continue to enter into agreements and other understandings with foreign governments to ensure appropriate security and confidentiality of exchanged information. We must also expect that foreign governments will seek the same assurances from us. As a general rule, such agreements and understandings should seek sufficient security of information while also permitting flexible handling of the exchanged information to allow practical use. We must strive to ensure that safeguarding and handling restrictions are calibrated to maximize both the quantity and quality of information shared with, or received from, a foreign government. To the maximum extent possible, we will adopt and adhere to commonly accepted and standard safeguarding and handling restrictions.

There is the basic requirement that shared information be appropriately safeguarded and protected from public disclosure. Our foreign partners at times may ask us to agree to particular restrictions on the dissemination or use of the information. While it is preferable to avoid such restrictions, it may be necessary in certain circumstances to accept some limitations as a condition for receiving information with particularly high value. How we proceed in such situations will depend on the circumstances presented and our need for the information at issue. Our guiding objective will be to ensure that information received from a foreign government can be disseminated as broadly as possible and used for critical counterterrorism purposes.

Similar challenges arise in regard to sharing information with foreign governments that may contain personal data about United States citizens and permanent residents. In particular, the *Privacy Act of 1974* confers certain protections upon information concerning citizens and lawful permanent residents. Accordingly and especially given considerations of reciprocity, we must remain sensitive to the potential impact on our citizens and lawful residents of sharing information involving U.S. persons with foreign partners. The United States must carry out its counterterrorism mission while also ensuring that appropriate protection of information regarding our citizens and lawful permanent residents. As part of approving the recommendations submitted to improve information sharing with foreign governments, the President directed that the potential impact on United States persons be considered when evaluating a proposed information sharing arrangement with a foreign government.

Special considerations present themselves in the area of sharing classified information with foreign governments. Such sharing will continue to occur in a relatively formal context, to account for the need to properly secure and limit disclosure of the information. Indeed, decisions of whether to share our Nation's classified information are extraordinarily sensitive and will be made with the utmost care. Our officials must remain cognizant of the imperative to our national security mission of maximizing the sharing of terrorism-related information, while also taking care to ensure that sharing arrangements do not result in the unintended compromising of our national security.

In summary, strong partnerships and trusted collaboration with foreign governments are essential components of the war on terror. Effective and substantial cooperation with our foreign partners requires sustained liaison efforts, timeliness, flexibility, and the mutually beneficial exchange of many forms of terrorism-related information. The strategic objectives for sharing information with foreign partners can be broadly summarized as follows:

- Expanding and facilitating the appropriate and timely sharing of terrorism-related information between the United States and our foreign partners;
- Ensuring that exchanges of information between the United States and foreign governments are accompanied by proper and carefully calibrated security requirements;
- Ensuring that information received by Federal agencies from a foreign government under a sharing arrangement: (1) is provided to appropriate subject matter experts for interpretation, evaluation, and analysis; and (2) can be disseminated and used to advance our Nation's counterterrorism objectives;
- Refining and drawing upon sets of best practices and common standards in negotiating sharing arrangements with foreign governments; and
- Developing standards and practices to verify that sharing arrangements with foreign governments appropriately consider and protect the information privacy and other legal rights of Americans.

Protecting Privacy and Other Legal Rights in the Sharing of Information

Protecting the rights of Americans is a core facet of our information sharing efforts. While we must zealously protect our Nation from the real and continuing threat of terrorist attacks, we must just as zealously protect the information privacy rights and other legal rights of Americans. With proper planning we can have both enhanced privacy protections and increased information sharing – and in fact, we must achieve this balance at all levels of government, in order to maintain the trust of the American people. The President reaffirmed this in his December 16, 2005, Memorandum to the Heads of Executive Departments and Agencies.

At the direction of the President, the Attorney General and the Director of National Intelligence developed a set of Privacy Guidelines to ensure the information privacy and other legal rights of Americans are protected in the development and use of the ISE. The Privacy Guidelines provide a consistent framework for identifying information that is subject to privacy protection, assessing applicable privacy rules, implementing appropriate protections, and ensuring compliance. An array of laws, directives, and policies provide substantive privacy protections for personally identifiable information. The parameters of those protections vary depending on the rules that apply to particular agencies and the information they are proposing to share. As described below, however, the Guidelines demand more than mere compliance with the laws; they require executive departments and agencies to take pro-active and explicit actions to ensure the balance between information privacy and security is maintained, as called for by the *National Commission on Terrorist Attacks Upon the United States*. The full text of the ISE Privacy Guidelines can be found at www.ise.gov.

Core Privacy Principles

The Privacy Guidelines build on a set of core principles that Federal departments and agencies must follow. Those principles require specific, uniform action and reflect basic privacy protections and best practices. Agencies must:

- Share protected information only to the extent it is terrorism information, homeland security information, or law enforcement information related to terrorism;
- Identify and review the protected information to be shared within the ISE;
- Enable ISE participants to determine the nature of the protected information to be shared and its legal restrictions (e.g., "this record contains individually identifiable information about a U.S. citizen");
- Assess, document, and comply with all applicable laws and policies;
- Establish data accuracy, quality, and retention procedures;
- Deploy adequate security measures to safeguard protected information;

- Implement adequate accountability, enforcement, and audit mechanisms to verify compliance;
- Establish a redress process consistent with legal authorities and mission requirements;
- Implement the guidelines through appropriate changes to business processes and systems, training, and technology;
- Make the public aware of the agency's policies and procedures as appropriate;
- Ensure agencies disclose protected information to non-Federal entities—including State, local, tribal, and foreign governments—only if the non-Federal entities provide comparable protections; and
- State, local, and tribal governments are required to designate a senior official accountable for implementation.

Privacy Governance

Successful implementation of the Privacy Guidelines requires a governance structure to monitor compliance and to revise the Guidelines as we gain more experience. The President, therefore, directed the Program Manager to establish the ISE Privacy Guidelines Committee. The Committee is chaired by representatives of the Attorney General and the Director of National Intelligence, and consists of the Privacy Officials of the departments and agencies of the Information Sharing Council. The Committee seeks to ensure consistency and standardization, as well as serve as a forum to share best practices and resolve agency concerns.

Institutionalizing the Strategy for Long-Term Success

Over the past six years we have made significant improvements in the way that terrorism-related information is shared. There remains more we can and must do to ensure that those responsible for protecting our people, interests, and infrastructure have the information they need to carry out their mission. Individual departments and agencies of the Federal Government have been directed to work together to ensure that Federal information and intelligence capabilities are brought together to form a national assured information sharing capability. These same individual departments and agencies have been directed to work together to ensure that State and major urban area fusion centers are interlinked with each other and Federal information and intelligence capabilities to form a national information sharing capability. This *Strategy* provides the vision of how we will build upon the progress of the past six years and establish an integrated information sharing capability to ensure that those who need information to protect our Nation from terrorism receive it and that those who have information share it.

The preceding sections of this *Strategy* described the four areas of information sharing and the overarching need to ensure that our efforts to expand the sharing of terrorism-related information are accompanied by adequate protections for information privacy rights and other rights guaranteed by the Constitution and laws of the United States. The challenge is to ensure that those areas, and the guiding principles on which they are based, are incorporated in a framework of specific, measurable activities that guide the development and implementation of the ISE and increase the sharing of terrorism-related information across the Federal Government and with State, local, tribal, and private sector entities and our foreign partners.

Ultimately, implementing this *Strategy* will create a powerful national capability to share, search, and analyze terrorism-related information that spans jurisdictional, organizational, and cultural boundaries and provides users a distributed, secure, and trusted environment for transforming data into actionable information. It also takes advantage of the vital roles played by State and major urban area information fusion centers, which are crucial investments for improving the nation's analytical capacity.

This *Strategy* is being institutionalized through many actions including the following:

The ISE Implementation Plan Report – In November 2006, the Director of National Intelligence produced and provided to the Congress a report containing an Implementation Plan for the ISE that outlines almost 100 specific actions and supporting recommendations for achieving the goals for the ISE, as envisioned in the *Intelligence Reform and Terrorism Prevention Act of 2004* and in Executive Order 13388.

This plan reflects the culmination of collaboration between the Program Manager, the Information Sharing Council, and Federal departments and agencies. It also incorporates the perspectives of representatives from State, local, and tribal governments who reviewed the ISE Implementation Plan Report during its development.

Sharing with State, Local, and Tribal Governments and the Private Sector

The Interagency Threat Assessment and Coordination Group – The Administration established an Interagency Threat Assessment and Coordination Group at the national level to better coordinate the sharing of terrorism-related information. The Group will facilitate the production of what will be officially defined as "federally coordinated" terrorism-related information products intended for dissemination to State, local, and tribal officials and private sector partners through the established channels. As noted previously, the Group will include representatives from DHS, FBI, and other relevant Federal entities as well as State and local government representatives. The Group will ensure that both classified and unclassified intelligence produced by Federal entities within the intelligence, law enforcement, and homeland security communities is fused, validated, de-conflicted, and approved for dissemination in a concise and, when possible, unclassified format.

State and Major Urban Area Fusion Centers – We will improve collaboration at the State and local levels by leveraging State and major urban area information fusion centers and by establishing a national integrated network of these centers. Appendix 1 delineates the specific roles and responsibilities of State and major urban area fusion centers.

Collocation of personnel from State and major urban area fusion centers and local JTTFs, Field Intelligence Groups, and National Guard intelligence units is also encouraged.

Through the Federal grants process and related technical assistance and training efforts, the Federal Government is working to ensure that these centers achieve and maintain a baseline level of operational and analytical capability by encouraging the adoption of the Global Justice Information Sharing Initiative/Homeland Security Advisory Council Fusion Guidelines and by expanding the amount of technical assistance and training provided.

Sharing with Our Foreign Partners and Allies

Standard International Agreement Text – We are developing standard language on information sharing and protection that can be used in international agreements pertaining to terrorism-related information sharing to facilitate agreement on a level of protection that would not unnecessarily impede re-dissemination for counterterrorism purposes.

Central Repository – We are establishing a central, electronically accessible repository of information on foreign government and international organization marking and handling regimes so that U.S. agencies and domestic partners can more readily understand safeguarding and handling rules for different kinds of foreign government information.

Protecting the Information Privacy and Legal Rights of Americans

ISE Privacy Guidelines – The ISE Privacy Guidelines are designed to establish a framework for sharing terrorism-related information in the ISE in a manner that protects privacy and civil liberties. These guidelines require agencies to identify any privacy-protected information to be shared and they put in place accountability mechanisms, audit mechanisms, and redress procedures.

ISE Privacy Officials – The Guidelines require Federal departments and agencies to designate an "ISE Privacy Official" to directly oversee implementation of the Guidelines.

ISE Privacy Guidelines Committee – The Guidelines also provide for an ISE Privacy Guidelines Committee, consisting of the ISE Privacy Officials of the Federal departments and agencies that are members of the Information Sharing Council, and chaired by a senior official designated by the Program Manager of the ISE.

Appendix 1
Establishing a National Integrated Network of State and Major Urban Area Fusion Centers

Roles and Responsibilities of Federal, State, Local, and Tribal Authorities

Roles of the State and Major Urban Area Fusion Centers

Federal, State, local, and tribal governments have specific responsibilities as it relates to the establishment and continued operation of State and major urban area fusion centers. The roles and responsibilities outlined in this *Strategy* were developed in partnership with State, local, and tribal officials and represent a collective (Federal, State, local, and tribal) view. This *Strategy* recognizes the sovereignty of State and local governments, and thus the roles and responsibilities are delineated with the understanding that State and major urban area fusion centers are owned and managed by State and local governments. Furthermore their incorporation into the ISE takes into account that these centers support day-to-day crime control efforts and other critical public safety activities. Interlinking and networking these centers will create a national capacity to gather, process, analyze, and share information. Incorporating these centers into the ISE will be done in a manner that protects the information privacy and other legal rights of Americans and corporations, as provided for under U.S. law.

The Federal Government may need to provide financial and technical assistance, as well as human resource support, to these fusion centers if they are to achieve and sustain a baseline level of capability. The objective is to assist State and local governments in the establishment and the sustained operation of these fusion centers. A sustained Federal partnership with State and major urban area fusion centers is critical to the safety of our Nation, and therefore a national priority.

State and major urban area fusion centers will be the focus, but not exclusive points, within the State and local environment for the receipt and sharing of terrorism information, homeland security information, and law enforcement information related to terrorism. These fusion centers support the efforts of State, local, and tribal entities in undertaking the following activities and responsibilities, in appropriate consultation or coordination with Federal departments and agencies:

- Share classified and unclassified information to address domestic security and criminal investigations with other States, localities, regions and the Federal Government in a manner that protects the information privacy and other legal rights of Americans, while ensuring the security of the information shared.
- Foster a culture that recognizes the importance of fusing "all crimes with national security implications" and "all hazards" information (e.g., criminal investigations, terrorism, public health and safety, and emergency response) which often involves identifying criminal activity and other information that might be a precursor to a terrorist plot.

- Support critical counterterrorism, homeland security, and homeland defense-related activities, including but not limited to the development or maintenance of:
    1. Mechanisms to contribute information of value to ongoing Federal terrorism risk assessments;
    2. Statewide, regional, site specific, and topical risk assessments;
    3. Processes in support of information responsive to federally communicated requirements and tasks;
    4. Alerts, warnings, notifications, advisories, and/or bulletins regarding time sensitive or strategic threats;
    5. Situational awareness reports; and
    6. Analytical reports regarding geographically relevant incidents or specific threats.
- Develop, in coordination with Federal authorities, critical infrastructure protection plans to ensure the security and resilience of infrastructure operations (e.g., electric power, transportation, telecommunications, water) within a region, State, or locality. The efforts of State and major urban area fusion centers in this regard will be coordinated with information sharing activities delineated in the National Infrastructure Protection Plan as well as other efforts already underway by DoD, DHS, FBI, and other Federal entities.
- Prioritize emergency management, response, and recovery planning activities based on likely threat scenarios and at-risk targets.
- Provide assessments of risk that support State and urban area homeland security preparedness planning efforts to allocate funding, capabilities, and other resources.
- Provide risk-related information to support efforts to develop training, awareness, and exercise programs to ensure that State, local, and tribal officials are prepared to deal with terrorist strategies, tactics, capabilities, and intentions and to test plans for preventing, preparing for, mitigating the effects of, and responding to events.
- Further customize federally supplied information for dissemination to meet intra- or inter-State needs, unless specifically prohibited or otherwise subject to additional security restrictions.
- Ensure that all locally generated terrorism-related information—including suspicious activity and incident reports—is communicated to the Federal Government and other States, localities, and regions, through the appropriate mechanism and systems. Locally generated information that does not appear to be threat or incident related will be gathered, processed, analyzed, and interpreted by the same State and major urban area fusion centers in coordination with locally-based Federal officials. The same information will be disseminated to the national level via appropriate Federal agencies.

Federal, State, Local, and Tribal Responsibilities

I. General

Federal Responsibilities

The Federal Government, in coordination with State, local, and tribal officials, will establish a working group of the Information Sharing Council, to coordinate Federal efforts to support the creation of a national network of State and major urban area fusion centers. Drawing upon existing and ongoing efforts at the Federal level, DoD, DOJ, DHS, the Office of the Director of National Intelligence, and National Guard Bureau shall establish a coordinated set of policies, protocols, and procedures to:

1. Develop, maintain and, as appropriate, disseminate an assessment of terrorist risks and threats to the United States and it interests.
2. Use risk and threat assessments to identify and gather information responsive to the identified threats and risks.
3. Gather and document the information needs of State, local, and tribal governments.
4. Continue to develop a prioritized listing of informational products needed by State, local, and tribal governments based on terrorism information requirements.
5. Maintain existing analytical resources capable of producing (researching, developing, drafting and packaging) these analytical products and coordinating both their development and dissemination.
6. Identify any gaps in production capabilities as it relates to the production of: alerts, warning and notifications regarding time sensitive threat, situational awareness reporting regarding significant events, strategic assessments of threats posed by individuals or terrorist organizations, tradecraft utilized by organizations, geographic risk assessments, or other related issues.
7. Mitigate production gaps by leveraging existing departmental, agency, or NCTC analytical capabilities.
8. Maintain the capability to produce and coordinate multi-channel dissemination of inter-agency coordinated alerts, warnings, and notifications of time sensitive terrorism-related information.
9. Support State, local, and tribal efforts to produce State, regional, and site-specific risk assessments by adopting common terminology and criteria and providing State and local officials an agreed upon assessment methodology for evaluating risk (threat, consequence, and vulnerability).
10. Coordinate the assignment of representative personnel to State and major urban area fusion centers and otherwise strive to integrate and, to the extent practicable, collocate resources.

11. Ensure the sharing of information is done in a manner that protects the information privacy and legal rights of Americans.

State, Local, and Tribal Responsibilities

Each State will be encouraged to define and document how it intends to carry out intrastate efforts to gather, process, analyze, and disseminate terrorism information, homeland security information, and law enforcement information. This process is commonly known as the "fusion process." Defining this process should include the following:

1. In those States where there exist multiple fusion centers, one fusion center, with the demonstrated capacity to serve as the statewide center or hub, should be designated as the primary interface with the Federal Government. This statewide fusion center should also coordinate the gathering, processing, analysis, and dissemination of homeland security information, terrorism information, and law enforcement information on a statewide basis.
2. The Executive Agent of each Urban Area Security Initiative (UASI), as well as the applicable State's homeland security advisor, must work together to determine the most effective manner in which to incorporate the UASI into the statewide information sharing framework.
3. In those instances in which the UASI has established a regional fusion center, the activities of the major urban area fusion center should be incorporated into the statewide fusion process.
4. Each State and major urban area fusion center is encouraged to coordinate with the appropriate Federal authorities to develop synchronized protocols for sharing information with the private sector.

II. Achieving and Sustaining Baseline Operational Standards for State and Major Urban Area Fusion Centers

Federal Responsibilities

The Federal Government, working in partnership with State, local, and tribal authorities, will seek to define the current national information sharing capability that exists through the existence of existing State and major urban area fusion centers. State and local authorities will be asked to support these efforts by assessing and documenting the baseline level of capability of their existing fusion centers.

The Federal Government, in consultation with State, local, and tribal authorities, shall compile, document, and disseminate baseline operational standards, the achievement of which will determine whether an individual State or major urban area fusion center is considered to have achieved a baseline level of capability. These baseline operational standards will build on the Global Justice Fusion Center Guidelines. Additionally, the Federal Government will initiate a series of activities to assist State and major urban area fusion centers to adopt and incorporate these baseline operational standards into their business operations. These standards will support the gathering, processing, analysis, and dissemination of terrorism information, homeland security information, and law enforcement information. Specific Federal activities include:

1. Defining, documenting, and disseminating the baseline operational standards.
2. Assessing the existing level of capability of each designated State and major urban area fusion center.
3. Providing technical assistance, training, and other support as needed by these fusion centers to support their achieving the defined baseline level of capability.
4. Amending relevant grants guidance and technical assistance to ensure that fusion center grant recipients, as a condition of receiving funding, meet delineated baseline operational standards.
5. Modifying grants, other applicable funding programs, and related technical assistance programs to support efforts to sustain the capacity of State and major area fusion centers to operate at a baseline operational level once achieved.
6. Establishing a best practices clearing house capability for fusion centers to include creating a list of Subject Matter Experts.
7. Developing a coordinated interagency approach that supports, wherever practical, the assignment of Federal personnel to State and major urban area fusion centers and otherwise strive to integrate and, to the extent practicable, collocate resources.

State, Local, and Tribal Responsibilities

State, local, and tribal authorities are encouraged to take the following steps to ensure that State and major urban area fusion centers achieve and sustain a baseline level of capability:

1. Support efforts to complete an assessment of existing capabilities within designated State and major urban area fusion centers.
2. Identify and document capability gaps (if any) and develop a strategy and investment plan to mitigate any capability gaps.
3. Track and report efforts to mitigate any capability gaps.
4. Develop an investment strategy to sustain fusion center operations, including a delineation of current and recommended future Federal versus non-Federal costs.
5. Document and report a strategy for integrating State and major urban area fusion center efforts with those of other Federal, State, local, tribal, and private sector information sharing and counterterrorism efforts.

III. Suspicious Activities and Incident Reporting

Federal Responsibilities

The Federal Government will develop a plan and provide State and major urban area fusion centers a mechanism to gather and report locally generated information to appropriate Federal entities, other States, and localities. This locally generated information will include reports by the public or governmental personnel regarding suspicious incidents, events, and activities. Specific activities include:

1. Providing reports and awareness training to State, local, and tribal authorities regarding the strategic goals, operational capabilities, and methods of operation utilized by international and domestic terrorist organizations so that local events and behaviors can be viewed within the context of potential terrorist threats.
2. Developing a prioritized listing of the specific types of locally generated information of interest to Federal entities responsible for assessing the national threat environment and which supports the rapid identification of emerging terrorist threats.
3. Identifying resources capable of communicating and updating these information requirements to State, local, and tribal officials via State and major urban area fusion centers.
4. Establishing a unified process to support the reporting, tracking, processing, storage, and retrieval of locally generated information.
5. Ensuring that efforts to gather, process, analyze, and store locally generated information are carried out in a manner that protects the privacy and legal rights of Americans.

State, Local, and Tribal Responsibilities

State and major urban area fusion centers will support the gathering of locally generated terrorism information, homeland security information, and law enforcement information related to terrorism. Specific activities may include:

1. Completion of a statewide and/or regional risk assessment (threat, vulnerability, and consequence).
2. Using this assessment to identify priority information requirements.
3. Identification of data sources and repositories of prioritized information.
4. Maintaining an information gathering and reporting strategy utilizing existing local capabilities.
5. Developing, implementing, and maintaining a method for communicating information priorities to local gatherers of information.
6. Ensuring that the processes and protocols for ensuring that priority information, including Suspicious Incident Reports (SIRs) and Suspicious Activities Reports (SARs), are disseminated to and evaluated by appropriate government authorities and appropriate critical infrastructure owners and operators.
7. Ensuring that the processes and protocols for ensuring that priority information, including SIRs and SARs, are reported to national entities to support its inclusion into national patterns and trends analysis and other States and localities to support regional trends analysis.
8. Identifying system requirements that support a unified process for reporting, tracking, and accessing SIRs and SARs.
9. Defining a feedback mechanism.

IV. Alerts, Warnings, and Notifications

Federal Responsibilities

The Federal Government, in coordination with State, local, and tribal authorities, will establish processes to manage the issuance of alerts, warnings, and notifications to State and major area fusion centers regarding time sensitive threats and other information requiring some type of State and/or local reaction or response. Specific activities include:

1. Documenting the types of informational products needed by State, local, and tribal governments and the format in which they are desired.
2. Identifying the Federal entities responsible for producing (researching, developing, drafting, and packaging) alerts, warning, and notifications for dissemination to State and major area fusion centers regarding time sensitive threats and coordinating both their development and dissemination.
3. Identifying any gaps in production capabilities as it relates to the production of: alerts, warnings, and notifications regarding time sensitive threats or other related issues.
4. Maintaining the capability to mitigate production gaps by leveraging existing departmental, agency, or NCTC analytical capabilities.

5. Coordinating inter-agency production and multi-channel dissemination of "federally coordinated" alerts, warnings, and notifications of time sensitive threats through the efforts of the Interagency Threat Assessment and Coordination Group.
6. Providing a communications platform, where needed, to transmit alerts, warnings, or notifications, and ultimately consolidating such communications platforms as agreed to through collaborative Federal, State, and local planning and deliberation.

State and Local Responsibilities

State and major urban area fusion centers are encouraged to ensure that alert notifications are disseminated as appropriate, to State, local, and tribal authorities, the private sector and the general public. Specific activities may include:

1. Implement a protocol to govern the receipt of federally generated threat, warning, and notification messages.
2. Develop and/or maintain a plan (processes, protocols, and communication methodology) to govern the further dissemination of federally generated threat, warning, and notification messages, bulletins and other information products to State, local, and tribal authorities, the private sector and the general public.
3. Develop and/or maintain a plan (processes, protocols, and communication methodology) to govern the gathering, processing, and reporting to Federal entities any actions taken by State, local, and tribal authorities and the private sector in response to federally generated threat, warning, and notification messages.
4. Identify and establish a communications platform to support the dissemination of these messages and information products.
5. Coordinate with the appropriate Federal authorities to develop synchronized protocols for sharing information with the private sector.

V. Situational Awareness Reporting

Federal Responsibilities

The Federal Government, in coordination with State, local, and tribal authorities, will establish processes to manage the reporting to key officials and the public information regarding significant events (local, regional, national, and international) that may influence statewide or local security conditions, which include:

1. Documenting the types of informational products needed by State, local, and tribal governments and the format in which they are desired.
2. Identify existing resources capable of producing (researching, developing, drafting, and packaging) these situational reports and coordinating both their development and dissemination.
3. Identify any gaps in production capabilities as it relates to the production of situational awareness reporting regarding significant events.

4. Maintain the capability to mitigate production gaps by leveraging existing departmental, agency, or NCTC analytical capabilities to produce terrorism-related situational reports.
5. Coordinate inter-agency production and multi-channel dissemination of "federally coordinated" situational awareness reports through the efforts of the Interagency Threat Assessment and Coordination Group.
6. Identifying and establishing a communications platform to support the dissemination of such reporting.

State and Local Responsibilities

State and major urban area fusion centers are encouraged to develop the processes to manage the reporting to key officials and the public information regarding significant events (local, regional, national, and international) that may influence State or local security conditions. Such actions may include:

1. Establishing and/or maintaining a protocol to govern the receipt of federally generated situational awareness reports.
2. Establishing and/or maintaining a plan (processes, protocols, and communication methodology) to govern the further dissemination of Federal situational awareness reports and those resulting from media reports to State, local, and tribal authorities, the private sector, and the general public.
3. Establishing and/or maintaining a plan (processes, protocols, and communication methodology) to govern the gathering, processing, and reporting to Federal entities any actions taken by State, local, and tribal authorities and the private sector in response to significant events.
4. Establishing and/or maintaining a protocol to govern the timely reporting of significant events occurring within State or local jurisdictions to Federal authorities and, when appropriate, other States, localities, and regional entities.
5. Coordinating with the appropriate Federal authorities to develop synchronized protocols for sharing information with the private sector.

INFORMATION SHARING ENVIRONMENT (ISE)-SUSPICIOUS ACTIVITY REPORTING (SAR) EVALUATION ENVIRONMENT IMPLEMENTATION GUIDE*

Version 1.0

January 9, 2009

* This document was previously known as the *Concept of Operations and Implementation Overview for the State and Local Law Enforcement Information Sharing Environment (ISE)-Suspicious Activity Reporting (SAR) Shared Space, Version 1.4.*

ISE-SAR Evaluation Environment Implementation Guide

1 Introduction

1.1 Overview of ISE-SAR Evaluation Environment

The purpose of the ISE-SAR Evaluation Environment (EE) is to develop a learning environment in which the process of gathering and reporting suspicious activity can be evaluated nationally to develop patterns of criminal activity with a nexus to terrorism. This evaluation environment will allow for modifications and improvements to be made with the goal of establishing an end-to-end process for reporting suspicious activity at the national level. Gathering information and reporting suspicious activity are not new concepts for law enforcement agencies. The ISE-SAR EE focuses on what law enforcement agencies have always done—gathering information—and establishes a process whereby information can be shared to detect and prevent criminal and terrorist activity. This Implementation Guide is intended to assist participating state and local law enforcement agencies with the implementation of the ISE-SAR Shared Spaces and aid them in understanding the procedures and processes within the ISE-SAR EE.

History

On October 31, 2007, President Bush issued the first *National Strategy for Information Sharing* (NSIS) to reinforce, prioritize, and unify our nation's efforts to advance the sharing of terrorism-related information among federal, state, and local government entities; the private sector; and foreign partners. The NSIS calls for, among other things, 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 and local governments and across the federal government. Consistent with the NSIS and as a priority for the establishment of the Information Sharing Environment (ISE), the Office of the Program Manager for the Information Sharing Environment (PM-ISE), the U.S. Department of Justice, the U.S. Department of Homeland Security, and the Office of the Director of National Intelligence have coordinated a comprehensive effort to develop a nationwide network of state and major urban area fusion centers that will facilitate the sharing of terrorism-related information across the federal, state, and local communities. The NSIS reiterates the need to collect SAR data and supports the ongoing activities being performed at the federal, state, and local levels. This project will attempt to formulate and enhance existing SAR efforts. The *Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.0* (ISE-SAR Functional Standard)[1] began development in the fall of 2006 and was issued in January 2008 by the PM-ISE to specifically address the sharing of ISE-SARs, with the overarching goal of enabling law enforcement analysts and officers with counterterrorism responsibilities at all levels of government to discover and identify terrorist activities and trends.

The term "suspicious activity report" does not refer to a particular form or type of document. Rather, it describes any official document in which a suspicious activity or incident is recorded by an organization participating in the ISE. In the course of conducting their missions or for the protection of their personnel and facilities, many federal, state, and local law enforcement agencies document suspicious activities observed or reported. This practice is well institutionalized in the law enforcement community and occurs with varying degrees of standardization and formality in other communities. Information collected generally falls into one of four categories—criminal incident, information (general data such as computer-aided

[1] See http://www.ctisr.net/web.

dispatch and management information), criminal intelligence, or criminal investigative. Some, but by no means all, of these records document activities with a potential nexus to terrorism. The main purpose of this evaluation environment is to demonstrate and evaluate the standardization process. Accordingly and consistent with the direction in the NSIS, it was deemed necessary to establish a standardized process that includes flexibility to meet the unique individual requirements of the jurisdiction in the area of privacy protection and associated data models for identifying, documenting, and sharing terrorism-related SARs to the maximum extent possible.

Summary of the ISE-SAR Process

The ISE-SAR Functional Standard Version 1.0 sets forth a two-part "integration/consolidation" process for identifying, out of the thousands of possible types of suspicious activities documented each day through "organizational processing," those activities conducted by source agencies that have a potential nexus to terrorism.[2] The activity must meet one or more of the criteria set forth in Part B of the ISE-SAR Functional Standard.[3] These criteria describe types of suspicious activities identified by counterterrorism experts as being indicative of or associated with terrorist activity. The ISE-SAR process provides for human review and vetting to ensure that information is both legally obtained and determined to have a potential terrorism nexus.

Law enforcement officers will be trained to recognize those behaviors and incidents that are indicative precursors to criminal activity related to terrorism. The process includes safeguards to ensure to the greatest degree possible that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared. These safeguards are intended to ensure that information which violates civil rights and civil liberties (e.g., information about race, ethnicity, national origin, or religious preference that has no reasonable relation to the criminal activity) will not be intentionally or inadvertently gathered, documented, processed, or shared. The process involves multiple steps carried out by trained law enforcement personnel, including identification of observable behaviors and incidents by trained personnel during their routine activity, review of the report by a first-line supervisor or other designated staff, and review by a trained expert to identify a SAR as terrorism-related. Information determined to have a potential nexus to terrorism will be documented in the format described in the standard and shared with all appropriate ISE participants. Exigent circumstances will require the SAR to be referred to the Joint Terrorism Task Force (JTTF).

Incremental steps are being taken to implement and institutionalize the flow of information in the manner described in the ISE-SAR Functional Standard at the individual organizational levels (Appendix D illustrates a functional flow of SAR information in the ISE). To facilitate this, ISE-SARs may be made available in one of two different formats (information exchange packages). The detailed format includes information contained in all 189 data fields set forth in Section IV of the ISE-SAR Functional Standard ("ISE-SAR Exchange Data Model"), to *include* those fields denoted as containing privacy information, also denoted as "privacy fields" in the Functional Standard. The summary format provides a subset of the detailed format, *excluding* 19 of the 189 privacy fields or data elements identified as containing personal information.[4] The ISE-SAR Functional Standard identifies the minimum data elements that must be excluded from

[2] An objective of the evaluation environments is to evaluate and adjust these criteria if needed.

[3] See http://www.ise.gov/docs/ctiss/ISE-FS-200SARFunctionalStandardIssuanceVersion1.0.pdf, p. 6.

[4] Since both detailed and summary formats contain the contact information of the submitting organization, recipients of the summary format can contact the submitting organization for additional information, as appropriate.

a summary ISE-SAR. Each ISE participant may exclude additional data elements from its summary ISE-SARs in accordance with its own statutory or policy requirements. By conducting this evaluation project, the Information Sharing Environment will gain a better perspective on:

- Which fields are captured.
- Which fields provide value.
- What can be done to ensure that ISE-SAR information is captured in a standardized manner across the country.

The goal of this project and the SAR process is to share detailed ISE-SARs, to the maximum extent possible, among federal, state, and local law enforcement agencies; homeland security; and other appropriate organizations participating in the ISE, recognizing that personal identifiers may not be available to all ISE participants. In this way, summary ISE-SARs can be made available to all ISE participant organizations with counterterrorism responsibilities.

Implementation of the ISE-SAR Functional Standard

The ISE-SAR Functional Standard is not intended to address all business rules, system requirements, or other details governing designation, documentation, and sharing of ISE-SARs across all five communities of the ISE.[5] The ISE-SAR Functional Standard is intended to build upon, consolidate, and standardize nationwide aspects of those ISE-relevant activities already occurring at the federal, state, and local levels with respect to the processing, sharing, and use of suspicious activity information. Entities such as JTTFs and state, regional, and major urban area fusion centers have established procedures for processing and sharing information (to include suspicious activity information) with local entities. Given the diversity of organizations involved with processing, sharing, and using suspicious activity information and the varied legal and policy requirements that apply to such activities, intraorganizational business rules governing implementation of the ISE-SAR Functional Standard will be developed by the participating organizations. Such business rules may provide detail on the further vetting of ISE-SARs, recipients' secondary dissemination of ISE-SARs, standards for auditing the use of ISE-SARs, notification of inaccuracies to the source and submitting organizations, and feedback on the usefulness of the information (The source agency/organization is defined as the entity that submits information to the fusion center, and the submitting agency/organization is the agency/fusion center that enters the data into the ISE-SAR Shared Spaces). The source and submitting agency/organization may be the same. Any additional rules for the sharing of ISE-SARs will build upon the participating organizations' existing policies and procedures and will incorporate all applicable legal requirements, including state laws and policies and local ordinances, and may become part of the next functional standards. All ISE-SAR business rules, whether generated locally or issued by the PM-ISE, must be consistent with the ISE Privacy Guidelines, *Privacy and Civil Liberties Implementation Guide and Implementation Templates, Privacy Guidelines Implementation Manual*, and the ISE-SAR Functional Standard.

Based on the *Findings and Recommendations of the SAR Support and Implementation Project*,[6] "local law enforcement entities should incorporate the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process)

[5] The five ISE communities are defense, foreign affairs, homeland security, intelligence, and law enforcement. *Information Sharing Environment Enterprise Architecture Framework*, Program Manager, Information Sharing Environment, August 2007, p. 6.

[6] In June 2008, the *Findings and Recommendations of the SAR Support and Implementation Project* (SAR Report) was developed to provide recommendations to the Criminal Intelligence Coordinating Council (CICC) from the Major Cities Chiefs Association. At the September 2008 meeting, the CICC unanimously passed the SAR Report.

into existing processes and systems used to manage other crime-related information and criminal intelligence so as to leverage existing policies and protocols utilized to protect the information, privacy, civil liberties, and other legal rights of the general public. See Section 3.2, Privacy and Civil Liberties Protection, for ISE-SARs privacy policy guidance.

Business rules for collecting, documenting, processing, and sharing terrorism-related suspicious activity information (the activity that takes place at the first, second, and third steps of the Information Flow Description contained in the ISE-SAR Functional Standard) are currently being developed and reviewed in several major cities and jurisdictions across the country. This effort is part of a PM-ISE-funded effort in collaboration with the Major Cities Chiefs Association (MCCA), the International Association of Chiefs of Police (IACP), the U.S. Department of Homeland Security, the Global Justice Information Sharing Initiative (Global), the Criminal Intelligence Coordinating Council (CICC), the U.S. Department of Defense, and the Bureau of Justice Assistance (BJA). These project partners reviewed the SAR business rules of four major police departments and a host of other major police agencies. They developed recommended guidelines for implementing a SAR process and identified best practices/business rules that can be leveraged across the law enforcement community.

Systems for Sharing SARs Among Participants

Section 1016(b)(2) of the Intelligence Reform and Terrorism Prevention Act of 2004, as amended, directs that the sharing of protected information through the ISE be done in a manner that leverages existing systems. At the present time, there is no single system or database that is used by or is available to all ISE participant agencies for sharing ISE-SARs.

The ISE-SAR Shared Spaces concept and environment described in the ISE Enterprise Architecture Framework (EAF) ultimately envisions the establishment of an ISE-wide system of attribute-based controls that would manage access authorization based on the mission and function of the ISE participant requesting access. Under such a federated system, it would be possible, for example, to grant full access to one set of users and partial access to another set of users based on credentialing levels. As more ISE-SAR Shared Spaces become operational and the standardized access rules and requirements for the shared spaces are issued, information sharing within the ISE will become more efficient. For example, once access, system certification, and accreditation rules are standardized and applied to ISE-SAR Shared Spaces that support connectivity between ISE members, members will have direct access to ISE information within those spaces, including ISE-SARs, rather than having to negotiate multiple systems with multiple access rules.

Project Sponsors and Partners

- U.S. Department of Justice (DOJ), Bureau of Justice Assistance (BJA), http://www.ojp.usdoj.gov/BJA
- Federal Bureau of Investigation (FBI), http://www.fbi.gov
- U.S. Department of Homeland Security (DHS), http://www.dhs.gov
- Program Manager, Information Sharing Environment (PM-ISE), http://www.ise.gov
- Major Cities Chiefs Association (MCCA), http://www.majorcitieschiefs.org

- DOJ's Global Justice Information Sharing Initiative (Global), Criminal Intelligence Coordinating Council (CICC), http://www.it.ojp.gov/global
- U.S. Department of Defense (DoD), http://www.defenselink.mil/policy/sections /policy_offices/hd/index.html
- International Association of Chiefs of Police (IACP), http://www.theiacp.org
- Major County Sheriffs' Association (MCSA), http://www.mcsheriffs.com

ISE-SAR Evaluation Environment

The PM-ISE is sponsoring an "evaluation environment," which includes an ISE-SAR Shared Spaces evaluation initiative, to test the assumptions of sharing ISE-SAR information (based on the ISE-SAR Functional Standard and business rules) across multiple domains: state and local law enforcement agencies, state and major urban area fusion centers, federal law enforcement (DOJ), DoD, and DHS. The ISE-SAR tests will examine the usefulness of the ISE-SAR Criteria Guidance (Part B of the ISE-SAR Functional Standard) and the sharing of ISE-SAR information among major city and other law enforcement agencies, JTTFs, and fusion centers and among the fusion centers, JTTFs, and the federal government. Specifically, the evaluation environment will provide the capability to establish, test, and assess end-to-end SAR processes. These include priority information needs (PINs)/guidance, information gathering and reporting, report vetting and standards application, shared SARs, analysis and other utilization, and enabling activities. The SAR Project Management Team will evaluate the evaluation project processes and leverage best/promising practices to develop a model to be expanded to additional agencies.

The agencies participating in the Evaluation Environment (EE) initiative will assess the process of designating information as ISE-SARs, the value of the ISE-SAR information (including the value of including personal information fields), the rules for providing access to the ISE-SAR information, and the types of feedback mechanisms (e.g., for notifying source and submitting organizations of inaccurate information) that are most effective. The ISE-SAR EE will also provide access to a library of free-text SAR summaries without personal information on criminal suspects.

The ISE-SAR Evaluation Environment initiative will use multiple secure Controlled Unclassified Information (CUI) (formerly Sensitive But Unclassified [SBU]) networks as the connection and transport mechanism for sharing SARs. This will give law enforcement agencies access to the SAR Evaluation Environment through the CUI network(s) they currently utilize. Those networks could include RISSNET™; Law Enforcement Online (LEO); the Homeland Security Information Network (HSIN), the DHS network for law enforcement access; Director of National Intelligence—Unclassified (DNI-U); and other CUI networks. The ISE-SAR Evaluation Environment uses a separate server for each agency, controlled by that agency. The server resides outside the agency's firewall and is accessible as the agency's "ISE-SAR Shared Space" to other evaluation environment participants as conceptualized in the PM-ISE EAF.

Lessons learned from the evaluation environment will be used to make recommendations for modifications and expansion of the ISE-SAR Functional Standard. Such modifications are not expected to significantly affect federal, state, and local activities currently under way to implement the ISE-SAR Functional Standard. In addition, the lessons learned will be used to establish applicable business processes and best practices and will inform the SAR Segment Architecture.

Agency Reporting of an ISE-SAR

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 preoperational planning related to terrorism, criminal, or other illicit intention" for a report documenting such activity to be considered a SAR under this standard.[7] Before any information is posted in an ISE Shared Space as an ISE-SAR, it will be subject to multiple levels of review and vetting by trained personnel to ensure that the information meets ISE-SAR criteria, has a potential nexus to terrorism, and was legally obtained. The ISE-SAR Functional Standard 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 state, local, and tribal SAR information), or
- A federal agency[8]

The ISE-SAR Functional Standard indicates that the designation of an ISE-SAR is a two-part process. 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. 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). 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.

The review and vetting process begins when a frontline law enforcement officer responds to a call for service or self-initiates law enforcement action based on a reported incident/observation or the officer's observation of suspicious behavior. To preclude reporting on individuals involved in innocent activities, frontline personnel must be able to recognize indicators of criminal activity associated with domestic and international terrorism and must understand the scope of their legal authority to obtain information. Frontline personnel will be trained to recognize behaviors and incidents indicative of criminal activity associated with domestic and international terrorism. This training will be designed to expand the knowledge of frontline personnel regarding the modus operandi (MO) of individuals and organizations known to be involved in criminal activity associated with terrorism. This training will be provided for the specific purpose of enabling frontline personnel to evaluate reported or observed behavior and other factors so that they can differentiate between those potentially related to criminal activity and those that are not, so as to minimize reporting on individuals who are, in fact, involved in innocent activities. Frontline

[7] See http://www.ise.gov/docs/ctiss/ISE-FS-200SARFunctionalStandardIssuanceVersion1.0.pdf, p. 2.

[8] 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 (DoD) has indicated intent to use the FBI's eGuardian system as its shared space for posting ISE-SARs. Accordingly, eGuardian may be one of several federal shared spaces.

personnel will also be trained on privacy, civil rights, and civil liberties issues, including an officer's legal authority to gather information.

Should the frontline officer document suspicious activities in a report, that report will be reviewed by a supervisor or other trained agency personnel to ensure that information relates to potential criminal conduct and was legally obtained by the officer. In many larger urban law enforcement entities, a third level of review will be established through the use of specially trained investigators/analysts who review the report to determine whether there is a potential terrorism nexus. If a potential nexus to terrorism is found, these locally generated SARs must be forwarded to the local JTTF for possible investigation and will be forwarded to the cognizant state or urban area fusion center where they, along with other SARs, will be subjected to a two-step vetting process by a trained expert using his or her knowledge and experience to determine whether each SAR (1) meets ISE-SAR criteria and (2) has a potential nexus to terrorism prior to being posted on an ISE Shared Space as an ISE-SAR. Each fusion center and local entity participating in the ISE-SAR EE will develop or follow established business rules that formalize this process. The goal is for ISE-SARs to be shared, to the maximum extent possible, among state, local, and federal law enforcement, homeland security, and other appropriate organizations participating in the ISE while protecting information associated with the designated privacy fields. At the time the decision is made to share the information with the ISE, it must be labeled as to its perceived reliability and validity.

SAR Information Sharing Goals—Complete, Accurate, and Timely

Efforts to prevent terrorist attacks are most effective when accurate, valid, and reliable information is used to support law enforcement investigations and other counterterrorism activities. Since the laws, statutes, and practices that support, prohibit, or otherwise limit the sharing of personal information vary considerably between and among the federal, state, and local levels, two SAR information exchanges are supported in the Information Exchange Package Documents (IEPD) of the ISE-SAR Functional Standard. Each set of SAR exchange partners can employ one of the two following exchange types, dependent upon the trust and legal relationship that exist between the SAR data provider and SAR data consumer.

1. Detailed SAR Exchange—includes all law enforcement-defined data elements. The privacy field elements are uniquely identified within the detailed SAR IEPD artifacts so that such elements can be reviewed and, where necessary, expanded to enable compliance with applicable data retention policies and practices by the originating agency.

2. Summary SAR Exchange—includes all law enforcement-defined data elements minus the privacy elements.

Each ISE participant may exclude additional privacy fields from its Summary ISE-SARs, in accordance with its own statutory or policy requirements.

The ISE-SAR Shared Spaces concept and environment were collaboratively developed in partnership with federal, state, and local law enforcement agencies. ISE-SAR information populated to the ISE will be provided by local law enforcement, state agencies, or field elements of federal agencies based on information gleaned from various sources and tracked within systems built and maintained by federal, state, and local authorities. Most of this information is also known as "tips" or "threat information" submitted by citizens to the police or reported by officers through their ordinary chain of command. Most agencies document this data into their records management system (RMS), field interviews (FI), or other related processes. This evaluation project does not seek to create new systems but rather to leverage the current systems and extract certain data concerning suspicious activity relating to terrorism and make it sharable with other agencies in the ISE.

The ISE-SAR Functional Standard does not dictate a common process that applies to data quality. Data contained in reports designated as ISE-SARs derives 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 systems to validate information relating to the incident or conduct.

The authors[9] of the *Initial Privacy and Civil Liberties Analysis of the Information Sharing Environment—Suspicious Activity Reporting (ISE-SAR) Functional Standard and Evaluation Environment (Version 1—September 2008)*[10] recommend that the ISE-SAR Evaluation Environment sites require source agencies documenting suspicious activity to assess their confidence in the information they report, including source reliability and content validity. 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 and ISE-SAR 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 and updating improves the quality of the information and also protects the information privacy and other legal rights of American citizens.

Each source and submitting agency is responsible for its own data. System and security administrators for the participating agencies will add, update, and/or delete data per the process to be designed. Each submitting agency maintains control over what is updated, added, modified, or deleted in the shared space, according to its established policy and practice. When a search occurs, the record is shared for informational purposes and follow-up with the agency, but it is not downloaded; therefore, the submitting agency always has control of the data. It is anticipated that analytical tools will be developed in the future to support trend analysis and other nonpersonal information analysis.

State constitutions, statutes, local ordinances, and policies will dictate the distributed housing of SAR and ISE-SAR data in each agency or fusion center. Some SAR elements or the SAR in its entirety may be deleted or retained for a specific maximum time period based on statutes, codes, and applicable policies. For example, some agencies and centers may require a data purge if an actionable offense or case is not established or pursued based on the data within a certain time frame. Review periods may be established in some agencies and centers where a

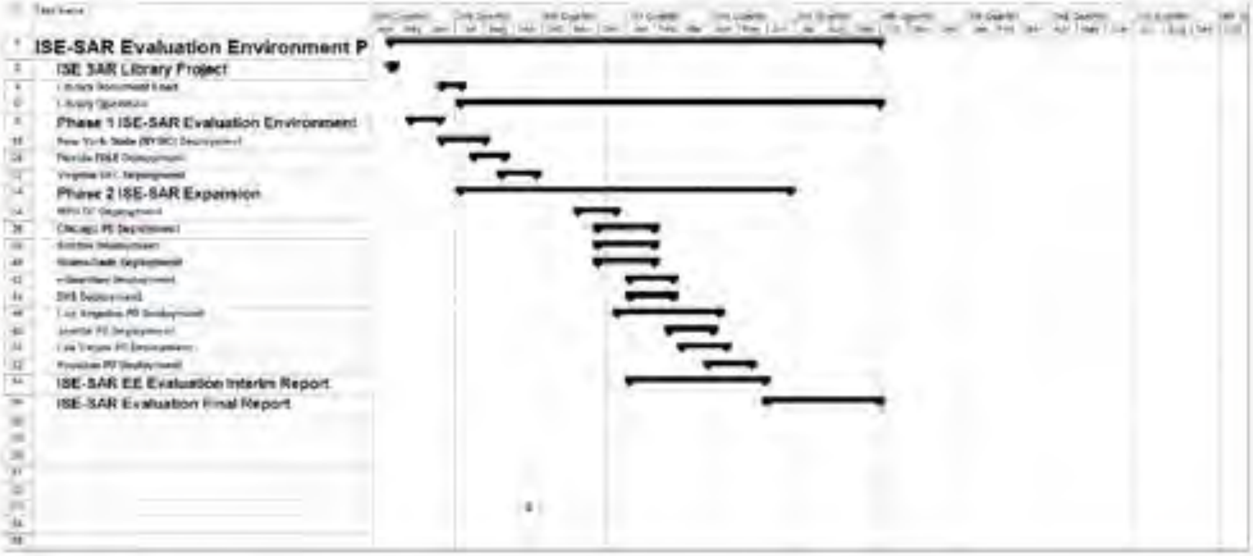
[9] The PM-ISE—in consultation with the Civil Liberties and Privacy Office of the Office of the Director of National Intelligence (ODNI), the Office of Privacy and Civil Liberties of the Department of Justice (DOJ), and the Legal Issues Working Group of the ISE Privacy Guidelines Committee—prepared and released an Initial Privacy and Civil Liberties Analysis of the ISE-SAR Functional Standard and included IEPD component.

[10] See http://www.ise.gov/docs/sar/ISE_SAR_Initial_Privacy_and_Civil_Liberties_Analysis.pdf.

decision is made as to whether the information should be retained for a longer period of time or otherwise purged. Each agency must develop written policy concerning information retention.

Deployment Timeline

Following is the nominal time schedule for deployment of the evaluation project:



Task Name
ISE-SAR Evaluation Environment P
ISE SAR Library Project
Library Document Load
Library Operation
Phase 1 ISE-SAR Evaluation Environment
New York State (NYSIC) Deployment
Florida FDLE Deployment
Virginia VFC Deployment
Phase 2 ISE-SAR Expansion
NYPD CT Deployment
Chicago PD Deployment
Boston Deployment
Miami-Dade Deployment
[illegible] Deployment
DHS Deployment
Los Angeles PD Deployment
Seattle PD Deployment
Las Vegas PD Deployment
Houston PD Deployment
ISE-SAR EE Evaluation Interim Report
ISE-SAR Evaluation Final Report

Potential Participating Agencies

A number of cities, states, and federal agencies are being considered as potential SAR Evaluation Environment project sites. The venues are being considered due to a number of factors, including involvement in the MCCA's SAR Support and Implementation Project, which developed several recommendations regarding implementation of the SAR process, level of technology, maturity of the fusion center, and existing data efforts in the area of SARs.

1.2 ISE-SAR EE Scope

The following provides further explanation as to what the SAR evaluation project is and what it is not:

- ISE-SAR Shared Spaces support information sharing across the ISE.
- The data contained in ISE-SAR Shared Spaces is not intended for use in statistical research and/or reports. Participants will not be able to download the shared data in order to ensure that outdated data will not be stored in systems outside of the participating agency's system.
- ISE-SAR Shared Spaces database is not a criminal intelligence system or database that would require application of 28 CFR Part 23.
- SAR Summary Exchange data will be maintained in ISE-SAR Shared Spaces and will serve as a pointer index to other agency systems/points of contact that contain/provide additional detailed information. The ISE-SAR Summary Library will

contain *only* SAR summary exchange and other data that is not "personal information" regarding a criminal subject.

- The data in ISE-SAR Shared Spaces is managed and maintained (controlled) by the submitting agency that is operating under individual state and local jurisdictional laws and policies.
- Once SAR data rises to the level of reasonable suspicion, the agency may also make a submission to a criminal intelligence information database or system.
- Data in ISE-SAR Shared Spaces will be accessible by authorized ISE-SAR EE participants in fusion centers, law enforcement agencies, JTTFs, and FBI Field Intelligence Groups (FIGs) via the CUI networks that provide secure communication.
- Vetting of data for inclusion in the ISE-SAR Shared Spaces will include contact with the local JTTF/National JTTF and the Terrorist Screening Center (for Violent Gang and Terrorist Organization File queries) in order to determine whether current investigative activity is ongoing.

1.3 SAR Data Control

Management of data placed in ISE-SAR Shared Spaces will remain the responsibility and be under the control of the submitting agency. The technology provides an aggregate query function for linking the distributed ISE-SAR data collected and maintained by each participating agency. Participating agencies must ensure that they comply with state and local laws, policies, and relevant federal rules and project guidelines.

The submitting agency may update/modify/delete the initial record based on additional information. The submitting agency is the only organization authorized to update/modify/delete the ISE-SAR data it enters into the shared space. In the event that an ISE-SAR is subsequently determined to be unsubstantiated, the agency must remove the report from the ISE-SAR Shared Space. In the event that the activity occurred but the privacy field data is invalid, the privacy field data must be removed and the ISE-SAR updated in the applicable ISE-SAR Shared Space.

An ISE-SAR EE participant who, on the basis of additional information, finds that there is a potential connection between two or more records in ISE-SAR Shared Spaces should contact the submitting agencies to update each of their individual records.

1.4 SAR Implementation Technology

ISE-SAR Shared Spaces will use the ISE EAF,[11] which provides a common architectural structure for agencies to use to incorporate their information sharing capabilities into the ISE. It provides a logical structure of ISE business processes, information flows and relationships, services, and high-level data packet descriptions and exchange relationships.

[11] See http://www.ise.gov/docs/eaf/ISE-EAF_v1.0_20070830.pdf.

1.5 Collaborative Development

ISE-SAR Shared Spaces will be designed and implemented in a collaborative and inclusive manner involving federal, state, and local law enforcement partners. This may include the development and documentation of previously nonexistent "collaborative" processes.

The scope of this project is to continue the national SAR implementation emphasized in the NSIS. The first phase of the initiative was the development of the SAR Library and the ISE Enterprise Architectural principle of ISE-SAR Shared Spaces as well as the testing of the ISE-SAR Functional Standard. This phase will include the formation of teams from each location with state, local, FBI, and DHS members to document the "as is" process, identification of the risk to the location, the development of an improved flow of ISE-SARs, and the use of coordinated collection; liaison and alerts, warnings, and notification capabilities leverage; and federal/national priority information needs. The *Findings and Recommendations of the SAR Support and Implementation Project* will assist with the front-end collection and the building of the server for ISE Shared Spaces. Additionally, templates will be developed for best practices to accelerate the national implementation of the ISE-SAR process.

2 Design and Implementation

This section describes how the ISE-SAR Evaluation Environment is technically designed and implemented.

2.1 Leveraging Existing Technology

ISE-SAR Shared Spaces will use multiple secure CUI networks as the connection and transport mechanism for sharing ISE-SARs. Those networks could include RISSNET, LEO, HSIN, possibly DNI-U and, potentially, others.

This project will be guided by the ISE-SAR Functional Standard, which includes the SAR IEPD, as its information sharing standard. The Common Terrorism Information Sharing Standards (CTISS) program is designed to develop, disseminate, and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations, as well as support the day-to-day operations of agencies throughout the nation.

To accelerate implementation of the ISE-SAR Shared Spaces, DOJ's existing National Criminal Intelligence Resource Center (NCIRC) system will host an ISE-SAR federated shared-space search page. The search page on the NCIRC system will afford multiple benefits, including secure access to ISE-SARs from multiple points; free-text searches, utilizing the ISE-SAR Library application; and access to specific originator contact information for follow-up purposes without compromising privacy rules or regulations. Appendix E illustrates the steps to conducting a federated SAR Search.

2.2 ISE-SAR Shared Spaces Design Assumptions

Basic design assumptions for ISE-SAR Shared Spaces application:

1. The query will check for all supplied search criteria.

2. The query will provide the opportunity for a search of all selected ISE-SAR Shared Spaces, to include eGuardian and DHS Shared Space servers as resource availability allows.

3. Sorting will provide grouping of results in a logical manner and will utilize user input to determine the most meaningful sorting criteria as future versions of the application are released.

4. The query responses will be limited if the search criteria is too broad and the number of results is excessive. Should this limitation be employed, the user will be alerted to refine the search criteria.

5. The user interface will be developed using commonly accepted secure Internet-based technologies.

6. The user will be able to select the individual agency data sources (or all) for each query. If a data source is unavailable, the query will complete with the data sources that are available and provide the user with a message indicating which sources were not queried.

7. Results from queries will be aggregated into a list from which the user may select individual responses for further review.

8. Items presented in the initial results list will display submitting organization, contact information, and ISE-SAR information.

9. The results interface will provide an option to sort results based on submitting organization, contact information, and ISE-SAR information.

10. Selection of a record from the query results list will retrieve the specific ISE-SAR identified in that selection.

11. Office of Justice Programs Web certification and Section 508, 29 U.S.C. 794d (as amended) compliance issues do not apply because the ISE-SAR Shared Spaces database is not a public database.

12. An audit log will be created to capture search transactions at a central query site and agency database.

13. An online help module will be created to assist users with system use.

14. User access to the ISE-SAR distributed search will be provided utilizing the RISSNET, HSIN, LEO and, possibly, DNI-U networks and the access control mechanisms associated with each (yet to be decided).

15. The ISE-SAR distributed search Web service connections will access the agency ISE-SAR Shared Spaces databases by Virtual Private Network (VPN) connection unless the agency prefers a different connectivity strategy.

16. The system administrator will support overall operation of the system.

17. The security administrator will monitor system security.

18. A front-end screen will be included when a user initially accesses the system. Standard language should be included; e.g., *Data is sometimes entered poorly, processed incorrectly, and generally not free from defect. This system should not be relied upon as definitively accurate. Before relying on any data this system supplies, verify the data independently or with the agency that originated the data. This information is provided for investigative purposes only unless otherwise cleared with the originating agency and disseminated only to authorized personnel.*

19. The system supports the documenting and viewing of ISE-SARs. While the information may be included in reports, no download or reporting functions or features are included as part of the baseline system.

20. Shared-space ISE-SAR systems will all provide a uniform data representation of agency data based on the ISE-SAR Functional Standard.

21. Shared-space ISE-SAR systems will provide Web services to be consumed by the central ISE-SAR query site to facilitate queries of ISE-SAR information held on each shared space server.

22. Shared-space ISE-SAR systems will perform the necessary database queries to provide a valid response to the ISE-SAR central query site.

23. An administrative page will be established on the NCIRC site to allow agencies to forward designated SARs to the eGuardian system.

System Security

ISE-SAR Shared Spaces EE is not a national security system and will not contain classified information. ISE-SARs will be considered law enforcement sensitive and, thus, warrant protection. The data will be categorized as CUI information. The ISE-SARs will be stored, processed, and disseminated in a protected information environment that provides adequate security controls. These controls will include:

- Controlled access to the information that allows only authorized users—limited to certain individuals during pilot—to access, retrieve, and display ISE-SAR information and restricts writing and updates to authorized members of the originating organization.

- DOJ's Trusted Broker solution will be used to allow access to the shared space from multiple CUI networks.

- Encrypted transmission of information sent between ISE members.

It is anticipated that the ISE-SAR Evaluation Environments will employ the following specific security measures:

- The ISE-SAR Shared Spaces EE exists in distributed, federated environments. The original hosting of the information is done by the local agency or state or major urban area fusion center that maintains the shared space. When the originating agency replicates the information to ISE-SAR Shared Spaces, a firewall will remain, allowing only the Web service developed for this project to conduct a search on that data in ISE-SAR Shared Spaces.

- The connection of the systems will be done using a secure connection tunnel via an encryption VPN.
- All information will be CUI. The originating agencies will move to ISE-SAR Shared Spaces only what they are allowed to share by their constitution or statutes; local ordinances; agency policy; or federal, state, and local laws and regulations.

A standardized participation agreement will be issued by PM-ISE to candidate sites for the ISE-SAR Shared Spaces evaluation project, and it will be used for future implementation of any part of the capability. Participation in the SAR evaluation project will be limited. The participant agreement will be used for the sharing of data with other federal, state, and local law enforcement agencies outlining the policies, procedures, and practices for the handling and use of ISE-SAR Shared Spaces data as well as the responsibilities of PM-ISE and the participating agency during the project term. These policies, procedures, and practices will cover the actions of source and submitting agencies as well as how recipients can use shared data. The source and submitting agencies have the shared responsibility to ensure that information was not acquired, contributed, or maintained in violation of any applicable constitution, law, or ordinance.

System Availability

To the extent possible, the ISE-SAR system will be available 24 hours a day, 7 days a week, except for scheduled periods of system maintenance or other downtime. The participating evaluation environment agencies will be responsible for any backup of their data in ISE-SAR Shared Spaces as well as any necessary maintenance repairs.

Technical Requirements

In order to participate in the ISE-SAR EE, an agency should have an existing source (database) of SARs that could be copied into a shared-space database server. Additionally, the agency must permit outside users to access this ISE-SAR data in the shared space via a secure Internet connection.

2.3 Data Submission Process

The ISE-SAR IEPD standard will be used for the ISE-SAR evaluation project. In addition, the Law Enforcement Information Sharing Program (LEISP) Exchange Specifications-Search and Retrieval (LEXS-SR) standard will be used to exchange search results between each shared space server and the central NCIRC portal. The LEXS-Publication and Discovery (LEXS-PD) standard will be used to "push" designated SARs from agency shared space servers to an eGuardian staging area for ingest into eGuardian and eventual publishing to the eGuardian shared space. As the ISE-SAR evaluation project matures, a standard set of data collection codes will be established and will ultimately be maintained by the ISE-SAR Steering Committee in coordination with the CTISS Committee.

2.4 Data Query Process

Search Parameters

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. Data hosted and housed within each participating agency will be retrieved based on a user making a query of a particular person, place, vehicle, or thing (MO or behavior), and the system will identify which documents contain the requested information. The user can then request to view the specific report(s) and/or elect to make direct contact with the agency contributing the data. Contact information for the data owner is part of the information that is returned to the user. This could be an individual officer or a main phone number for the respective investigative unit within a department.

2.5 Data Output and Data Dissemination Constraints

Because of schedule and funding constraints, functional capabilities for the ISE-SAR Search capability have been limited. Although these capabilities may be added in the future, the initial SAR EE is purposely designed to support only read-only search functions.

- Analytical software capabilities are not planned for the initial SAR Evaluation Environment project. The need for those capabilities will be determined during this initiative.

- Agencies will not have permission to download data from ISE-SAR Shared Spaces for inclusion into local systems.

- During the evaluation project, capability for online collaboration with data submitters/data query agencies will not be available; however, the project will attempt to leverage technology that is available for this purpose through RISSNET and LEO.

- The evaluation project will not support any "subscription-type" services (e.g., "I'm looking for Man X, and I'm going to have a standing search order that every time an ISE-SAR is submitted that matches Man X, I'm notified via e-mail."). The need for this type of services will be evaluated as part of the evaluation project.

- The system will not have the capability to notify specific groups about a particular ISE-SAR during this evaluation project; however, this capability is planned in future iterations.

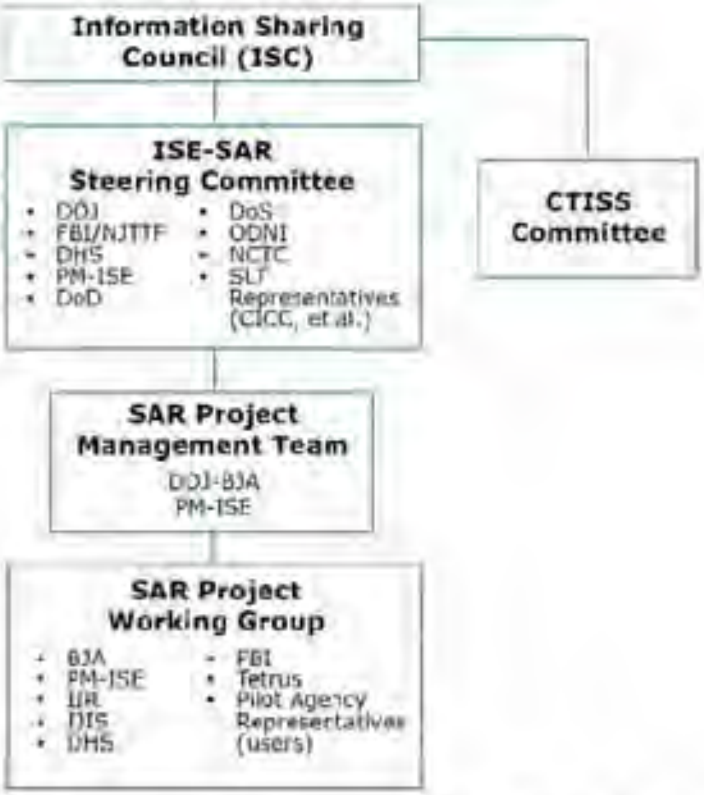
- Data will be retrieved based on a user making a query of a particular person, place, vehicle, or thing and the system identifying which reports contain the requested information. The user can then request to view the specific reports and/or elect to make direct contact with the agency contributing the data. Contact information for the data source is part of the information that is returned to the user.

Data uploads to the solution from its source will be accomplished via secure Internet transmission. The initial uploads may be large and will require manual copying to protected media, but subsequent updates can be sent to the evaluation solution, utilizing the published IEPD.

3 Project Governance

3.1 Project Administration

The following graphic depicts the SAR Governance Structure:


Information Sharing Council (ISC)
ISE-SAR Steering Committee
• DOJ
• FBI/NJTTF
• DHS
• PM-ISE
• DoD
• DoS
• ODNI
• NCTC
• SLT Representatives (CICC, et al.)
CTISS Committee
SAR Project Management Team
DOJ-BJA
PM-ISE
SAR Project Working Group
• BJA
• PM-ISE
• IIR
• DIS
• DHS
• FBI
• Tetrus
• Pilot Agency Representatives (users)

The ISE-SAR Steering Committee provides strategic direction to the ISE-SAR EE. The committee synchronizes interagency activities, resolves major issues, and addresses resource needs. It is charged with developing ISE-SAR policies and practices and addressing evolving SAR requirements and will be responsible for addressing agency noncompliance issues. The ISE-SAR Steering Committee forwards needed change requirements from this project for the ISE-SAR Functional Standard to the CTISS Committee for incorporation into future versions of the ISE-SAR Functional Standard and consideration with other functional or technical standards of the CTISS.

The SAR Project Management Team is responsible for overall oversight of the evaluation project. The Project Management Team provides guidance to the SAR Project Working Group; approves the project scope, modifications, and updates; and resolves issues forwarded by the Project Working Group.

The SAR Project Working Group is composed of the Project Management Team members, the service providers implementing the project, and representatives from the state and local agencies involved in the evaluation project. The Project Working Group is responsible for the day-to-day project implementation and issue resolution, providing subject-matter expertise when developing system requirements and capabilities and maintaining/tracking project decision items. The Project Working Group may constitute user/focus groups for specific project purposes. Unresolved issues from the Project Working Group will be pushed to the Project Management Team for resolution and, ultimately, the ISE SAR Steering Committee, if needed.

Rules/Regulations Related to Participation

Participating agencies will receive a letter (attached) from the PM-ISE describing the ISE-SAR EE project and outlining the responsibilities of each party during the term of the evaluation project. The agency will be asked to acknowledge acceptance of the responsibilities outlined in the PM-ISE letter.

3.2 Privacy and Civil Liberties Protection

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] intention." Each government entity that collects and documents suspicious activities at the local, state, tribal, and federal levels must do so in accordance with applicable law and policy.

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. 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.

Participating fusion centers may adopt the umbrella ISE-SAR Evaluation Environment Privacy, Civil Rights, and Civil Liberties Protection Policy as a stand-alone policy for the EE Initiative or have in place an approved fusion center privacy protection policy that is "at least as comprehensive" as the ISE Privacy Guidelines. If the umbrella policy is used, it must be modified, as necessary, to be consistent with the state's constitution, statutes, local ordinances, and other legal requirements. Each participating fusion center is encouraged to use the Global Privacy Impact Assessment (Global PIA, in draft, see attachment) to determine whether additional protections are warranted.

As part of the evaluation environment, each participating site will document the manner in which the ISE-SARs information is being posted and shared via the shared space and how the site is complying with its ISE-SARs privacy and civil liberties protection policy.

Should federal entities deploy a federal system, they will have to comply with the Umbrella Policy (or their agency's ISE Privacy Protection Policy) and applicable federal requirements—including the ISE Privacy Guidelines, statutes, and regulations—and develop a Privacy Impact Assessment (PIA) in accordance with the E-Government Act of 2002.

The PM-ISE—in consultation with the Office of the Director of National Intelligence (ODNI) Civil Liberties and Privacy Office, DOJ Office of Privacy and Civil Liberties, and the ISE Privacy

Guidelines Committee (PGC) Legal Issues Working Group—has prepared and publicly released a report entitled *Initial Privacy and Civil Liberties Analysis of the Information Sharing Environment—Suspicious Activity Reporting (ISE-SAR) Functional Standard and Evaluation Environment (Version 1—September 2008).* The purpose of this analysis is to ensure that the implementation of the ISE-SAR Functional Standard and Evaluation Environment is conducted in a manner that fully protects the legal rights of Americans, including information privacy, civil rights, and civil liberties guaranteed by the Constitution and the laws of the United States. The analysis 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.

The *Initial Privacy and Civil Liberties Analysis* consists of an introductory section explaining the purpose of the ISE-SAR Functional Standard and plans to test at various evaluation environment sites, a set of questions and answers exploring the privacy and civil liberties ramifications of the ISE-SAR data exchange model and of implementing the ISE-SAR initiative, and a conclusions and recommendations section identifying key privacy and civil liberties concerns that entities participating in the ISE-SAR Evaluation Environment initiative should address as they implement ISE-SAR sharing activities.

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 throughout implementation.

After the implementation of the ISE-SAR Functional Standard, the PM-ISE—in consultation with the ODNI Civil Liberties and Privacy Office, DOJ Office of Privacy and Civil Liberties, and the ISE PGCs Legal Issues Working Group—will release a *Final ISE-SAR Privacy and Civil Liberties Analysis* that will identify how the key privacy and civil liberties issues identified in the conclusion and recommendations section of the *Initial ISE-SAR Privacy and Civil Liberties Analysis (Version 1—September 2008)* were addressed during the implementation of the ISE-SAR Functional Standard in the evaluation environment.

The authors of the *Initial Privacy and Civil Liberties Analysis* recommend the following minimum protections for the EE initiative:

- Train frontline and supervisory personnel regarding recognized behaviors and incidents associated with terrorism-related criminal activity as well as the privacy and civil liberties implications of suspicious activity reporting (e.g., constitutional and other legal protections),the application of the ISE Privacy Guidelines in the ISE-SAR context, and U.S. person-related collection limitations.
- Develop and implement robust privacy, civil rights, and civil liberties protection policies for all information collection, use, storage, and sharing activities.
- 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.
- Establish multiple levels of vetting to ensure that only information that meets SAR and ISE-SAR criteria, including that it has been legally obtained, is shared with other law enforcement and homeland security authorities.

- Promote a policy of openness and transparency when communicating to the public regarding their SAR process.
- Delay sharing privacy field information until such time as adequate privacy and civil liberties protections are in place.
- Integrate 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.
- Clearly articulate when federal regulations regarding the handling of criminal intelligence (e.g., 28 CFR Part 23) should be applied.
- Ensure that privacy and civil liberties protection policies address core privacy principles, such as accuracy, redress, retention and disposition, and disclosure of personal information, consistent with federal, state, and local legal requirements.
- Audit SARs for quality and substance to ensure that the integrity of the SAR program is maintained.
- Use legal or privacy advisors in the development of the SAR process.
- Adopt an appropriate policy for documenting (written or electronic) error notification (feedback) in three areas:
    1. Feedback to originators when fact information is incorrectly designated as ISE-SAR.
    2. Feedback to all participants if further evidence determines that an ISE-SAR was designated incorrectly.
    3. Recommended changes to the ISE-SAR Criteria Guidance (Part B of the ISE-SAR Functional Standard).
- Incorporate checks/procedures to prevent "profiling" based 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).
- 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.
- Require that 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.
- Provide multiple levels of review and vetting.
- Require a demonstration of a law enforcement need for accessing personal information elements (privacy fields) before sharing those elements from the detailed ISE-SARs.
- Provide notice to sources or users of errors in the content or designation of an ISE-SAR.
- Provide appropriate notice of source reliability and content validity of an ISE-SAR.
- Maintain detailed information logs (queries, accesses).

- Establish an audit element and technical safeguard requirements.
- Prohibit users from "reverse engineering" Summary ISE-SAR information in an effort to determine the identity of protected persons.
- Implement user restrictions for ISE-SARs, such as user training, and user notification mechanisms.
- Limit functionality in the ISE Shared Spaces so that access 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.

3.3 Data Access Policy

Data Access Protocols to Ensure Protections

Information in this system is safeguarded in accordance with applicable laws, rules, policies, and practices. Records and technical equipment will be maintained in buildings with restricted access. This evaluation project will have complete audit logs for all additions, edits, and deletions of records.

Passwords, password protection identification features, and other system protection methods also restrict access to information in this system. Only criminal investigative/analytical personnel from other evaluation project participating federal, state, and local law enforcement agencies, by express agreement, are permitted access to the system. All authorized personnel will be vetted using the current authentication processes and procedures for the CUI/SBU systems providing access to ISE-SAR Shared Spaces.

Personal information will be used for official criminal law enforcement and national security purposes only. The information cannot be accessed or used for any other purpose, including general licensing, employment, eligibility for federal or state benefits, or background investigations. The information may be disclosed regarding information controlled by the agency in response to a request made under any state or local information access law.

Several administrative and technological controls secure the information contained in this evaluation project. The security administrator and system administrator are two distinct roles that will be created in the evaluation project application. The security administrator is responsible for viewing, monitoring, and archiving security logs and audit trails and has the ability to add, change, or delete users and their system access privileges. The system administrator is responsible for the maintenance and operation of the system as a whole, including backing up the system and its recovery.

User agreements will be created to ensure that the system is accessed for law enforcement purposes only and that only individuals supporting a law enforcement mission will have access to ISE-SAR Shared Spaces. This may include investigators, agents, officers, and analysts performing functions in a federal, state, or local law enforcement agency or fusion center.

Access will be limited to evaluation project agency personnel, selected law enforcement agency personnel, and selected federal participants (FBI, DHS, DoD), and they will have access to ISE-SAR Shared Spaces for testing purposes. Participating agencies will agree to share ISE-SAR information, at least in the Summary SAR Exchange form, with all other participants. In particular, cities will agree at the initiation of the evaluation project that their state fusion center will have access to their shared spaces. Participating agencies will identify their internal test user group for access to ISE-SAR Shared Spaces.

Access Rights

- User authentication process

Participation in the SAR evaluation project is limited, and only those users associated with selected participating entities will have access to the system and its data. Access to the data by system administrators and/or security officers will be limited to only that needed to perform these functions and will be restricted to authorized law enforcement personnel and analysts of federal, state, and local agencies with a need for access. All such personnel (either government employees or contractors/subcontractors) shall be vetted and authenticated for system access, and their access shall be monitored and audited.

A "purpose screen" will require users to document access to the system.

All users must be trained on the system use and privacy policies before access is given.

4 Data Security Policy

Security policies and protocols will be developed for use in the evaluation project. The security policy will address the following areas: project security agent, agency security agreements/user security agreements, firewalls and network security, data location security, privacy policy, audits, and user activity monitoring.

5 Logs and Audits

The evaluation system has an audit capability that will log the date, time, subject, and originating account of all user queries at both the system and participating agency level. The parties will maintain these audit logs for up to five years. The security staff will also be able to review these audit logs.

Several administrative and technological controls secure the information contained in this evaluation project. Security and system administration activities will occur in the evaluation project, and these functions include viewing, monitoring, and archiving security logs and audit trails; the ability to add, change, or delete users and their system access privileges; and maintenance and operation of the system as a whole, including backing up the system and its recovery.

6 Training and Technical Assistance

The ISE-SAR Shared Spaces Help Desk is designed to assist users in finding answers to preliminary technical and operational questions. The help desk will be located at the IJIS Institute Web site, http://www.IJIS.org. Secondary assistance will be provided by project technical assistance providers as needed. Specific information on the help desk function and technical points of contact will be provided to participating agencies as their shared-space systems become operational.

An online user manual will be accessible from the shared-space query page.

As in existing law enforcement training and academy and in-service settings, officers will be trained to investigate SARs based upon "the totality of circumstances." This training and methodology prepares officers to follow established investigation practices, contributes to appropriate decision making, and supports proper information flow in the SAR process.

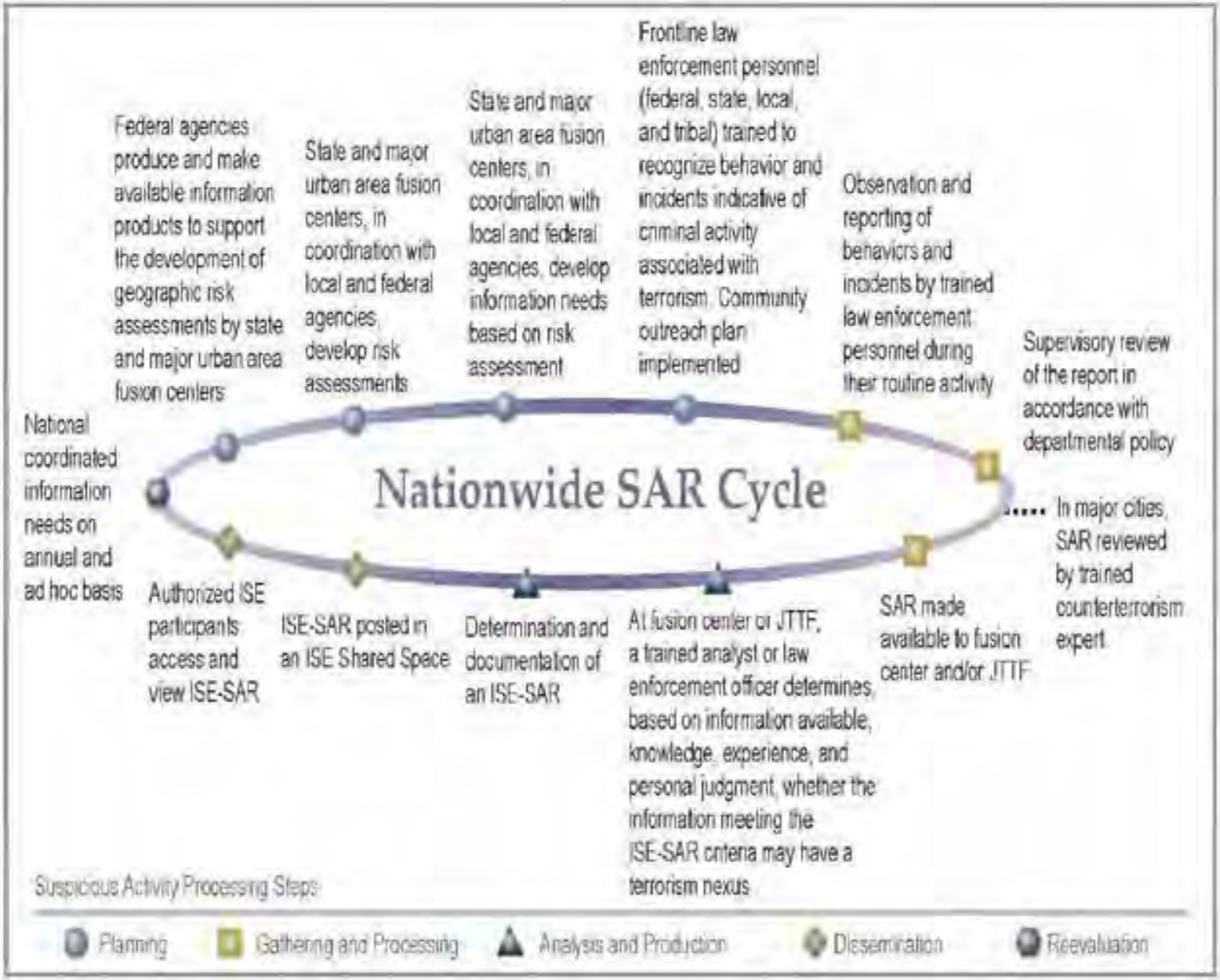
Online training tools will be developed, and as the project progresses and additional phases are implemented, other training methodologies will be developed as needed (WebEx training scenarios and other methods, as appropriate).

Training will be required for all users, including those accessing information from other systems, participating in the evaluation project. The training will include policies, procedures, and practices to ensure that users know how to properly use the information. This training will be provided to make users of the information aware of what information can be accessed from the system and will include a description of the information contained in the system and other appropriate information. All users will participate in a project WebEx training before being able to access information from ISE-SAR Shared Spaces. Verification of the training completed will occur before providing access to ISE-SAR Shared Spaces.

Appendix A: Acronyms and Abbreviations

BJA	Bureau of Justice Assistance
CFR	Code of Federal Regulations
CICC	Criminal Intelligence Coordinating Council
CTISS	Common Terrorism Information Sharing Standards
CUI	Controlled Unclassified Information
DHS	U.S. Department of Homeland Security
DoD	U.S. Department of Defense
DNI-U	Director of National Intelligence—Unclassified
DOJ	U.S. Department of Justice
EAF	Enterprise Architecture Framework
EE	Evaluation Environment
FBI	Federal Bureau of Investigation
FI	Field Interview
FIG	Field Intelligence Group
Global	Global Justice Information Sharing Initiative
HSIN	Homeland Security Information Network
IACP	International Association of Chiefs of Police
IEPD	Information Exchange Package Document
ISE	Information Sharing Environment
JTTF	Joint Terrorism Task Force
LEISP	Law Enforcement Information Sharing Program
LEO	Law Enforcement Online
LEXS-PD	LEISP Exchange Specifications-Publication and Discovery
LEXS-SR	LEISP Exchange Specifications-Search and Retrieval
MCCA	Major Cities Chiefs Association
MCSA	Major County Sheriffs' Association
MO	Modus Operandi
NCIRC	National Criminal Intelligence Resource Center
N-DEx	National Data Exchange Program
NIEM	National Information Exchange Model
NSIS	*National Strategy for Information Sharing*
ODNI	Office of the Director of National Intelligence
PIA	Privacy Impact Assessment
PIN	Priority Information Need
PGC	[ISE] Privacy Guidelines Committee
PM-ISE	Program Manager, Information Sharing Environment
RISSNET	Regional Information Sharing Systems Network
RMS	Records Management System
SAR	Suspicious Activity Reporting
TSC	[FBI] Terrorist Screening Center
VPN	Virtual Private Network
XML	Extensible Markup Language

Appendix B: Nationwide SAR Cycle



National coordinated information needs on annual and ad hoc basis

Federal agencies produce and make available information products to support the development of geographic risk assessments by state and major urban area fusion centers

State and major urban area fusion centers, in coordination with local and federal agencies, develop risk assessments

State and major urban area fusion centers, in coordination with local and federal agencies, develop information needs based on risk assessment

Frontline law enforcement personnel (federal, state, local, and tribal) trained to recognize behavior and incidents indicative of criminal activity associated with terrorism. Community outreach plan implemented

Observation and reporting of behaviors and incidents by trained law enforcement personnel during their routine activity

Supervisory review of the report in accordance with departmental policy

In major cities, SAR reviewed by trained counterterrorism expert

SAR made available to fusion center and/or JTTF

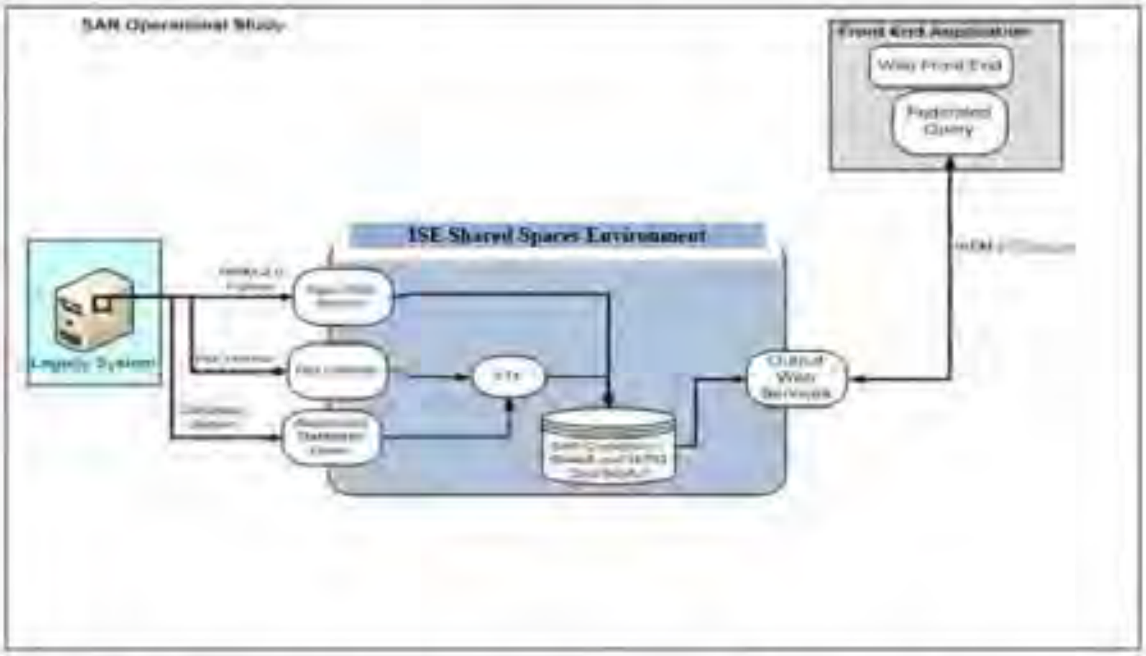
At fusion center or JTTF, a trained analyst or law enforcement officer determines, based on information available, knowledge, experience, and personal judgment, whether the information meeting the ISE-SAR criteria may have a terrorism nexus

Determination and documentation of an ISE-SAR

ISE-SAR posted in an ISE Shared Space

Authorized ISE participants access and view ISE-SAR

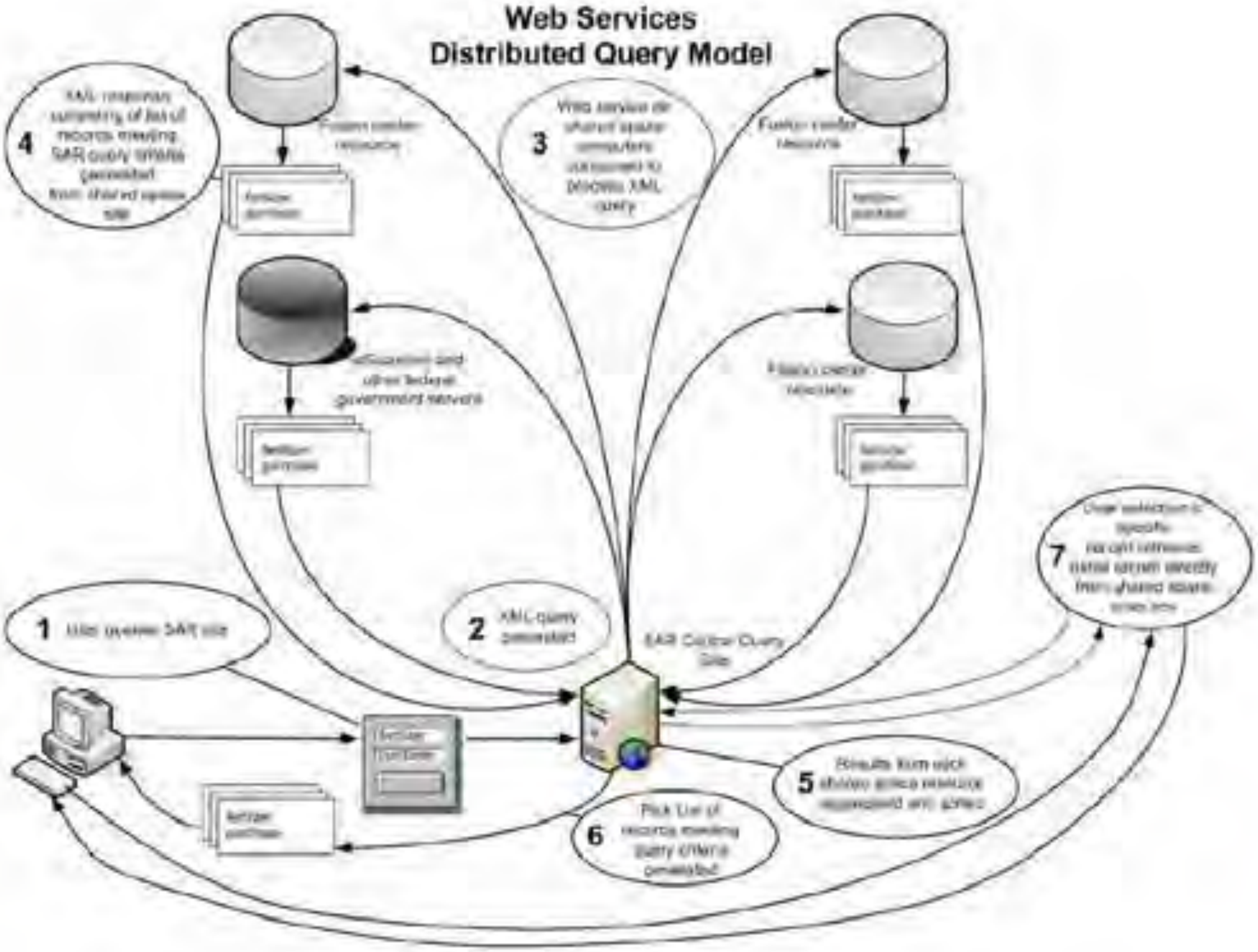
Appendix C



As shown above, the high-level system architecture consists of three major components:

- Front-End Application—Using the NCIRC Portal, a separate set of user screens will be developed to allow users to issue queries against ISE-SAR Shared Spaces and evaluate search results.
- ISE Shared Spaces—This component represents the ISE Shared Spaces and other Shared Spaces, if integrated, hardware and software environments that will reside at each center to process incoming queries of each center's SAR reports contained in a separate SAR database.
- Legacy System—This component represents the ISE-SAR source system that will be used to periodically copy sharable ISE-SAR data into the ISE-SAR Shared Spaces SAR database using a variety of data migration techniques.

Appendix D

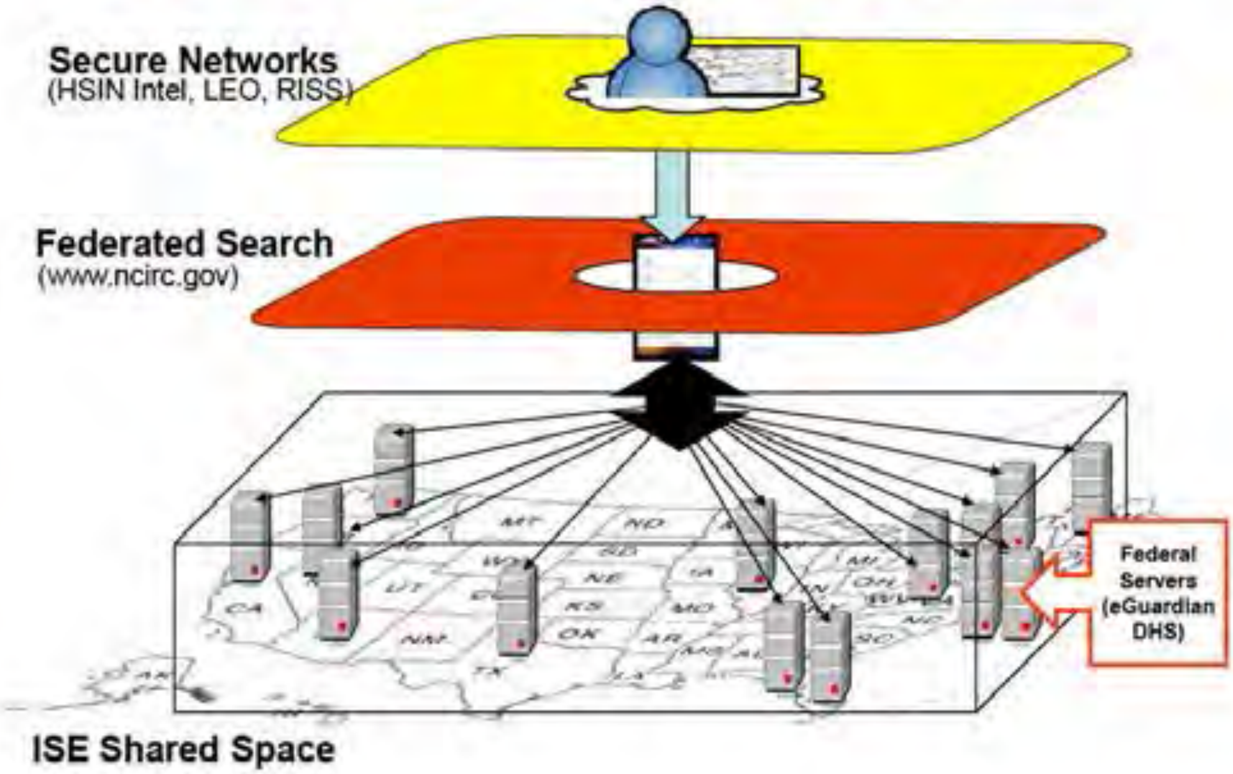

Web Services
Distributed Query Model
4
XML response summary of list of records meeting SAR query criteria generated from shared space site
Fusion center resource
3
Web service on shared space computers … to process XML query
Fusion center resource
… and other federal government networks
Fusion center resource
1
User queries SAR site
2
XML query generated
SAR Central Query Site
7
User selection of specific record retrieves detail record directly from shared space site
5
Results from each shared space resource aggregated and sorted
6
Pick List of records meeting query criteria generated

In the diagram above, the general work flow is illustrated as a series of steps:

1. The user generates a query.
2. The query is translated into an XML document that is forwarded to a Web service application which resides in each center's shared-space environment.
3. The ISE-SAR Shared Spaces Web service processes the query transaction and issues a database query to the ISE-SAR Shared Spaces database.
4. The query results from each ISE shared-space server are sent back to the Portal as a NIEM 2.0-based ISE-SAR document in accordance with the SAR IEPD.
5. The Portal application takes all of the results (from all of the fusion centers) and organizes the material for presentation to the user.
6. Initially, the query results are presented to the user as a pick list showing summary information about the ISE-SAR report.
7. The user can select any record from the pick list of choices (SARs that met the query criteria) and request additional detail about that report.

Appendix E

Conducting a Federated SAR Search



Appendix F: References

Common Terrorism Information Sharing Standards

http://www.ise.gov/pages/ctiss.html

ISE Privacy Guidelines

http://www.ise.gov/pages/privacy-implementing.html

ISE-Suspicious Activities Reporting (SAR) Initiative

http://www.ise.gov/pages/sar-initiative.html

ISE-SAR Functional Standard and Evaluation Environment Initial Privacy and Civil Liberties Analysis

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

Criminal Intelligence Systems Operating Policies (28 CFR Part 23)

http://www.iir.com/28cfr

DOJ *Privacy and Civil Liberties Policy Development Guide and Implementation Templates*

http://it.ojp.gov/documents/Privacy_Guide_Final.pdf

For questions regarding the ISE-SAR Evaluation Environment project, contact:

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

Mr. David Lewis
Senior Policy Advisor
Information Technology Office, Policy Division
Bureau of Justice Assistance
U.S. Department of Justice
[redacted]

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

Global Justice Information Sharing Initiative
United States Department of Justice

Final Report: Information Sharing Environment (ISE)-Suspicious Activity Reporting (SAR) Evaluation Environment

FINAL REPORT:
INFORMATION SHARING ENVIRONMENT (ISE)-
SUSPICIOUS ACTIVITY REPORTING (SAR)
EVALUATION ENVIRONMENT

JANUARY 2010

This project was supported by Grant No. 2008-DD-BX-K480 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the SMART Office, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United States Department of Justice.

TABLE OF CONTENTS

TABLE OF FIGURES

ACKNOWLEDGMENTS

The success of any project is dependent upon strong leadership by both individuals and organizations to ensure that the goals of the project are fully implemented. Leadership was particularly important to this project because of the nationwide nature and underlying activities. We would like to acknowledge the following individuals and organizations for their contributions to the success of the ISE-SAR Evaluation Environment.

A key component of this project was the development of the report *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project.* This report could not have been completed without the leadership of the Major Cities Chiefs Association (MCCA) and, in particular, the work of former ***Chief Gil Kerlikowski***, Seattle Police Department and President of the MCCA; former ***Chief William Bratton***, Los Angeles Police Department; and ***Sheriff Douglas Gillespie***, Las Vegas Metropolitan Police Department.

The Intelligence Commanders from MCCA played a valuable role in developing the findings and recommendations that served as the foundation for the policies and procedures implemented during the ISE-SAR Evaluation Environment. Four agencies volunteered to have their suspicious activity reporting processes assessed and used as the basis for developing the findings and recommendations. These Intelligence Commanders were ***Commander Joan McNamara***, Los Angeles Police Department; former ***Commander David Sobczyk***, Chicago Police Department; former ***Deputy Superintendent Earl Perkins***, Boston Police Department; and ***Major Michael Ronczkowski***, Miami-Dade Police Department.

This project originally started as an effort to connect 3 state fusion centers so that they could share their suspicious activity reporting with each other. The project later expanded to include 9 other major cities, which together made up the 12 participating agencies in the ISE-SAR Evaluation Environment. The leadership of these state fusion center directors—***Captain Doug Keyer***, New York State Police; ***Lieutenant Lee Miller***, Virginia State Police; and ***Chief of Statewide Intelligence Jennifer Cook-Pritt***, Florida Department of Law Enforcement—was important to the initial stages of the project. In addition to the agencies mentioned above, the following persons provided vital leadership in implementing this project: ***Lieutenant Tom Monahan***, Las Vegas Metropolitan Police Department; ***Lieutenant Robert Montalvo***, Houston Police Department; ***Commander Dan Wells***, Arizona Department of Public Safety; ***Lieutenant Ron Leavell***, Seattle Police Department; and ***Director Jeff Wobbleton***, Washington, DC, Metropolitan Police Department.

Training was an essential element in the success of the ISE-SAR Evaluation Environment. Three organizations participated in developing three levels of training that were delivered to members of the participating agencies. The *International Association of Chiefs of Police* developed the line officer training, the *Major Cities Chiefs Association* developed the executive training, and the ***Institute for Intergovernmental Research***® developed the analytic training.

The development of technology and ongoing support for the participating agencies was essential to the successful implementation of the Evaluation Environment. The ***IJIS Institute*** and ***Tetrus Consulting*** provided vital technical support to the project and assisted the participating agencies in connecting their existing systems to the ISE-SAR Shared Spaces.

The ISE-SAR Evaluation Environment would not have been possible had it not been for the work of a select group of state and local officials who earlier had developed a set of standardized data elements that needed to be shared among agencies. These standards were incorporated into the "Information Exchange Package Document for the Suspicious Activity Report (SAR) for Local and State Entities." Key state and local participants and the agencies they represented at the time of this effort were ***Dan Anderson***, Collier County, Florida, Sheriff's Office; ***Norm Beasley***, Maricopa County, Arizona, Sheriff's Office; ***George Bivens***, Pennsylvania State Police; ***Roger Bragdon***, Spokane, Washington, Police Department (retired); ***Ernest Chambers***, Las Vegas Metropolitan Police Department; ***Bryan Costigan***, Montana Department of Justice; ***Scott Dutton***, Georgia Bureau of Investigation; ***Robert Fox***, Los Angeles Joint Regional Intelligence Center; ***Bill Harris***, Delaware State Police; ***Michael Haslip***, Blaine, Washington, Police Department; ***Bart Johnson***, New York State Police; ***Lance Ladines***, Washington State Patrol; ***Lloyd Michaud***, Utah Department of Public Safety; ***Ted Oakley***, Ohio Association of Chiefs of Police; ***Lisa Palmieri***, Massachusetts State Police; ***Daniel Perales***, Houston, Texas, Police Department; ***Russell Porter***, Iowa Department of Public Safety; ***Steven Raubenolt***, Ohio Law Enforcement Gateway; ***Larry Shaw***, Florida Department of Law Enforcement; ***Jim Slater***, Massachusetts State Police; ***Chief Gary Vest***, Powell, Ohio, Police Department; ***Mike Wells***, New York State Police; and ***Gary Williams***, Los Angeles, California, Police Department.

This project represented a unique partnership between many federal agencies with terrorism related responsibilities and state and local law enforcement agencies. The common desire to protect our communities was tantamount and led to common understandings and protocols for effectively and efficiently sharing terrorism related suspicious activity information. The federal partners involved in the project were: the **U.S. Department of Justice (DOJ), Bureau of Justice Assistance (BJA)**; the **Federal Bureau of Investigation (FBI)**; the **U.S. Department of Homeland Security (DHS)**; the **Program Manager, Information Sharing Environment (PM-ISE)**; **DOJ's Global Justice Information Sharing Initiative (Global), Criminal Intelligence Coordinating Council (CICC)**; and the **U.S. Department of Defense (DoD)**,

Executive Summary

The design and development of the Information Sharing Environment Suspicious Activity Reporting Evaluation Environment (ISE-SAR EE) stemmed from five key factors: a national need for increased information sharing of suspicious activity; a need for an enhanced technology solution to address many of the previous information sharing impediments; a requirement to continuously protect privacy and civil liberties; a recognized need to develop a nationwide SAR training program; and a need for the existence of a robust, collaborative partnership among all federal, state, and local ISE-SAR EE participants to create a nationwide SAR program. Combining these factors has created a project that engages 12 state and major urban area fusion centers in an all-crimes approach to gathering, processing, reporting, and sharing of suspicious activity based upon behaviors identified to be reasonably indicative of preoperational planning related to terrorism or other criminal activity. Beginning October 1, 2008, the ISE-SAR EE initiative initiated several core elements to prepare for the implementation of the project. These elements included the evaluation of the status of the current SAR environment within the participating agencies, developing robust business processes for the initiative, and designing and implementing the technology to support the ISE-SAR EE. At the conclusion of the initiative, September 30, 2009, the ISE-SAR EE had created a dynamic approach to information sharing that leverages existing operational processes, technology, and policies. This summary provides an overview of the five key factors and selected lessons learned and recommendations relating to the gathering, processing, and sharing of terrorism-related suspicious activity.

Information Sharing: A National Priority

The recognized need to advance the sharing of terrorism-related law enforcement information was clearly articulated in the Intelligence Reform and Terrorism Prevention Act of 2004 and in several national-level documents, such as the *National Strategy for Information Sharing* (NSIS), issued to reinforce, prioritize, and unify our nation's efforts to advance the sharing of terrorism-related information among federal, state, and local government entities; the private sector; and foreign partners. The primary purpose of this initiative is to identify those behaviors that are reasonably indicative of preoperational planning related to terrorism or other criminal activity and coordinate the sharing of information with the appropriate fusion center and the FBI's Joint Terrorism Task Forces. The NSIS calls for the federal government to support a nationwide capability for the gathering, analysis, and sharing of information, including suspicious activity and incident reporting related to terrorism, with state and local governments and across the federal government. Consistent with the NSIS and as a priority for the establishment of the ISE, the Office of the Program Manager for the Information Sharing Environment (PM-ISE); the U.S. Department of Justice (DOJ); the U.S. Department of Homeland Security (DHS); the Office of the Assistant Secretary of Defense for Homeland Defense and America's Security Affairs, U.S. Department of Defense (DoD); and the Office of the Director of National Intelligence (ODNI) have coordinated a comprehensive effort to develop a nationwide network of state and major urban area fusion centers. This network is one of the foundational pieces of the ISE-SAR EE in identifying fusion centers to participate in the project.

Additionally, the *Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Functional Standard* (ISE-SAR Functional Standard)[1] was released by the PM-ISE to build upon, consolidate, and standardize nationwide aspects of those ISE-relevant activities already occurring at the federal, state, and local levels with respect to the processing, sharing, and use of suspicious activity information. The ISE-SAR Functional Standard continues to evolve and provides guidance on a limited end-to-end information sharing process. It was developed for the analysis of SARs and includes the business rules for gathering, documenting, processing, and sharing terrorism-related suspicious activity information. Ultimately, the ISE-SAR Functional Standard was used to outline the scope, objectives, and goals of the ISE-SAR EE.

The ISE-SAR EE project began with the implementation of three state fusion center pilot sites—the New York State Intelligence Center, the Florida Fusion Center, and the Virginia Fusion Center. Additional sites were added to the Evaluation Environment, including the Washington, DC, Metropolitan Police Department; the Seattle Police Department; the Los Angeles Police Department; the Boston Police Department; the Chicago Police Department; the Miami-Dade Police Department; the Arizona Counter Terrorism Information Center; the Houston Police Department; and the Las Vegas Metropolitan Police Department. Additionally, the eGuardian system, designed by the Federal Bureau of Investigation (FBI), participated in the ISE-SAR Evaluation Environment, as well as DHS. eGuardian also serves as the connection between the FBI's Joint Terrorism Task Force and the ISE-SAR Shared Spaces Servers. Similar to how eGuardian functions as one of the ISE-SAR Shared Spaces, SAR information from DHS will function as an ISE-SAR Shared Space.

MULTILAYERED TRAINING

The design and implementation of a cohesive national ISE-SAR training program were vital parts of the final project design. The training component was developed through the recognition that the ISE-SAR EE must provide a consistent, nationwide message concerning the handling of SARs. To reinforce the tenets of the project, three separate but coordinated training efforts were developed targeting law enforcement professionals with varying duties and responsibilities—agency executives, analytic/investigative personnel, and line officers. The executive-level training was developed by the Major Cities Chiefs Association (MCCA) and focuses on executive leadership, policy development and privacy and civil liberties protections, agency training, and community outreach. The analyst/investigative-level training was developed by the Bureau of Justice Assistance (BJA) and focuses on the SAR process, with an emphasis on review and vetting of information to ensure compliance with

[1] See http://www.ise.gov/pages/sar-initiative.aspx.

the ISE-SAR Functional Standard; privacy and civil liberties protections; terrorism indicators, including recent trends in terrorism, stages of terrorism, and behaviors tied to the ISE-SAR Criteria Guidance; and resources and tools. The line officer training was developed by the International Association of Chiefs of Police (IACP) and focuses on understanding the critical role line officers have in the effective implementation of the SAR process. The goal of the training efforts is to facilitate agency implementation of the SAR process and to enhance the nationwide SAR capability.

Protection of Privacy and Civil Liberties

The third critical aspect of this initiative is the continuous need to emphasize the importance of protecting privacy rights and civil liberties. Integral to this project, which often includes sensitive personal information, is the protection of Americans' privacy, civil rights, and civil liberties. In addition to the U.S. Constitution, many laws and policies protect these important rights, including the Privacy Act of 1974; the E-Government Act of 2002; and other federal laws, executive orders, and policies, as well as state, local, and tribal constitutions, laws, and policies. During September 2008, the PM-ISE—in consultation with the Civil Liberties and Privacy Office of ODNI, the Office of Privacy and Civil Liberties of DOJ, the DHS Office of Privacy, and the Legal Issues Working Group of the ISE Privacy Guidelines Committee—prepared the Initial Privacy and Civil Liberties Analysis of the ISE-SAR EE. Based on this analysis, the *ISE-SAR Evaluation Environment Privacy, Civil Rights, and Civil Liberties Protection Policy Template* was finalized and approved for distribution to the EE participants in January 2009. Based on the work of DOJ's Global Justice Information Sharing Initiative's (Global) privacy document, *Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Template*, the template was designed to cover all ISE-SAR EE activities conducted by participating pilot sites, including source, submitting, and use agencies. It was designed in such a manner that participating agencies can make any necessary modifications to include the requirements of their state constitution, executive orders, court decisions, statutes, rules and regulations, and local codes/ordinances as they develop their individual agency privacy policies. The policy template requires each participating agency to address specific items: purpose specification, collection limitation, data quality, use limitation, security safeguards, openness, individual participation, and accountability. Prior to participating in the ISE-SAR EE and sharing information, all agencies had to develop and implement a privacy framework that met the minimum guidelines provided in the privacy template.

The ISE-SAR EE was designed, in accordance with the ISE-SAR Functional Standard, to consider privacy throughout the SAR process. The ISE-SAR Functional Standard requires a four-part review before any SAR information can be shared in the ISE-SAR Shared Spaces. This review process includes an analytic judgment as to the information's relevance to terrorism, identification of specified activity, reliability, and validity. In addition to and compliant with the direction of the project sponsors, extensive training regarding the criticality of the protection of privacy and civil liberties has been provided to the participating agencies whose role requires analysis of suspicious activity and the ultimate determination as to the level of sharing of that information.

Technology: A Way Forward

The second key factor of the project is the ability to enhance information sharing through the creative use of technology. Throughout the law enforcement community, the need to share information is generally accepted and understood; however, the technology used for many information sharing initiatives often fails to gain wide support due to its failure to meet the expectations of the law enforcement agencies. Some of these expectations include the ability to self-populate the data that is shared, the ultimate control and disposition of the agency's data, and the ability to utilize the existing legacy records management system. The ISE-SAR EE was designed to utilize a unique technology configuration that allows data sharing through a distributed model in compliance with the National Information Exchange Model (NIEM) standards, which emphasize the importance of maintaining the originating agency's ownership of the data. Additionally, this technology solution leveraged existing state and local systems as well as national information sharing platforms, minimizing the need to develop a new system or database.

Technology is often seen as an impediment to information sharing due to the stand-alone nature of many law enforcement records management systems. The ISE-SAR EE utilized a unique technology approach by implementing a "shared space" environment. This technology solution provides a distributed data model to make SAR information available through Common Terrorism Information Sharing Standards, applications, and services. The ISE-SAR Shared Spaces allow authorized users to securely search the ISE-SAR data located on local agency-controlled servers from one central location—the National Criminal Intelligence Resource Center. The ISE-SAR Shared Spaces integrate the NIEM standard and the ISE-SAR Functional Standard into a standardized process to efficiently and effectively share information. Each state and major urban area can develop a plan for the sharing of SARs based upon the technology that it decides best meets its operational needs.

Collaborative Partnerships to Develop a Nationwide SAR Program

The final key to this initiative is the collaborative and dynamic partnerships among the federal sponsors and state and local sites. Through conference calls, user group meetings, and site visits, the ISE-SAR EE partners maintained an aggressive project timeline and commitment to establish the project at each site. Moreover, it was the supportive aspects of this partnership, such as cross-agency collaboration, that ultimately made the project a success. The federal partners—PM-ISE, DOJ, BJA, DoD, the FBI, and DHS—worked together to develop the foundational elements of the project. The involvement of multiple federal agencies in this coordinated effort will help ensure that relevant pieces of information that may be indicative of a terrorist event or activity are shared.

This project created new and enhanced existing partnerships among the state and local ISE-SAR EE participant sites. Working with their federal partners, these agencies articulated a common need for a unified SAR process. Throughout the implementation, the users provided constructive feedback and recommendations to improve the initiative. Partnerships within the larger law enforcement community have also proved to be critically important to the achievement of the project goals. An important factor in the development of the project was the leadership of the MCCA and its Major Cities Chiefs Intelligence Commanders Working Group. Using the tenets of the successful Los Angeles Police Department SAR initiative, the MCCA and its working group provided leadership and guidance in the development of standard processes and policies to guide the sharing of SAR information. Further, in June 2008, to illustrate their support of the project, both the MCCA and the Major County Sheriffs' Association unanimously passed resolutions supporting the implementation of the SAR process within their member agencies. Additionally, the National Sheriffs' Association, the IACP, the FBI, the Criminal Intelligence Coordinating Council (CICC), and Global[2] have endorsed this project.

KEY RECOMMENDATIONS

A number of recommendations were made by the participating agencies based upon the lessons learned from the Evaluation Environment.[3] The key recommendations were:

> **Leadership:** Prior to initiating the next phase of this project, the project team must ensure that each agency has the support of its executive leadership. This can be accomplished through regular briefings to law enforcement associations and through the MCCA's Chief Executive Officer Briefing. Face-to-face briefings are important to allow agency executives to understand the full scope of the project and the requirements and resources necessary from their agency.
>
> **Policy and Common Processes:** If the ISE-SAR EE is expanded, future participating agencies should develop policies and processes that govern the processing of SARs within all areas of their agency. This will ensure compliance with the ISE-SAR Functional Standard and related project resources. It is understood that each agency will have unique requirements, but a common set of processes across the initiative is needed.
>
> **Privacy:** Future participating agencies should continue to be required to have a privacy framework that is consistent with the ISE Privacy Guidelines. Agencies should ensure transparency and openness in their privacy policy development

[2] In June 2008, the *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project* (SAR report) was developed to provide recommendations to the CICC from the MCCA. The SAR report was unanimously approved by the CICC in September 2008 and by Global in October 2008.

[3] Additional information and background regarding each of the recommendations and lessons learned can be found within the full report.

efforts by engaging privacy advocates and community leaders as the policies are developed or refined.

Technology: The proposed program management office should evaluate the best method of deploying operating systems and examine the pros and cons of other programming languages. Specific training courses or targeted technical assistance should be identified to help site staff improve their technical system administration capabilities.

Training: The executive, analytic, and line officer training programs should be delivered to all agencies that are developing a SAR process and will participate in the Nationwide SAR Initiative (NSI). Varied methods of delivery—including CD-based training, Web-based training, and video streaming—should be considered as delivery mechanisms for these courses.

Outreach: Agencies engaged in a SAR program should train their Liaison Officers to assist in public, private sector, and law enforcement outreach and awareness opportunities. Providing additional training to officers utilizing the *Safeguarding America* DVD and providing additional outreach material to the officers to interact with the public and private sectors will provide greater awareness of behaviors indicative of potential terrorism activity.

Next Steps

Moving forward, the technology, training design, types of technical assistance support offered, and business processes developed during this project can be replicated for the sharing of other types of criminal activity information. Based on feedback received from the 12 participating state and local agencies, the ISE-SAR EE has proved successful in providing law enforcement agencies with a reliable and consistent method of sharing terrorism-related SARs, and this type of project can be expanded to other law enforcement activities. The following sections are contained in the full report:

- Project Overview and Background
- Leveraging Promising Practices
- Lessons Learned
- Appendices:
  - Appendix One: Project Participants
  - Appendix Two: Project Timeline
  - Appendix Three: Acronyms and Abbreviations
  - Appendix Four: Participating Agency Assessments
- Contacts for Questions

PROJECT OVERVIEW AND BACKGROUND

> *Chief Cathy Lanier, DC Metro: "The hope is that everyone across the country will start doing this. The value of this program lies in the number of people that buy in and participate."*

The exchange of information is a critical component of law enforcement investigative efforts. Exchanging information becomes even more important when crime prevention becomes multijurisdictional. The ability to share information in a consistent and timely manner across jurisdictional boundaries is a key element to the law enforcement process. Historically, gaps in information sharing among federal, state, and local law enforcement agencies have hindered law enforcement's ability to effectively and efficiently detect, deter, prevent, and respond to criminal and terrorist events. Information sharing gaps often stem from the fact that although law enforcement agencies individually may have pieces of information concerning criminals or terrorists and their activities, these agencies often lack a standardized mechanism by which information can be exchanged with other agencies and/or collected to support crime detection and prevention. Consequently, the law enforcement community's efforts to prevent crime or respond to a criminal or terrorist incident may be fragmented, duplicative, and/or limited.

Addressing these issues, the *National Strategy for Information Sharing* (NSIS) was released in October 2007 to prioritize and unify our nation's efforts to advance the sharing of terrorism-related information among federal, state, and local government entities; the private sector; and foreign partners while continuing to protect privacy, civil rights, and civil liberties. The NSIS calls for the federal government to support a nationwide capability for the gathering, analysis, and sharing of information, including suspicious activity and incident reports related to terrorism, with state and local governments and across the federal government. The development of the NSIS was based on several foundational documents, including the report of the National Commission on Terrorist Attacks Upon the United States,[4] also known as the 9/11 Commission, which identified a breakdown in information sharing as a key factor contributing to the failure to prevent the September 11, 2001, attacks. In response to the 9/11 Commission's recommendations, Congress passed—and the President signed—the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). Per Section 1016, the Information Sharing Environment (ISE) was created and is defined as "an approach that facilitates the sharing of terrorism and homeland security information." Further, the IRTPA required the President to designate a Program Manager for the ISE and establish the Office of the Program Manager for the Information Sharing Environment (PM-ISE). The PM-ISE has government-wide authority to manage the ISE, assist in the development of ISE standards and practices, and monitor and assess its implementation by federal agencies as well as state and major urban area fusion centers.

[4] See http://www.9-11commission.gov.

Consistent with the IRTPA, the ISE sought an information sharing solution that would allow data to be shared through a distributed mechanism by which law enforcement agencies could retain data ownership and control. The solution would need to be economically developed and deployed, ideally with the ability to be easily replicated nationwide.

Consistent with the NSIS and as a priority for the establishment of the ISE, the PM-ISE—in conjunction with the U.S. Department of Justice (DOJ), Bureau of Justice Assistance (BJA); the Federal Bureau of Investigation (FBI); the Office of the Assistant Secretary of Defense for Homeland Defense and America's Security Affairs, U.S. Department of Defense; and the U.S. Department of Homeland Security (DHS)—supported a comprehensive effort to develop a nationwide network of state and major urban area fusion centers. One of the goals of this integrated network is to facilitate the sharing of terrorism-related information across federal, state, and local communities. The information to be shared in this national network includes information based on an everyday activity of most law enforcement agencies: documenting suspicious activities observed or reported. This practice is well-institutionalized in the law enforcement community and occurs with varying degrees of standardization and formality in other communities, such as in the public health and private sectors. Throughout most communities, the reporting of SARs is not represented by a formalized, institutional process, and there is typically no established mechanism for the reporting of preoperational terrorism behaviors. Leveraging the existing SAR collection functions, the ISE-SAR Evaluation Environment (EE) recognized a broader mission need. Accordingly and consistent with the direction in the NSIS, it was deemed necessary to establish a standardized process that includes flexibility to meet the unique individual requirements of the jurisdiction in the area of privacy protection and associated data models for identifying, documenting, and sharing terrorism-related suspicious activity reports (SARs) to the maximum extent possible (initially referred to as the SAR initiative).

> *Former Chief William Bratton, LAPD: "We have learned from the past that there are early warning signs. Terrorism and behaviors are linked. How do I maximize our efforts and multiply our force? Analysis is critical to differentiate criminal from terrorist activity.... We all need to assess our vulnerability. Similarly with SAR—we need a united front and leadership support so that every agency in the area is contributing. If we don't have a seamless Web and some agencies are not cooperating, we are in trouble. The effort today is not only to educate but to enlist your support and make sure you understand the importance to this effort. We want to move in a big and aggressive way to move this issue forward. We hope those of you here 'get it.' This is not a departure from what we normally do—there are some enhancements—we want you to take it to your people. Embrace the concept and appreciate the enhancements."*

In October 2006, a foundational meeting was held in Denver, Colorado, to bring together state and local subject-matter experts, as well as the federal project partners, to discuss the initial plans for the development of what would eventually become the ISE-SAR EE. In response to the need of the state and local law enforcement community to develop a standardized SAR reporting process, this meeting highlighted the need to build the project using a common set of behavior-specific categories that can be related back to the precursors of terrorism.

From the beginning of this initiative, it was evident that there was a need to leverage existing technology standards, such as the National Information Exchange Model (NIEM).[5] NIEM is based on the work of the Global Justice Information Sharing Initiative's XML Data Model and is designed to develop, disseminate, and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations, as well as support the day-to-day operations of agencies throughout the nation. NIEM enables information sharing, focusing on information exchanged among organizations as part of their current or intended business practices. The NIEM exchange development methodology results in a common semantic understanding among participating organizations and data formatted in a semantically consistent manner. NIEM standardizes content (actual data exchange standards) and provides tools and managed processes.

In early 2007, the project discussions continued with a series of conference calls and WebEx meetings to further develop the project's behavior codes, business processes, and implementation strategies. These efforts continued with the development of a reference Information Exchange Package Documentation (IEPD) intended to support SAR exchanges between and among fusion centers and their federal, state, local, and tribal law enforcement partners. Developed by state and local stakeholders, the IEPD was ultimately enhanced to be consistent with the ISE Privacy Guidelines and the *Privacy and Civil Liberties Policy Development Guide and Implementation Templates.* The development of the IEPD ultimately resulted in the development of the ISE-SAR Functional Standard.

Commissioner Gerald Bailey, Florida Department of Law Enforcement: "Law enforcement has excellent information gathering techniques and skills in place. However, in order for that information to be useful, it must be shared. Simply put, the heart of this initiative is to glean information from routine police work for the fusion centers so that they may provide the analysis and intelligence that is critical to our efforts against crime and terrorism. We can no longer operate as 50 independent states, but as one country with one goal—to keep our citizens safe."

In January 2008, the first ISE-SAR Functional Standard was released by the PM-ISE to build upon, consolidate, and standardize nationwide aspects of those ISE-relevant activities already occurring at the federal, state, and local levels with respect to the

[5] See www.it.ojp.gov/iepd.

processing, sharing, and use of suspicious activity information. The ISE-SAR Functional Standard provides guidance on a limited end-to-end information sharing process and continues to be enhanced to meet the needs of the agencies. It was developed for the analysis of SARs and includes the business rules for gathering, documenting, processing, and sharing terrorism-related suspicious activity information. These efforts ultimately resulted in the development of the ISE-SAR EE, which was used to outline the scope, objectives, and goals of the project, including the implementation of the SAR Summary Reports Library Pilot Project and SAR Operational Study Evaluation Project (now known as the ISE-SAR Evaluation Environment [ISE-SAR EE]).

The Evaluation Environment officially began on September 1, 2008, and concluded on September 30, 2009. The purpose of the Evaluation Environment (EE) at state and major urban area fusion centers and local law enforcement organizations was to test and evaluate the policies, procedures, and technology needed to implement a unified process that fosters a broader sharing of SARs that are reasonably indicative of potential intelligence gathering or preoperational planning related to terrorism or other criminal activity. The project was developed in a phased approach beginning with the development of privacy frameworks and the implementation of the technology. The first data was not shared until May of 2009. The participating agencies continue to implement the processes and procedures needed to successfully share SAR information.

Sheriff Gillespie, Las Vegas Metro Police Department: "The strength [of the NSI] is in partnering and the common mission. Today, we face unique challenges in law enforcement not only from the traditional aspect. We cannot allow the human trust aspects to interfere with the actions we must take. This is a VERY worthwhile approach to information sharing, and I look forward to utilizing it in southern Nevada."

The SAR Summary Reports Library was a conceptual pilot project that provided a collection point for existing SAR summary or free-text narrative information reports. The Library pilot was designed to provide a method for fusion centers and other authorized individuals (e.g., sworn law enforcement and analysts) to enter, store, and access SAR documents (e.g., Summary SARs, Daily Briefs, and Weekly Analytic Reports), regularly created and published by fusion centers and other contributing agencies. Because of the need to concentrate on the larger ISE-SAR EE rollout, the full implementation of the Library project was suspended in order to focus on the primary purpose of the project. However, the development of the Library project and its initial testing demonstrated the potential success of the technology design and provided a viable tool for further applications.

The ISE-SAR EE operated on the concept of "Shared Spaces," which is an idea consistent with the guidance provided in the IRTPA. The Shared Spaces concept uses a networked and distributed information exchange process to make standardized terrorism-related information available through Common Terrorism Information Sharing

Standards,[6] applications, and Web Services. Ultimately, the ISE-SAR EE, through the use of the Shared Spaces concept, provides a solution for law enforcement agencies to share terrorism-related suspicious activity information, while continuing to maintain control of their data through a distributed model of information sharing.

In December 2008, a short-term study was conducted with some of the participants to determine the value of including personally identifying information (PII) data in the search results versus querying data with no PII included. The study was conducted with data from the Florida Fusion Center and the New York State Intelligence Center. When a query was made, the analyst was requested to complete a series of questions to determine the value of the information provided. The results of this study showed that data containing PII information had more value to the user than data without PII. Additionally, a focus group was established at the conclusion of the study, and the participants confirmed the value of including PII data in the ISE-SAR EE.

Chief Harold Hurtt, Houston Police Department: "If you're not committed to it [the NSI] at the top of your organization, it's not going to happen. The officers may be introduced to it, but if there's not interest from the chief or the person at the top of the organization, it won't be done properly and won't be processed and will really be wasting a lot of government funding. Hopefully, we look at this as a program for the Houston region. We talk about homeland security, but this is also about hometown security… and it would behoove all of us to protect our communities…. What we do every day is important, and we're going to step up to the plate—it's as simple as that. We need to be able to count on each other."

In early 2008, development began on the *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project* report. This report was developed to provide recommendations to the Criminal Intelligence Coordinating Council (CICC) from the Major Cities Chiefs Association (MCCA). The findings and recommendations regarding the gathering, processing, reporting, analyzing, and sharing of suspicious activity (also referred to as the SAR process) were developed through site visits with police departments in Los Angeles, California; Chicago, Illinois; Boston, Massachusetts; and Miami-Dade, Florida. These agencies provided this information to a SAR subject-matter expert team, who documented the agencies' processes. The subject-matter expert teams were selected by the sponsoring agencies—BJA, DOJ, MCCA, Global, CICC, DHS, and the FBI. After the site visits, the *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project* report was further developed by the SAR Executive Steering Committee, which was composed of local, state, and federal agencies representing the CICC, the Global Advisory

[6] Additional information on Common Terrorism Information Sharing Standards is available at http://www.ise.gov/pages/ctiss.aspx.

Committee (GAC), and the MCCA. Promising practices from these site visits were identified and are detailed throughout this report.

In July 2008, police chiefs, sheriffs, and intelligence commanders from more than 25 major cities and counties and representatives from several federal agencies met in Las Vegas, Nevada, to discuss the implementation of the *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project*. Held in conjunction with the Major Cities Chiefs Intelligence Commanders meeting and led primarily by state and local stakeholders, this meeting focused on the further development of foundational issues such as activity classification codes, privacy framework, and training recommendations. Based on the outcomes and recommendations from this meeting, the project partners were able to reconcile the behavior codes existing within the state and local agencies with those codes enumerated in the ISE-SAR Functional Standard. The privacy recommendations identified during the meeting included the requirement for each participating agency to have a privacy framework. The group also advocated for continued project transparency through the inclusion of privacy and civil liberties advocates where feasible. Recommendations from the training committee focused on the development of the three levels of training—for line officers, analysts, and executives.

Mr. Michael Heimbach, Assistant Director, Counterterrorism Division, FBI: "[eGuardian] will allow [a suspicious activity report] to be vetted through its own police department, with the proper approvals put into the. . .system, and then it sits there, and then we have a mechanism to potentially connect the dots. Because if somebody is filming a power plant facility on the East Coast; they talk to the individual, no big deal, find no derogatory information, no threat concern, and close it out. But it goes in the system. But then the same individuals, or a car used by the individuals, shows up at the Hoover Dam. Now we're saying, 'Okay, what's going on here?' That's the important thing. Today it may not link, but five years or ten years from now, it could link."

Following approval by the GAC and the CICC, the *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project* was released in October 2008. The report and its recommendations establish national guidance for state, local, and tribal agencies to facilitate the improved sharing of SAR information. The report advocates that agencies use their existing processes and technology as they implement the SAR process at their agency.

The *Suspicious Activity Reporting Process Implementation Checklist* was released in November 2008 as a companion document to the *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project* report. Working with state and local subject-matter experts to identify the major SAR process categories impacting their operations and processes, this document provides a simplified checklist for chief executives and senior leadership. It is designed to be used as agencies develop an internal SAR process; aids in their crime prevention efforts; and assists with successfully incorporating state, local, and tribal agencies into the nationwide SAR process.

Throughout the project, strong partnerships were developed. In 2008, both the Major Cities Chiefs Association and the Major County Sheriffs' Association unanimously passed resolutions supporting the implementation of the SAR process within their member agencies to illustrate their support of the project. Additionally, the National Sheriffs' Association, the International Association of Chiefs of Police, the FBI, the CICC, and DOJ's Global[7] have endorsed this project.

On December 23, 2008, the *Nationwide SAR Initiative Concept of Operations*[8] (NSI CONOPS) was released by the PM-ISE. This document provides top-level operational guidelines for the gathering and processing, analysis and production, and dissemination of SARs. Additionally, the NSI CONOPS describes a comprehensive approach that includes not only the ISE-SAR Shared Spaces concept but also the integration of federal agencies, such as FBI's eGuardian system and DHS's suspicious activity reporting systems, as part of the NSI. The NSI CONOPS defines the requirements of the project and associated implementation activities, including areas such as:

- Description of the overall ISE-SAR process and multiple ISE-SAR-related activities in sufficient detail to ensure that these activities adhere to standard approaches and that all embody adequate protection for privacy and civil liberties.
- Clarification of the role of the ISE-SAR EE as a microcosm of the broader NSI.
- Description of the roles, missions, and responsibilities of NSI participating agencies and the top-level NSI governance structure.

Using the NSI CONOPS document, the partner agencies of DHS, DOJ, the FBI, PM-ISE, and the Office of the Assistant Secretary for Homeland Defense and America's Security Affairs, in support of the U.S. Department of Defense force protection/anti-terrorism mission, created the foundation for the NSI. Furthermore, these agencies aligned their SAR policies and procedures with the NSI process.

[7] In June 2008, the *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project* (SAR report) was developed to provide recommendations to the CICC from the MCCA. The SAR report was unanimously approved by the CICC in September 2008 and by Global in October 2008.

[8] See http://www.ise.gov/docs/sar/NSI_CONOPS_Version_1_FINAL_2008-12-11_r5.pdf.

Figure 1 describes the NSI process:[9]

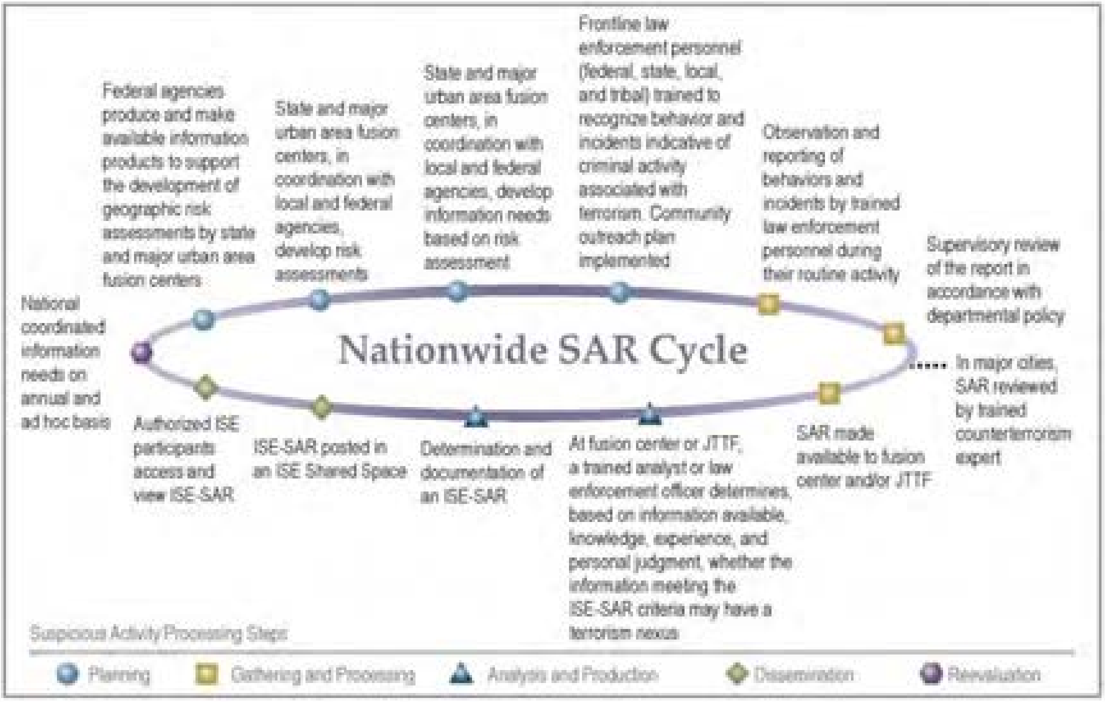

Federal agencies produce and make available information products to support the development of geographic risk assessments by state and major urban area fusion centers
State and major urban area fusion centers, in coordination with local and federal agencies, develop risk assessments
State and major urban area fusion centers, in coordination with local and federal agencies, develop information needs based on risk assessment
Frontline law enforcement personnel (federal, state, local, and tribal) trained to recognize behavior and incidents indicative of criminal activity associated with terrorism. Community outreach plan implemented
Observation and reporting of behaviors and incidents by trained law enforcement personnel during their routine activity
Supervisory review of the report in accordance with departmental policy
National coordinated information needs on annual and ad hoc basis
Nationwide SAR Cycle
In major cities, SAR reviewed by trained counterterrorism expert
Authorized ISE participants access and view ISE-SAR
ISE-SAR posted in an ISE Shared Space
Determination and documentation of an ISE-SAR
At fusion center or JTTF, a trained analyst or law enforcement officer determines, based on information available, knowledge, experience, and personal judgment, whether the information meeting the ISE-SAR criteria may have a terrorism nexus
SAR made available to fusion center and/or JTTF
Suspicious Activity Processing Steps
Planning
Gathering and Processing
Analysis and Production
Dissemination
Reevaluation

FIGURE 1: NSI PROCESS

In late 2008, three fusion center sites—New York, Florida, and Virginia—were prepared to begin the Shared Spaces pilot; however, due to delays in finalizing the site privacy policies, the pilot was not immediately made operational. Initial proof-of-concept success occurred during the preparation for the 2009 Presidential Inauguration. The Washington, DC, Metropolitan Police Department and its fusion center—Washington Regional Threat and Analysis Center—installed Shared Space servers and created a collection of potential suspicious activity reports. The SARs were then entered into the FBI's eGuardian system. This partial implementation was accompanied by training for the executive leadership, analysts, and line officers within the agency. Significantly, the Washington, DC, pilot project and training material were thoroughly reviewed by representatives from privacy advocacy groups. The input from this review, as well as input received during the Privacy and Civil Liberties Dialogue meeting (held September 2008) provided input which was used to strengthen the ISE-SAR EE training programs and Functional Standards. The implementation of the SAR process in Washington, DC, provided valuable evidence to support the continuance of the initiative.

[9] Ibid.

On January 9, 2009, the *Information Sharing Environment (ISE)-Suspicious Activity Reporting (SAR) Evaluation Environment Implementation Guide* (Implementation Guide)[10] was issued after a collaborative effort by federal, state, and local partners and participants of the ISE-SAR EE. The Implementation Guide builds upon the previous SAR project efforts and was developed to assist participating state and local law enforcement agencies with the implementation of the ISE-SAR Shared Spaces. Additionally, the Implementation Guide aids them in understanding the procedures and processes within the ISE-SAR EE and provides in detail:

- Summary and overview of the ISE-SAR EE
- Technology, design assumptions, system security, and implementation
- Project governance, to include privacy and civil liberties protections
- Data access and security policies
- Logs and audits capabilities
- Training and technical assistance

On May 21, 2009, the PM-ISE issued the updated ISE-SAR Functional Standard, Version 1.5,[11] to specifically address the sharing of terrorism-related SARs at all levels of government, with the objective of enabling analysts and officers with counterterrorism responsibilities to discover and identify terrorist activities and trends. This update clarified a number of privacy-related issues and aligned the Functional Standard with the business process description in the NSI CONOPS. The ISE-SAR Functional Standard 1.5 defines *suspicious activity* as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." Such activities could include, but are not limited to, surveillance, photography of facilities, site breach or physical intrusion, cyber attacks, possible testing of security or security response, indications of unusual public health sector activity, unauthorized attempts to obtain precursor chemicals/agents or toxic materials, or other unusual behavior or sector-specific incidents.

Ultimately, the updated ISE-SAR Functional Standard creates guidance for the recommendations in the NSIS and aligns the operational process descriptions within the NSI CONOPS.

[10] The *Information Sharing Environment (ISE)-Suspicious Activity Reporting (SAR) Evaluation Environment Implementation Guide* was provided to all participating agencies and is considered a For Official Use Only document.

[11] Additional information regarding the ISE-SAR Functional Standard can be found at http://www.ise.gov /pages/ctiss.html.

ISE-SAR EE IMPLEMENTATION

The ISE-SAR EE, made up of 12 state and major urban area fusion centers, provided a relatively controlled environment to test the documented ISE-SAR policies, business process, capabilities, architecture, and standards. Additionally, the ISE-SAR EE allowed for the assessment and refinement of processes and capabilities prior to full-scale operation. The objectives of the ISE-SAR EE included, but were not limited to, the following:[12]

- Improve operational processes at federal, state, local, and tribal law enforcement agencies and fusion centers by providing capabilities to document, store, and share terrorism-related SARs.
- Test and validate fundamental ISE Enterprise Architecture Framework[13] concepts and core services.
- Incorporate "lessons learned" and "promising practices" into an implementation guide and template for establishing a nationwide ISE-SAR process.
- Continue to evaluate the need to update the ISE-SAR Functional Standard.

The project was also built upon and continues to place emphasis on the protection of privacy, civil liberties, and civil rights.

Using the Shared Spaces concept, the ISE-SAR EE was introduced in two phases. The first phase, the SAR Operational Evaluation Project, began in September 2007 and involved the design, development, and deployment of hardware, software applications, and network equipment that integrated state fusion centers in Florida, New York, and Virginia into the Shared Spaces.

In September 2008, representatives from the three state pilot sites and potential future pilot site cities met in St. Louis, Missouri, to discuss the ISE-SAR EE.[14] The group discussed the SAR business process, privacy and civil liberties protections, and technology and training related to the SAR project. During this meeting, the project sponsors received commitments from several new sites indicating their willingness to participate in the ISE-SAR EE. The meeting participants received a significant amount of training concerning privacy framework development, personnel roles/responsibilities, and overview of the project implementation guide. The state and local technology points of contact also met with the project technical team to discuss the rollout for each site. As a result of this meeting, the second phase of ISE-SAR EE participants became fully educated on the project, process,

[12] See *Fact Sheet: Establishing a Terrorism-Related Suspicious Activity Reporting Initiative* for additional information (http://www.ncirc.gov/sar/Fact_Sheet_NSI_-_December_23_2008_Final.pdf).
[13] For additional information regarding the *ISE Enterprise Architecture Framework*, see http://www.ise.gov /pages/eaf.aspx.
[14] The participating agencies are listed in Appendix One.

training, and technology. Ultimately, building on the successes of the first Shared Spaces participants, the second phase expanded the project to other major metropolitan law enforcement agencies and regional fusion centers, including Boston, Massachusetts (UASI); Chicago, Illinois (UASI); Houston, Texas (UASI); Las Vegas, Nevada (UASI); Los Angeles, California (UASI); Miami-Dade, Florida (UASI); Phoenix/Arizona (UASI/State); Seattle/Washington (UASI/State); and Washington, DC (UASI). In addition, the federal agencies of DHS and the FBI's eGuardian were included as part of the ISE-SAR EE.[15]

Summary of the ISE-SAR Process

The ISE-SAR EE was designed to test the functionality of the ISE-SAR process in a controlled environment and, if successful, examine the expansion of the NSI across the United States. The ISE-SAR process begins when a frontline law enforcement officer responds to a call for service or self-initiates law enforcement action based on a reported incident/observation or the officer's observation of suspicious behavior. The initiation of this process could also occur when citizens or private sector personnel report some kind of suspicious activity. Many agencies document this data into their records management system, field interviews, or other related processes. This project has not sought to create new systems but rather to leverage the current business processes and automated systems to extract certain data concerning suspicious activity relating to terrorism and make it sharable within the Shared Spaces.

Deputy Chief Clark Kimerer, Seattle Police Department: "The next terrorist attack will be solved by a private citizen, a utility worker, or an observant person that gets to the authorities, that will prevent the loss of life, the crippling of our country. That is why it's so critical that executive leadership make it [the NSI] come about. If I look at the world prior to 9/11 and approaching this threat, we have made incredible strides. We need to recognize that SAR is one of the critical components of this process. People are fatigued with talking about, thinking about, preparing for terrorism. The fact that our interest in 9/11 attenuates—it gets more and more uninteresting as we get farther from 9/11—we do not want to 'nod' at the switch. That's exactly what our enemies want us to do."

The ISE-SAR process, as outlined in the ISE-SAR Functional Standard, sets forth a four-part "integration/consolidation" process for identifying and gathering those activities that have a potential nexus to terrorism. The first part of the process involves ensuring that the activity meets one or more of the criteria detailed in Part B of the ISE-SAR Functional Standard. Developed by state and local counterterrorism experts, these criteria describe behaviors that are indicative of or associated with terrorism. For example, the Los Angeles Police Department (LAPD) researched and developed an extensive set of behavior-specific codes for the reporting of suspicious activity. These codes provided agencies with the method for

[15] The ISE-SAR EE includes the initial 12 sites. It is anticipated that the ISE-SAR EE will be expanded into the Nationwide SAR Initiative and will encompass all 72 fusion centers.

documenting behavioral indicators that have a potential nexus to terrorism. LAPD used the codes to train its personnel in the recognition of suspicious activity. The process was continuing to mature as LAPD conducted research to develop patterns and determine the frequency of use with the codes. For the ISE-SAR EE initiative, additional subject-matter experts from the state and local agencies reviewed the LAPD codes as well as those identified in the Functional Standard. Throughout the project, these behavior codes were consistently mapped and validated to ensure they are representative of the current terrorism threat environment. Additionally, BJA's State and Local Anti-Terrorism Training (SLATT®) Program analyzed and mapped recent terrorism events with the behavior codes for validation of the ISE-SAR EE codes. Based on this research, the SLATT Program is also piloting a searchable Terrorism Incident Database that lists and displays the terrorist events in four formats—chronological, by topic, search engine, and geospatial.

New York State Police Superintendent Harry J. Corbitt: "The same principles that make a neighborhood watch program successful in keeping a neighborhood safe apply on a larger scale to keep municipal, statewide, and national communities safe. If the keystone to success is communication from all eyes and ears of our communities, the foundation is the building and maintenance of trusting relationships between police and the citizens they serve."

The second part of the process involves the review and vetting of the information to ensure that it is both legally obtained and has a potential terrorism nexus. In most agencies, this initial review is completed by a first-line supervisor trained to recognize activity associated with terrorism. The third and fourth steps of the process include an additional vetting step, which requires that all SARs be reviewed by analysts or officers who have been trained to assess the SAR's validity and accuracy. This multilayered review occurs prior to the information being entered into the Shared Spaces. Measuring the observed activity, both through the use of recognized indicators and hands-on evaluation, increases the accuracy of the process. Suspicious activity must be "an observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity"[16] for a report documenting such activity to be considered an ISE-SAR under this standard.

Following this review and a determination that the SAR has a relation to terrorism, the information will be formatted as described in the ISE-SAR Functional Standard and shared through the use of the Shared Spaces with all appropriate ISE-SAR EE participants. This process does not supersede other notification processes, such as when exigent circumstances require that ISE-SARs be immediately referred to the FBI's Joint Terrorism Task Force (JTTF); rather, it helps to enhance information sharing efforts.

[16] ISE-SAR Functional Standard.

SAR Information Sharing Goals—Complete, Accurate, and Timely

Efforts to prevent terrorist attacks are most effective when accurate, valid, and reliable information is used to support crime prevention and other counterterrorism activities. Since the laws, statutes, and practices that support, prohibit, or otherwise limit the sharing of personal information vary considerably between and among the federal, state, and local levels, each ISE participant may exclude additional privacy fields from its ISE-SARs, in accordance with its own statutory or policy requirements.

The ISE-SAR Functional Standard does not dictate a common process but provides a degree of standardization amongst participating agencies. Key to the design is the use of existing internal agency processes. For example, several participating agencies leveraged their existing behavior codes and SAR reporting processes as they entered the ISE-SAR EE. LAPD modified its existing Investigative Report used by officers to report crimes. Three changes were made: (1) the addition of a check box to identify the report as containing suspicious activity, (2) the addition of a check box for distribution to the Counter-Terrorism and Criminal Intelligence Bureau (CTCIB) Major Crimes Division (MCD), and (3) a check box for "Involved Party (IP)" information.[17] Modifying the existing report allowed LAPD to simplify the introduction of the SAR process within the department and was instrumental in the institutionalization of the SAR process. From these examples, it becomes clear that agencies, even large agencies, are capable of entering the ISE-SAR EE with a modicum of effort.

Commissioner Ed Davis, Boston Police Department: "History shows that the reason programs fail is due to the lack of implementation…. This is our chance to put the pieces of the puzzle together…. SAR is probably the most important thing we can do to protect the homeland…. Parochialism, not playing well with others, is something from the past and can only hurt us as an organization…. In everyday activities, the information we have and collect as an organization has to be shared…."

Data contained in reports designated as ISE-SARs originate from information gathered by source or reporting law enforcement organizations. Before the suspicious incident or behavior is documented in the first instance, entities apply various 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 of the reportedly "suspicious" circumstances. Law enforcement officers also may query systems to validate information relating to the incident or conduct.

[17] The term "Involved Party (IP)" did not exist on the previous Investigative Report. It was added with the idea that when the SAR box is checked, the officer will write the report using the term "IP" instead of "suspect." LAPD does not consider someone engaging in suspicious activity as a suspect but an IP, because, in reality, the suspicious activity may not be a crime; therefore, there would be no suspect.

The authors[18] of the *Information Sharing Environment—Suspicious Activity Reporting Functional Standard and Evaluation Environment: Initial Privacy and Civil Liberties Analysis* (Version 1—September 2008)[19] recommended that the ISE-SAR EE sites require source agencies documenting suspicious activity to assess their confidence in the information they report, including source reliability and content validity. 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 and ISE-SAR 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.

State constitutions, statutes, local ordinances, and policies may dictate the distributed housing of SAR and ISE-SAR data in each agency or fusion center so that local control is retained. The ISE-SAR Shared Spaces were designed by the state and local law enforcement representatives to meet their needs and to match their willingness and ability to share the data. For example, policy and technology prohibit the printing, download, and exporting of SAR data. Another state and local priority concerned the retention of the SAR information. Some SAR elements or the SAR in its entirety may be deleted or retained for a specific maximum time period based on statutes, codes, and applicable policies. For example, some agencies and centers may require a data purge if an actionable offense or case is not established or pursued based on the data within a certain time frame. Review periods have been established in some agencies and centers where a decision is made as to whether the information should be retained for a longer period of time or otherwise purged. Accordingly, each agency has developed a written policy concerning information retention. Ultimately, each source and submitting agency is responsible for the accuracy of its own data. Each submitting agency maintains control of its data residing in the Shared Spaces as it is updated, added, modified, or deleted, according to its established policy and practice. For the ISE-SAR Evaluation Environment, it was decided that when a search occurs, the record is shared for informational purposes but the data is not available for download; therefore, control of the data always remains with the submitting agency.

[18] The 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 DOJ, and the Legal Issues Working Group of the ISE Privacy Guidelines Committee—prepared and released an *Initial Privacy and Civil Liberties Analysis* of the ISE-SAR Functional Standard and included an IEPD component.

[19] See http://www.ise.gov/docs/sar/ISE_SAR_Initial_Privacy_and_Civil_Liberties_Analysis.pdf.

PROTECTION OF PRIVACY RIGHTS AND CIVIL LIBERTIES

The third important aspect of the NSI is its emphasis on protecting the privacy, civil rights, and civil liberties of Americans. Implementation of an approved privacy policy, application of the revised SAR Functional Standard, and privacy training of personnel ensured a comprehensive framework for the protection of privacy throughout the SAR process.

In September 2008, the PM-ISE, in consultation with the Civil Liberties and Privacy Office of ODNI, the Office of Privacy and Civil Liberties of DOJ, and the Legal Issues Working Group of the ISE Privacy Guidelines Committee (PGC), prepared the *Initial Privacy and Civil Liberties Analysis of the Information Sharing Environment-Suspicious Activity Reporting (ISE-SAR) Functional Standard and Evaluation Environment* (report). The report called for the development of a robust privacy, civil rights, and civil liberties protection process that included a requirement to have a written privacy policy for each participating SAR Evaluation Environment (EE) site.

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) The site could complete a comprehensive privacy policy based on Global's *Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template*.

(2) The site could formulate an ISE-SAR specific policy based upon the *ISE-SAR Evaluation Environment Privacy, Civil Rights, and Civil Liberties Protection Policy Template*.[20]

(3) The site could use its existing privacy policy and refine it to ensure that it addressed all the ISE Privacy Guidelines requirements for enhanced protection of terrorism-related information.

Each 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 PGC cochairs (privacy officials from ODNI, DOJ, and DHS) 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.

Throughout the Initiative, the PM-ISE and its federal partners remained committed to privacy by collaborating with privacy and civil liberties advocacy groups. Advocacy groups, including the American Civil Liberties Union and representatives from the Muslim advocacy

[20] The Privacy Guidelines Committee's Legal Issues Working Group finalized and approved the template for distribution to the participating sites in January 2009.

community, served an essential role in shaping the privacy protection framework for ISE-SAR information sharing activities, assisted with the development and review of products (e.g., templates and training), and met with the ISE-SAR EE implementation group on numerous occasions.

The development and revision of the Functional Standard illustrates the importance of building a strong partnership with advocacy groups. Following extensive outreach and consultation with privacy and civil liberties advocacy groups, the Functional Standard was developed with PGC participation and was revised in May 2009 to enhance its privacy protection focus. The revised Functional Standard identifies the types of activity that may be deemed suspicious and the circumstances under which such information may be shared. The revised standard defines suspicious activity as *"observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity."* A determination that a SAR, initially gathered and vetted by a source agency, constitutes an ISE-SAR must be made as part of a two-step process by trained analysts. Analysts use explicit terrorism behavior criteria and consider all relevant facts and circumstances in deciding that the behavior observed is reasonably indicative of terrorism activity. By focusing on *observed behavior,* this standard mitigates the risk of profiling based on race, ethnicity, national origin, or religion. It also improves mission effectiveness by enabling ISE-SAR EE personnel to scope and address potential threats in a more efficient and standardized manner.

Each participating EE site also had the responsibility to train its personnel. At the direction of the PGC and project sponsors, the Initiative and its partners[21] provided extensive SAR-specific training focusing on protecting privacy, civil rights, and civil liberties to the EE sites' executives, analysts, investigators, managers, and line officers.

Following the end of the EE pilot phase, privacy officials debriefed each site and assessed the extent to which the revised Functional Standard and the privacy protection framework mitigated implementation risks associated with ISE-SAR information sharing activities. While it is clear that the Initiative resulted in major accomplishments, the assessment pointed out certain areas that will require enhanced focus during the broader NSI implementation in 2010, including:

- NSI sites are strongly encouraged to engage in outreach to members of the public, private sector partners, and privacy and civil liberties advocacy groups during their privacy policy development and to address their concerns and recommendations through the adoption of appropriate privacy and civil liberties safeguards. A transparent process and collaboration with advocacy groups will reinforce the ongoing commitment

[21] The entities that provided training included the Major Cities Chiefs Association, the Institute for Intergovernmental Research, and the International Association of Chiefs of Police.

by federal, state, and local partners to fostering the trust of the public and the privacy and civil liberties community.

➢ Given that participating sites generally experienced delays in developing and implementing their privacy policies during the EE Initiative, the broader NSI will require each site to fully adopt the NSI privacy protection framework prior to participation in the NSI.

- To expedite privacy policy development and implementation, it is strongly recommended that the sites have access to the services of a trained privacy officer who is available to provide ongoing advice and assistance regarding privacy, civil rights, and civil liberties.

- The revised Functional Standard must be effectively communicated to personnel with responsibilities in the ISE-SAR arena to ensure the proper application of this standard. Line officers in particular should receive specialized training to strengthen their ability to recognize the types of behavior that may be indicative of terrorism.

- Although no sites reported a breach of personal information contained in privacy fields during the ISE-SAR EE, it is essential that site personnel receive ongoing training that focuses on safeguarding personal information in order to strengthen their ability to prevent breaches involving personal information and to underscore their reporting obligations.

- Even though no complaints for redress were filed during the Initiative, sites must consistently provide thorough explanations in response to public inquiries about sites' privacy policies, information availability, and redress procedures. Full and candid statements about the privacy policy framework are essential to ensuring the transparency of ISE-SAR processes and to fostering the public's trust.

- Given that extensive training of site personnel was effective in increasing privacy awareness at the participating sites, all site personnel in the broader NSI implementation must be informed and trained regarding their respective responsibilities relative to protecting privacy, civil rights, and civil liberties and the consequences and accountability for violation of these responsibilities. Each site is responsible for developing ongoing role-based training regarding the ISE and the SAR process for frontline, investigative, analytic, and supervisory personnel.

- The sites confirmed that the technical assistance provided during the Initiative facilitated the development and implementation of the privacy protection framework. The Initiative should therefore continue to provide technical assistance to sites to support privacy policy adoption, implementation, and training.

The results from the EE Initiative support the conclusion that the sites successfully implemented the privacy policy framework and that the extensive training provided to key personnel heightened awareness of basic privacy safeguards, thus reinforcing the privacy protection framework for the NSI. The continued success of the NSI largely depends on our ability to earn and maintain the public's trust. To further foster the public's trust, the PM-ISE and its federal partners are committed to a transparent ISE-SAR process. In January 2010, the ISE PGC cochairs will complete and release the final in-depth privacy analysis of the NSI ISE-SAR EE.

TRAINING

Training was a critical element of the ISE-SAR EE and is a vital component of the implementation of an agency's SAR process. As part of the ISE-SAR EE, a training plan was designed to ensure that personnel at all agency levels receive instruction regarding the SAR process. The training also served to institutionalize the effort throughout the agency. For this project, three coordinated training courses—executive leadership, analyst/investigator, and line officer—were developed to target the different operational roles existing within law enforcement agencies.[22]

The Chief Executive Officer Briefing (also known as the Executive Leadership Course) focuses on establishing an understanding of the ISE-SAR EE, policy development and privacy and civil liberties protections, the importance of developing agency training and community outreach, determining the level of commitment to implement or participate in the ISE-SAR EE, determining the level of technical assistance needed, and gaining commitment for implementation and participation in the ISE-SAR EE. The Chief Executive Officer Briefing was delivered to the 12 pilot sites, and attendance included 389 participants from 180 law enforcement agencies.[23]

The SAR analyst/investigator course focuses on the review and vetting of SAR information as it relates to the ISE-SAR Functional Standard. Additionally, this course provides extensive

[22]The Major Cities Chiefs Association developed the Chief Executive Officer Briefing. BJA developed the SAR analyst/investigator course. The International Association of Chiefs of Police developed the line officer training component.

[23] Arizona Counter Terrorism Information Center; Boston, Massachusetts, Police Department; Chicago, Illinois, Police Department; Florida Department of Law Enforcement; Houston, Texas, Police Department; Las Vegas, Nevada, Metropolitan Police Department; Los Angeles, California, Police Department; Miami-Dade, Florida, Police Department; New York State Intelligence Center; Seattle, Washington, Police Department; Virginia State Police; and Washington, DC, Metropolitan Police Department.

coverage of the importance of privacy and civil liberties protections; terrorism indicators, recent trends, and stages of terrorism; behaviors tied to the ISE-SAR Criteria Guidance; and resources and tools available. The SAR analyst/investigator course was delivered to 16 sites, and attendance included 489 participants from 159 agencies. In addition to the 12 participating agencies within the ISE-SAR EE, training was also provided to representatives of 11 DHS components. Understanding the vital role analysts/investigators play in the SAR process, the Florida Department of Law Enforcement sponsored additional SAR analyst/investigator training at three of its regional offices.

The line officer training focuses on enriching the critical role line officers have in the effective implementation of the ISE-SAR process. The training was piloted in the classroom for the pilot state fusion centers of New York, Virginia, and Florida. An online version of the course was delivered to the Washington, DC, Metropolitan Police Department. Participants are trained to recognize those behaviors and incidents that could be indicative precursors to activity related to terrorism. The line officer training was delivered by the International Association of Chiefs of Police to more than 4,000 officers in Washington, DC; New York State; Virginia; and Florida.[24]

To continue the theme of transparency and openness, the American Civil Liberties Union and other privacy advocates were invited to review the training courses as they were developed. The input from these advocates provided significant enhancements and improvements of the overall SAR training programs.

Technology Solutions

The IRTPA requires that the ISE be "a decentralized, distributed, and coordinated environment" that "to the greatest extent practicable, . . . connects existing systems . . .; builds upon existing systems capabilities currently in use across the Government; . . . facilitates the sharing of information at and across all levels of security; . . . and incorporates protections for individuals' privacy and civil liberties." To this end, the ISE-SAR EE utilized a distributed data model to connect its Shared Spaces—the eGuardian System and DHS's SAR data—to make terrorism-related information available through Common Terrorism Information Sharing Standards, applications, and Web Services. By utilizing two different methods for sharing information, the EE allows agencies to choose the method most beneficial and efficient for them to share terrorism-related information.

The Shared Spaces allow authorized users to securely search the ISE-SAR data housed on local agency-controlled servers from one central location—the secure National Criminal Intelligence Resource Center (NCIRC) portal. In most cases, a two-server system was installed in which a server designed to house the ISE-SARs was protected inside an agency's firewall while the second server, designed to receive ISE-SAR queries from the NCIRC portal,

[24] The dates and location of all training sessions is listed in Appendix Two: Project Timeline.

remained outside. These servers are connected to create the ISE-SAR EE Shared Spaces, which are accessible to all Evaluation Environment participants. When a query is submitted to the Shared Spaces by an agency, the data elements are transmitted to each of the participating agency Shared Spaces servers and the database for that location is searched. Results matching the query elements are transmitted back from the participating agency's Shared Spaces servers to the Shared Spaces portal, where they are aggregated into a single result set, allowing users to identify items of interest. The communication backbone that allows this query to occur uses virtual private network (VPN) technology to deliver information between sites in a secure manner.

eGuardian is available through the secure Law Enforcement Online Internet portal. Those agencies that participate in eGuardian will be able to directly input terrorism-related suspicious activity and conduct searches. Their entries will be automatically sent to a state "fusion center" or a similar intelligence-based center for vetting, where trained personnel will evaluate it and then either monitor it, close it, or refer it to the appropriate FBI Joint Terrorism Task Force for investigation. Ultimately, eGuardian will add additional capabilities for conducting analysis.

Figure 2 depicts a high-level overview of the Shared Spaces Concept.[25]

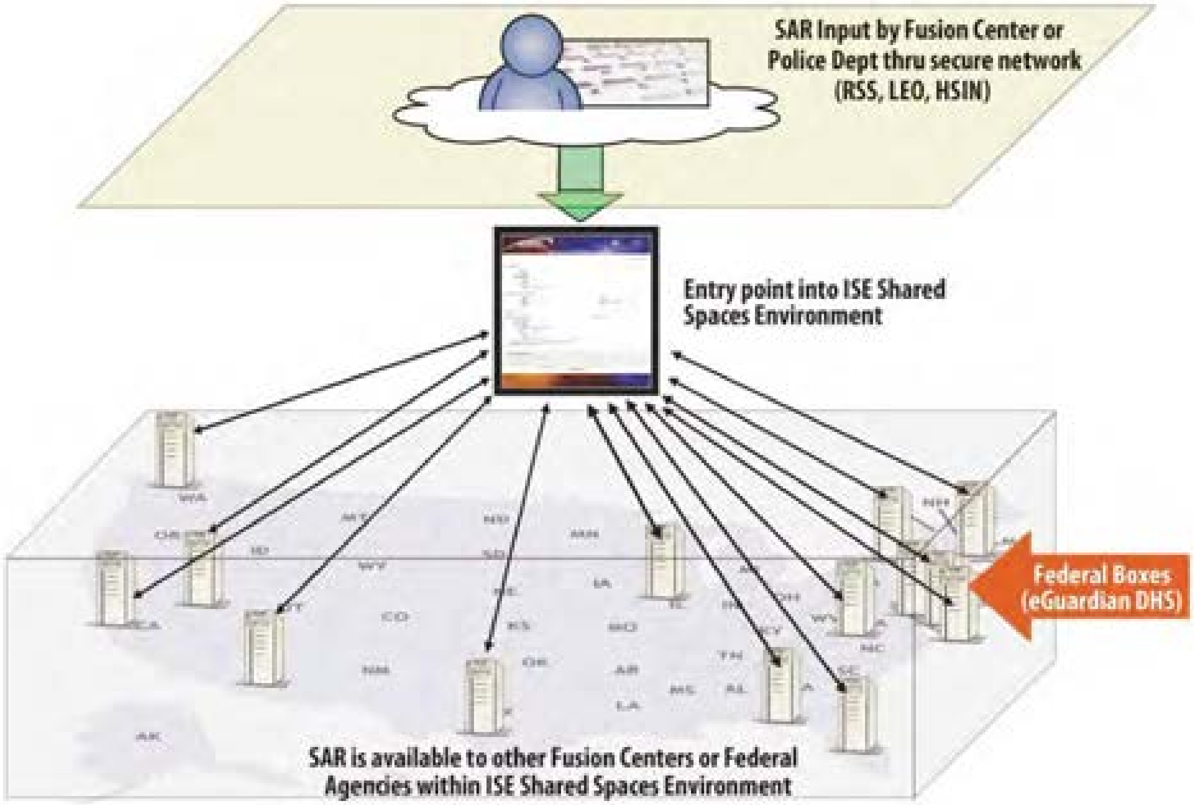

SAR Input by Fusion Center or Police Dept thru secure network (RSS, LEO, HSIN)
Entry point into ISE Shared Spaces Environment
Federal Boxes (eGuardian DHS)
SAR is available to other Fusion Centers or Federal Agencies within ISE Shared Spaces Environment
WA
OR
CA
ID
MT
WY
CO
NM
ND
SD
NE
KS
OK
MN
IA
MO
AR
LA
MS
AL
TN
KY
IL
OH
WV
NC
SC
NH
AK

FIGURE 2: OVERVIEW OF SHARED SPACES CONCEPT

[25] See http://www.ise.gov/docs/sar/NSI_CONOPS_Version_1_FINAL_2008-12-11_r5.pdf.

The Shared Spaces integrate the National Information Exchange Model (NIEM) standards, DOJ's Logical Entity eXchange Specifications (LEXS) Search and Retrieve messaging protocol, and the ISE-SAR Functional Standard into a standardized process to efficiently and effectively share information. The next level of technical detail, which enhances the NSI CONOPS, the ISE-SAR EE Segment Architecture, was released in December 2008. It documents a logical arrangement of business and functional drivers, information exchange requirements, and outcomes and constraints for extending capabilities implemented during the ISE SAR EE project. This segment architecture, derived from ISE Architecture program documentation, identifies enabling services required for operational implementation and use. It also will assist program managers, chief architects, and systems designers and implementers as they determine the programmatic and solution strategies that support the business case for future NSI and ISE SAR capabilities.[26]

During discussions with project participants in September 2008, key challenges were identified that impact an agency's participation in the project. These challenges included:

- Inability to consolidate SAR reports from multiple sources.
- Inability to vet reports and identify the SAR reports that have a nexus to terrorism and hence need to be forwarded to the ISE-SAR Shared Spaces.
- Inability to enhance SARs since multiple data elements identified in the SAR IEPD may not be fully supported by the agency's existing SAR records management system.

As a result of these discussions, it was determined that there was a need for the provision of a "bridge" between the existing SAR legacy systems and the semiautomated processes that are being used today at many agencies. This would improve the quality and completeness of the SAR IEPD-based content and ensure that SAR records that were submitted to the ISE Shared Spaces met the SAR criteria and the privacy guidelines established by the ISE-SAR Functional Standard. This would also ensure that the agency would retain operational control and would be able to vet the SAR information being forwarded to the ISE-SAR Shared Spaces.

The SAR Vetting Tool (SVT) was identified as a solution that could be developed once and deployed to the various organizations as a tool for managing the SAR creation and update processes and ensures that high-quality and complete SAR reports could be forwarded to an agency's ISE Shared Spaces environment.

[26] See http://www.ise.gov/docs/eaf/ISE-EAF_v2.0_20081021.pdf.

System Security

The ISE-SAR EE is not a national security system and does not contain classified information. The ISE-SAR EE project uses multiple secure Sensitive But Unclassified (SBU) networks, including the DOJ-supported Regional Information Sharing Systems® Secure Intranet (RISSNET™), the FBI-supported Law Enforcement Online, and DHS-supported Homeland Security Information Network,[27] as the connection and transport mechanisms for sharing SARs. This gives law enforcement agencies access to the ISE-SAR EE through the SBU network(s) they currently utilize. The ISE-SAR EE uses a separate server for each agency controlled by that agency. Additionally, the eGuardian system provides the connection between the JTTF and the ISE-SAR Shared Spaces, whereas the DHS Shared Space provides a connection to all DHS entities.

The ISE-SARs are stored, processed, and disseminated in a protected information environment that provides adequate security controls. These controls include:

- ➢ Controlled access to the information that allows only authorized users—limited to certain individuals assigned by participating fusion centers—to access, retrieve, and display ISE-SAR information.
- ➢ Use of DOJ's Trusted Broker solution to allow access to the Shared Spaces from multiple SBU networks. The Trusted Broker is an identity management process that allows users to avoid having to use multiple usernames and passwords to sign on to different systems.
- ➢ Encrypted transmission of information sent between Shared Spaces sites and the NCIRC portal.
- ➢ Use of VPN and additional firewall technology installed at the fusion center sites to limit access by ISE-SAR EE users to only those servers that are supporting the Shared Spaces environment.
- ➢ Force a ISE-SAR EE participating agency to explicitly "mark" SARs that should be pushed to the agency's Shared Spaces repository and thereby ensure that only information it is allowed to share by its constitution or statutes, local ordinances, or agency policy is made available to the broader ISE-SAR EE community.
- ➢ The Implementation Guide is used to ensure that all participants use the same standards, rules, process, and guidelines.

[27] Homeland Security State and Local Intelligence Community (HSLIC).

METHODOLOGY TO MEASURE, DOCUMENT, AND EVALUATE THE ISE-SAR EE

The ISE-SAR EE was developed to test the assumptions of sharing ISE-SAR information across multiple domains in accordance with the ISE-SAR Functional Standard and business rules. The project sought to identify pilot site partners from state and major urban area fusion centers, DOJ, and DHS. The ISE-SAR EE examined the usefulness of the ISE-SAR Criteria Guidance (Part B of the ISE-SAR Functional Standard) and the sharing of ISE-SAR information among major city and other law enforcement agencies, JTTFs, and fusion centers. The Evaluation Environment has provided the capability to establish, test, and validate the end-to-end agency SAR processes, including the development of priority information needs, information gathering and reporting policies, report vetting and analysis, and other enabling activities.

Following meetings with the participating agencies, the project partners developed an assessment for each of the pilot sites to evaluate their current SAR processes and procedures and to determine the standing and threat-based information sharing need priorities. Additionally, the site visits were conducted to evaluate the existing technology capabilities and current business processes surrounding the gathering, analysis, and sharing of terrorism-related SAR information. These site visits allowed project partners to document the "As-Is" SAR process of the pilot sites. The discussion and determination of each agency's "As-Is" SAR process questions were developed based on the *Suspicious Activity Reporting Process Implementation Checklist*. The reports developed as a result of these site visits outline the current workflow, technology, and business processes of the SAR sites. The assessments were held for the following locations on the following dates:

Washington, DC, Metropolitan Police Department	November 4, 2008
Los Angeles, California, Police Department	December 4, 2008
Chicago, Illinois, Police Department	December 16, 2008
Boston, Massachusetts, Police Department	December 17, 2008
Houston, Texas, Police Department	January 13, 2009
Las Vegas, Nevada, Metropolitan Police Department	January 15, 2009
Miami-Dade Police Department	February 18, 2009
Florida Department of Law Enforcement	February 20, 2009
Seattle, Washington, Police Department	February 24, 2009
New York State Intelligence Center	April 23, 2009
Virginia State Police	May 1, 2009
Arizona Counter Terrorism Information Center	July 23, 2009

Leading up to and following these site visits, numerous partner meetings and conference calls were held to ensure partner collaboration and project awareness.

SAR Performance Measurement

The PM-ISE created a Performance Measurement Plan (Plan) to measure the effectiveness of the SAR activities in the EE. The Plan incorporated a set of discrete performance measures designed to monitor implementation of required privacy protections, to analyze SAR statistics, and to address the effectiveness of the SAR process. Measures included:

- Tracking training programs to facilitate proper implementation of privacy and civil liberties protections.
- Monitoring numbers of SARs gathered and processed, placed into the Shared Spaces, and reported to the FBI's JTTF.
- Identifying investigations, arrests, and convictions that benefited from SAR data.

Observations:

The SAR team used a variety of techniques to collect information, including automated tools, interviews, and survey reporting by the sites. After analyzing this information, the team developed three observations that indicate sites effectively shared SAR data and that SAR data can have a positive operational impact.

Observation 1: Few sites were able to fully implement the SAR process and share data.

By the end of the evaluation, the Florida Department of Law Enforcement (FDLE), the Virginia Fusion Center (VFC), the New York State Intelligence Center (NYSIC), and the Boston, Massachusetts, Police Department (BPD) completed the activities necessary to share SAR data with other sites and their analysts regularly performed searches of the ISE-SAR Shared Spaces. Figure 3, below, illustrates the level of search activity over the 14 biweekly periods of the ISE-SAR EE. There is a significant increase in the number of searches toward the end of the EE. This increase may be attributed to additional sites gaining access to the Shared Spaces and is consistent with the increase in users (see Figure 4). FDLE experienced a sharp increase in the number of searches, which may be attributed to a change in policy at that site. FDLE management modified its training for its analysts, requiring them to search the ISE-SAR Shared Spaces as part of their standard operating procedures.

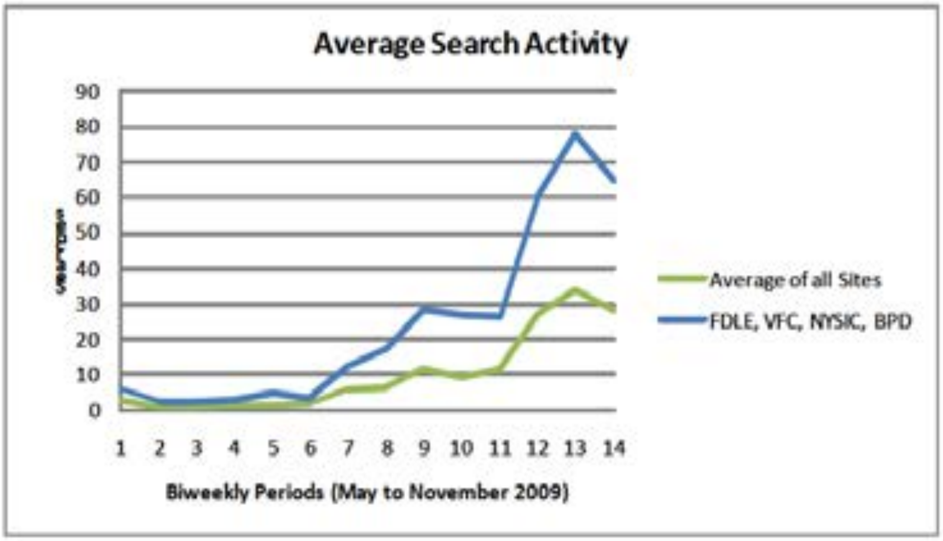


FIGURE 3: FDLE, VFC, NYSIC, AND BPD FULLY IMPLEMENTED THE REQUIREMENTS TO ENABLE ANALYSTS TO SEARCH THE ISE-SAR SHARED SPACES.

Figure 4, below, illustrates that three of the four active sites had a significant increase in the number of users. This timing of the increase in users coincides with the increases in overall search activity across the EE.

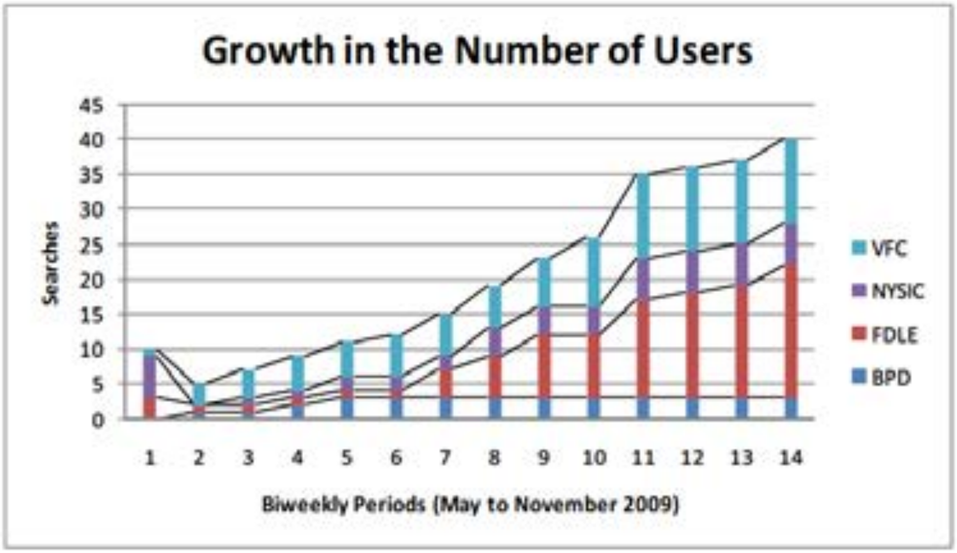


FIGURE 4: FDLE, VFC, AND NYSIC SHOWED THE GREATEST INCREASE IN USERS OF THE ISE-SAR SHARED SPACES, POSSIBLY CONTRIBUTING TO THE INCREASE IN SEARCH ACTIVITY ORIGINATING AT THOSE SITES.

Observation 2: It proved challenging for sites to provide performance statistics on activities prior to posting SARs in the Shared Spaces (after identification as ISE-SAR).

The sites were asked to track the total number of SARs collected prior to and during the evaluation period as well as the number of ISE-SARs identified (i.e., SARs with a nexus to terrorism). Several sites had difficulty providing statistics on the total number of SARs received prior to being assessed as ISE-SARs—some for lack of an automated tracking capability and others because they only receive SARs evaluated for a possible connection to terrorism by another organization—e.g., the local police department.

Of the sites that were able to implement an effective screening process to identify ISE-SARs, FDLE and VFC stand out as examples:

- FDLE: Over the course of the evaluation, FDLE vetted 5,727 SARs (most predating the evaluation) and identified 12 ISE-SARs.
- VFC: Over the course of the evaluation, VFC vetted 347 SARs and identified 7 ISE-SARs.

Observation 3: Reported activities demonstrate that the SAR process produced operational impact.

The majority of sites were unable to calculate the number of arrests and investigations resulting from SAR data; however, five sites successfully linked operational results to the implementation of the SAR process, including:

- Four of the five sites reported the number of federal investigations initiated as a result of ISE-SARs.
- Three of the five sites reported the number of local investigations initiated as a result of ISE- SARs.
- Two of the five sites reported on the number of local or federal investigations that led to arrests or convictions in cases involving ISE-SARs.
- Two of the five sites reported that they use ISE-SARs for critical infrastructure protection and in the products generated as a result of pattern and trend analysis.

The five sites providing this results data are major urban area fusion centers, not state fusion centers. By design, these fusion centers work more closely with the officers and detectives investigating SARs in their jurisdiction than other fusion centers. For instance, in Washington, DC, the investigation of four SARs received at the fusion center led to the arrest of an individual for producing 25 bomb threats.

RECOMMENDATIONS

It became apparent during the evaluation that any future SAR performance measurement plan should provide a results-oriented approach to monitor progress and performance, optimize resources, and promote accountability. That plan must:

Recommendation 1: Focus on helping sites to improve their automated reporting capability to monitor and report on SAR process activities. Although sites were able to monitor SARs once posted to the Shared Spaces, most were not able to track and report on SAR activities that occurred prior to being posted or after they were used in analytical and law enforcement activities.

Recommendation 2: Develop the means to differentiate training and testing searches in the Shared Spaces from operational activity in the Shared Spaces. Currently, test data appears identical to operational data in the Shared Spaces, and unless manually deleted by the site, it may distort usage statistics.

Recommendation 3: Review national law enforcement best practices to identify potential new performance measures and identify areas of improvement with existing measures.

PROJECT GOVERNANCE

A project management structure was developed at the beginning of this initiative that emphasized state and local law enforcement participant project ownership. The governance process relied on several key methods for communicating the project goals, objectives, current status, and next steps, including:

- Weekly project team meetings via conference call
- Face-to-face working group meetings held approximately every 45 days
- Semiannual user group meetings
- User group conference calls as necessary
- Monthly activity summary newsletters

The federal project sponsors were essential to the success of the initiative. Through their work and collaboration, the project was able to meet its project goals and achieve project objectives. These federal partners include:

- U.S. Department of Justice, Bureau of Justice Assistance
- Federal Bureau of Investigation
- U.S. Department of Homeland Security

- Office of the Program Manager for the Information Sharing Environment
- DOJ's Global Justice Information Sharing Initiative
- Criminal Intelligence Coordinating Council
- U.S. Department of Defense
- Office of the Director of National Intelligence

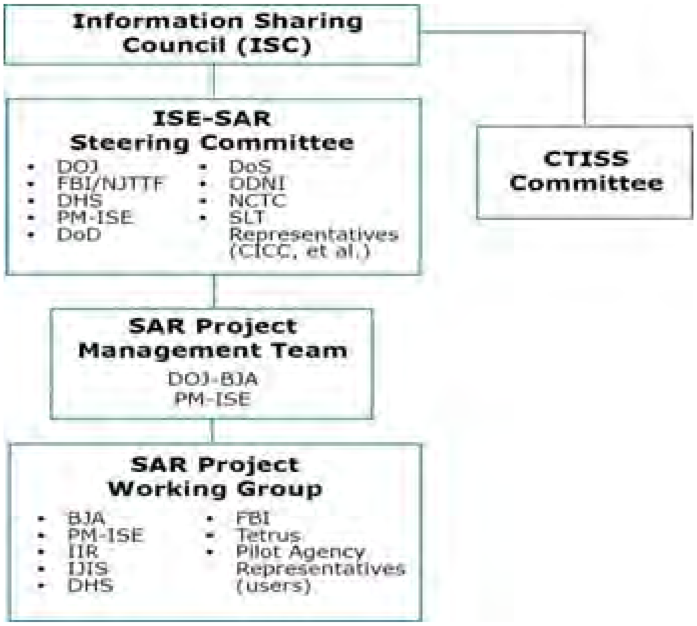
Other key participants in governance of the project were the International Association of Chiefs of Police and the Major Cities Chiefs Association. Blending state and local users with the federal partners created a unified and coordinated effort that produced a seamless governance structure. The openness and transparency of the governance structure represents one of the key successes of the overall project.

The support mechanism in place for the ISE-SAR EE included a Steering Committee, which provided strategic direction for the project. The committee synchronizes interagency activities, resolves major issues, and addresses resource needs. It is charged with developing ISE-SAR policies and practices, addressing evolving SAR requirements, and addressing agency noncompliance issues. The ISE-SAR Steering Committee forwarded recommended changes regarding the ISE-SAR Functional Standard gleaned from this project to the Common Terrorism Information Sharing Standards (CTISS) Committee for incorporation into future versions of the ISE-SAR Functional Standard and consideration with other functional or technical standards of the CTISS.

The SAR Project Management Team was responsible for overall oversight of the evaluation project. The Project Management Team provides guidance to the SAR Project Working Group; approves the project scope, modifications, and updates; and resolves issues forwarded by the Project Working Group.

The SAR Project Working Group is composed of the Project Management Team members, the service providers implementing the project, and representatives from the state and local agencies involved in the evaluation project. The Project Working Group is responsible for the day-to-day project implementation and issue resolution, providing subject-matter expertise when developing system requirements and capabilities, and maintaining/tracking project decision items. The Project Working Group constituted user/focus groups for specific project purposes. Unresolved issues from the Project Working Group were provided to the Project Management Team for resolution and, ultimately, to the ISE SAR Steering Committee.

The following graphic depicts the SAR Governance Structure:[28]


Information Sharing Council (ISC)
CTISS Committee
ISE-SAR Steering Committee
DOJ
FBI/NJTTF
DHS
PM-ISE
DoD
DoS
ODNI
NCTC
SLT Representatives (CICC, et al.)
SAR Project Management Team
DOJ-BJA
PM-ISE
SAR Project Working Group
BJA
PM-ISE
IIR
IJIS
DHS
FBI
Tetrus
Pilot Agency Representatives (users)

[28] *ISE-SAR Evaluation Environment Implementation Guide*.

ISE-SAR Evaluation Environment Observations and Lessons Learned

Leadership

Executive Leadership

> ***Lesson Learned:** Executive leadership is an important component of developing any new law enforcement process. The need to have executive buy-in and support, both from the agency leadership and the project managers, was determined to be critical to the successful implementation of the Information Sharing Environment-Suspicious Activity Reporting Evaluation Environment (ISE-SAR EE).*

Background: The support of the law enforcement agency executives was critical throughout the development and implementation of the ISE-SAR EE. Successful implementation and sustainment of the ISE-SAR EE required a strong commitment by the participating agency—especially the agency's leadership. Executive leadership is seen through the adoption of new General Orders, policies, and procedures supporting the ISE-SAR EE. Executive-level training was provided to all of the ISE-SAR EE sites. At the onset of the project, the Major Cities Chiefs Association (MCCA); the U.S. Department of Justice (DOJ), Bureau of Justice Assistance (BJA); the U.S. Department of Homeland Security (DHS); and the Global Justice Information Sharing Initiative (Global) issued a report titled *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project*. This report was subsequently endorsed by those agencies as well as the International Association of Chiefs of Police, the National Sheriffs' Association, the Major County Sheriffs' Association, and the Federal Bureau of Investigation (FBI). These endorsements reinforced to agency executives the importance of the SAR Initiative to law enforcement.

The fusion center leadership course being developed by the Naval Postgraduate School holds promise of providing continuity of leadership training for the nation's fusion centers.

> **Recommendation 1:** Prior to initiating the next phase of this project, the project team must ensure that each agency has the support of its executive leadership. This can be accomplished through regular briefings to law enforcement associations and through the MCCA's Chief Executive Officer Briefing. Face-to-face briefings are important so that agency executives understand the full scope of the project and the requirements and resources necessary from their agency.

> **Recommendation 2:** If the ISE-SAR EE is expanded, consideration should be given to conducting regional meetings with agency heads and fusion center directors to ensure that the agency command staff understand the tenets of the

initiative and are prepared to support the activities needed to implement the process within their agencies. Continuous trainings and briefings could offset the concerns raised by leadership turnover. Meetings with the fusion center leadership should take place at least biannually, with conference calls every quarter.

Recommendation 3: Consideration should be given to the development of an online training course for chief executives to facilitate the rapid distribution of information concerning the processing of SARs.

Recommendation 4: Executive-level training for fusion center leadership—including directors, deputy directors, and other command personnel—should be developed and provided for continuity of effort on major projects.[29]

Recommendation 5: Periodic project status meetings should be held between the proposed Nationwide SAR Initiative (NSI) Program Manager's Office and the executive leadership of the participating agency.

National Program Management

***Lesson Learned:* There must be leadership at the national level to ensure that all components of the ISE-SAR EE are fully implemented and integrated into existing law enforcement processes.**

Background: During the ISE-SAR EE, the project was managed jointly by the various partners, including the Office of the Program Manager for the Information Sharing Environment (PM-ISE), DOJ, BJA, the FBI, and DHS. BJA provided the leadership umbrella to ensure the coordination of all aspects of the project. During the project, each agency contributed its knowledge concerning the sharing of suspicious activity information. It was discussed that if the ISE-SAR EE is expanded, a national program office should be established to provide consistency of procedures and processes as well as assistance to the participating agencies. A single coordinating entity for all aspects of the project, as well as management of the technology and support functions, is critical to maintaining consistency and effective use of resources.

During the ISE-SAR EE, agencies received assistance from privacy subject-matter experts in developing and strengthening their privacy policies. This assistance proved to be invaluable as agencies worked through issues associated with the protection of privacy and civil liberties. As the program develops, there will be additional privacy issues that must be addressed concerning the appropriateness of sharing certain SAR information and any restrictions placed by local, state, or federal law or rule. The ISE Privacy Guidelines

[29] The development of the Naval Postgraduate School fusion center leadership program may help meet this need.

Committee (PGC)[30] members met several times with privacy and civil liberties advocacy groups to listen to concerns and to incorporate new ideas into revised ISE-SAR EE policies and processes. Some of the participating agencies agreed that assistance with privacy and civil liberties issues should be continued to provide consistency of policies and procedures.

During the ISE-SAR EE, the sponsoring agencies provided technical assistance in the form of training, policy development, and overall project coordination. The assistance provided was beneficial to the state and local agencies in developing, standardizing, and implementing procedures and processes for the gathering, analysis, and sharing of suspicious activity. Without the provision of policy templates, coordination project meetings, and policy reviews, it would have been difficult to develop a consistent nationwide process for the sharing of SAR information.

> **Recommendation 1:** Should the federal government expand the ISE-SAR EE beyond the 12 agencies currently involved, consideration should be given to creating a program management office to oversee the expansion of the ISE-SAR EE process nationwide. This would include the ability to provide technical training, business process, privacy expertise, and support to the participating agencies.

> **Recommendation 2:** National partnerships should identify financial support for future participating agencies to help implement the business processes, training, technology development, and privacy and civil liberties requirements in a consistent and appropriate manner.

> **Recommendation 3:** The proposed program management office should continue the technical assistance provided in the ISE-SAR EE to the participating agencies to ensure consistency and efficiency in the development of a nationwide program, technology, and policies. The proposed program management office should continue dialogue with privacy and civil liberties advocacy groups to continue to maintain transparency and openness of the process.

[30] The ISE Privacy Guidelines Committee is a standing committee established by the PM-ISE composed of each Information Sharing Council agency's ISE Privacy Official. The committee provides ongoing guidance on the implementation of the ISE Privacy Guidelines so that, among other things, agencies can follow consistent interpretations of applicable legal requirements, avoid duplication of effort, share best practices, and have a forum for resolving issues on an interagency basis. See Section 12(b) of the ISE Privacy Guidelines.

SAR Business Process

Existing SAR Processes

> *Lesson Learned:* ***Prior to the ISE-SAR EE, most participating sites had policies and procedures governing the handling of general law enforcement information; however, most did not have an established process to ensure compliance with the requirements of the ISE-SAR Functional Standard.***

Background: During the initial phases of the ISE-SAR EE, site assessments were conducted with the participating agencies in order to document the existing SAR processes. Prior to the implementation of the ISE-SAR EE, all of the sites had some form of process; however, the degree to which it was institutionalized throughout the agencies differed (during these site assessments, many promising practices were identified). The site visit teams documented the agency's process for gathering information regarding behaviors and incidents associated with crime and establishing a process whereby information can be shared to detect and prevent criminal activities, including those associated with terrorism. Additionally, during the ISE-SAR EE, several participating agencies either developed or enhanced specific policies concerning the handling of terrorism-related SAR information.

Prior to the initiation of the ISE-SAR EE, all participating agencies had some processes in place to manage the flow of suspicious reports emanating from citizens but had not developed processes to support all of the needed activities identified in the Nationwide SAR Cycle. During the project, several of the Nationwide SAR Cycle activities were addressed, including training, outreach, and risk assessments. However, due to the short duration of the project, not all of the activities of the Nationwide SAR Cycle were fully addressed.

Prior to the beginning of the project, several of the agencies had codes to identify the behaviors associated with terrorism. For example, the Los Angeles Police Department had more than 100 codes. Additionally, the state and local SAR Information Exchange Package Document (IEPD) had more than 20 codes. During the MCCA Intelligence Commanders meeting in July 2008, a consensus was reached that all participating agencies could take their existing code structure and map it to the code enumerated in Appendix B of the ISE-SAR Functional Standard. This allowed the project managers to develop consistent training on behaviors and allowed for a common message to be delivered to the public.

During the ISE-SAR EE, the project team recognized the importance of consistent SAR processes nationwide. These processes ensure consistency in the collection and sharing of SAR information. Agencies may have different internal procedures to process SARs, but it is important that all comply with the various resources, documents, and standards related to the national project.

Recommendation 1: If the ISE-SAR EE is expanded, future participating agencies should develop and implement policies and processes that govern the processing of SARs within all areas of their agency. This will ensure compliance with the ISE-SAR Functional Standard and related project resources. It is understood that each agency will have unique requirements, but a common set of processes across the initiative is needed.

Recommendation 2: User groups composed of representatives from the participating agencies should continue to meet and share best practices. This will allow for the continued refinement of policy and procedural templates, which ensure the optimal consistency and effectiveness of any future expansion.

Privacy Policies

***Lesson Learned:* Agencies participating in the ISE-SAR EE generally required assistance with updating existing privacy policies or developing a policy that meets the applicable requirements of the ISE Privacy Guidelines.**

Background: The development of policies that protect the privacy, civil rights, and civil liberties of citizens is a foundational element of the ISE-SAR EE. These policies demonstrate to the public that as law enforcement carries out its official duties, it does so while ensuring that citizens' rights are protected. The *National Strategy for Information Sharing* (NSIS) and the ISE Privacy Guidelines identify key tenets that should be included in an agency's policy. The ISE Privacy Guidelines also notate that state and local agencies should develop and implement appropriate policies and procedures that are, at a minimum, as comprehensive as those established by the Guidelines to participate in the Information Sharing Environment. Prior to participating in the ISE-SAR EE, most of the participating agencies had policies concerning the gathering and sharing of information, although none were in total compliance with the Guidelines. Participating agencies were eventually able to overcome additional hurdles such as the more recent release of the ISE Privacy Guidelines and the systemic complexity of the agency policy development and approval process. Obtaining approval for privacy policies from the participating agency's command and legal staff proved to be a time-consuming effort. To assist in the privacy framework development effort, project staff developed privacy policy templates and provided direct technical assistance to the sites.

Recommendation 1: Future participating agencies should continue to be required to have a privacy framework that is consistent with the ISE Privacy Guidelines.

Recommendation 2: Agencies should ensure transparency and openness in their privacy framework development efforts by engaging privacy advocates and community leaders as the policies are developed or refined.

Recommendation 3: Privacy subject-matter expertise assistance should continue to be provided to the state and local fusion centers as they develop their privacy policies. The templates developed during the project are useful to agencies; however, there are many unique state and local legal issues that must be addressed. As such, hands-on assistance and review by a common subject-matter authority are beneficial.

Recommendation 4: Completed policies should be posted on the secure National Criminal Intelligence Resource Center (NCIRC), with agency permission, for viewing by other participating agencies or other agencies wishing to adopt the policies and procedures developed during the project.

Criteria for Entering Data

Lesson Learned:* *At the beginning of the ISE-SAR EE, there was not a clear agreement on what constituted a terrorism-related suspicious activity. In addition, the level of suspicion needed to classify terrorism-related information as an ISE-SAR that would be shared with other law enforcement agencies was not clearly defined.

Background: At the outset of the ISE-SAR EE, there were several discussions concerning what suspicious activities were terrorism-related and how to apply the tenets of the ISE-SAR Functional Standard to the sharing of terrorism-related suspicious activity reports among law enforcement agencies. After discussion among project participants, legal experts, and representatives of privacy advocacy groups, a determination was made that the reasonably indicative standard would be required for this project.

The more appropriate term for information gathering during this project would be that information which is "reasonably indicative of terrorism-related activity." The development of training that stresses this issue and provides understanding to the participants about what activities would be appropriate to share was a key component in this project. Suspicious activity being collected and documented by the project for the ISE-SAR EE is the kind of data that agencies have always collected concerning suspicions of other criminal activities.

Recommendation: NSI leadership should provide specific guidance to future participating agencies concerning the appropriate level of suspicion needed for the inclusion of information in the NSI. A review should take place concerning the SARs entered during the evaluation period to determine the consistence of determining the level of suspicion.

PERSONALLY IDENTIFIABLE INFORMATION

> *Lesson Learned:* ***There was no common policy among the participating local, state, and federal agencies concerning the sharing of personally identifiable Information.***

Background: During the implementation of the ISE-SAR EE, considerable discussion surrounded the inclusion of personally identifiable information (PII) within the ISE-SAR Shared Spaces environment. This discussion centered around who could view PII and under what circumstances. During the discussion, there was a difference of opinion among the federal, state, and local participants in the ISE-SAR EE on the value of PII from a ISE-SAR Shared Spaces investigative or analysis perspective. As currently deployed, authorized ISE-SAR EE users have access to all SAR data including PII. The PII issue and the balance between privacy and civil liberties protection and authorized data accessibility will remain as additional homeland security partners request access to the Shared Spaces data. With the adoption of an identity management application, the ability to introduce role-based access is achievable. However, even with role-based access, because some SAR records entered into the Shared Spaces may contain PII within free-text or narrative fields, the system cannot guarantee that all PII is protected. Despite that constraint, two approaches are suggested that may minimize the impact.

> **Recommendation:** The user interface at the NCIRC portal could provide a filter solution that would display only fields that a user is authorized to see based on the credentials established when system access is originally authorized. The advantage of this solution is that the central control of security access and software applications installed at existing and near-term site installations would not have to be modified since all modifications could be implanted at the portal (NCIRC). The disadvantage from a security perspective is that the PII data is retrieved but hidden from view as opposed to not being retrieved at all. A second disadvantage is that should an individual site need to invoke locally controlled role-based access, based on center policy, statute, or regulation, and restrict sharing of PII to another agency, to a role, or to a specific individual, the centralized approach probably is not the right solution.

SHARED SPACE DATA ENTRY

> *Lesson Learned:* ***Because there are two options available to agencies, the Shared Space technology and the eGuardian program, there was confusion among some agencies as to the best method for their agency to participate in the ISE-SAR EE.***

Background: The FBI's eGuardian program and the ISE SAR Shared Spaces are both components of the ISE-SAR EE. Each of these data entry options has its strengths and weaknesses, and one may be more appropriate for use by a local agency or fusion center than the other method. The process for gathering, assessing, and sharing the information is the same for both systems. There remains some lack of clarity among law enforcement agencies as to the differences between the two options and which one would be the most appropriate for their agency to utilize in the sharing of SAR information. During the initial implementation of this project, there remained a great concern over the control of the information being shared. Many of the participant agencies were adamant that the data should not be located in a central location where they would lose control of their local information.

Recommendation 1: Continue to provide a clear understanding of the process involved with both the ISE-SAR Shared Spaces and eGuardian through briefings and outreach efforts. This will enable agencies to determine the best process for their agency to participate in any future phase of the project.

Recommendation 2: There should be a unified training effort for the two systems so that participants fully understand both methods of entering information into the ISE-SAR Shared Spaces.

Shared Space Access

***Lesson Learned:* At the beginning of the project, there was a lack of clarity regarding which agencies could access the ISE-SAR Shared Spaces.**

Background: The ISE-SAR EE Implementation Guide states that "only criminal investigative/analytical personnel from other evaluation project participating federal, state, and local law enforcement agencies, by express agreement, are permitted access to the system." This allows participating fusion centers to decide who has access to the system. Some have restricted access to only a few members of the fusion center, whereas others desire to open system access to other local law enforcement agencies, fire, emergency medical services, and public sector organizations with which they have a working relationship. As the system continues to grow, additional agencies may have need to access the information but may not be one of the participating agencies.

Recommendation 1: The proposed program management office, working with the participating agencies, should develop an appropriate policy to govern access to users outside of law enforcement.

Recommendation 2: As the ISE-SAR EE expands, user agreements should be developed and signed by all participants agreeing to abide by the policies. This effort should be led and controlled by the states and local participants.

Training

Project-Delivered Training

> ***Lesson Learned:* The three training courses developed for the ISE-SAR EE—executive level, analyst/investigator, and line officer—ensured that consistent training was received nationwide and assisted in the successful development and initial implementation of the agencies' SAR process.**

Background: During the initial development of the ISE-SAR EE, the project team identified three (3) levels of training that should be developed and delivered to the agencies participating in the ISE-SAR EE. The three levels focus on the roles of the executive, analyst/investigator, and line officer and established consistency among the participants of the ISE-SAR EE as they developed and implemented their SAR process.

> **Recommendation 1:** The three training programs should be delivered to all agencies that are developing a SAR process and will participate in the Nationwide SAR Initiative (NSI). If at all practical, trainings should be held contemporaneously.
>
> **Recommendation 2:** Because it will be a large challenge to deliver these three training courses to the more than 18,000 state, local, and tribal law enforcement agencies, varied methods of delivery—including CD-based training, Web-based training, and video streaming—should be considered as delivery mechanisms for these courses.
>
> **Recommendation 3:** The Chief Executive Officer Briefing should be delivered to organizations representing chiefs of police, sheriffs, and other public safety executives to maximize chief executives' exposure to the NSI and their responsibilities.

Additional Training

> ***Lesson Learned:* As agencies began to implement their SAR process and provide SARs to the ISE-SAR Shared Spaces, it became evident that additional training beyond the three initial courses was necessary to assist agencies in fully and consistently implementing a SAR process.**

Background: As the ISE-SAR EE sites were identified, they were provided the three initial levels of training—executive, analyst/investigator, and line officer. However, as the project moved forward and agencies institutionalized their SAR process, it became apparent that additional, more specific training should be developed and delivered to the agencies participating in the ISE-SAR EE. The additional training identified included SAR Vetting Tool (SVT) user training, first-line supervisor training, continued privacy and civil liberties training, and technical assistance on developing policies.

SAR Vetting Tool (SVT) User Training—During the ISE-SAR EE, a tool (the SVT) was developed by the BJA team to assist state or regional fusion centers in the vetting of SAR information. This program allows agencies to enter their SAR data (either manually or by automated interfaces to existing legacy systems) into the SVT and use the tool to determine that appropriate and high-quality information is being pushed to the ISE-SAR Shared Spaces. It is important that the users of the program be provided sufficient training with the SVT to allow for the correct utilization of the tool. Lack of sufficient training could ultimately lead to inappropriate information being pushed to the ISE-SAR Shared Spaces.

First-Line Supervisor/Midlevel Manager Training—A review of the processes of the source agencies submitting SAR information to state and regional fusion centers determined that the first real analysis for SAR information is conducted by first-line supervisors of these law enforcement agencies. Further review of the information and process is conducted by midlevel managers in the agencies. If first-line supervisors and midlevel managers are unfamiliar with the ISE-SAR EE and the behaviors critical to determining precursor activities to potential terrorist attacks, then important SAR information may not be reported and shared. The first-line supervisors and midlevel managers should also ensure that they gain a complete understanding of their local agency policies and procedures for the review and forwarding of SAR information to the appropriate fusion center. A key aspect of training first-line supervisors was the use of Terrorism Liaison Officers (TLO) or similar type of programs. These officers provide fusion centers with direct liaison officers to field operational units and provide for continuation training and programmatic understanding.

Continuing Privacy Training—An important component of the ISE-SAR EE is ensuring that all sites are fully educated regarding privacy and civil liberties protections, as well as federal rules and regulations concerning these topics. Prior to the ISE-SAR EE, training and technical assistance were delivered to state and major urban area fusion centers. The training focused on the understanding of privacy, civil rights, and civil liberties rules and regulations to state and local law enforcement agencies. Additionally, during the ISE-SAR EE, a basic privacy and civil liberties training program was developed.

> **Recommendation 1:** Training programs should be developed for both users of the SVT and the first-line supervisors/midlevel managers. These additional courses will ensure a complete training package for agencies implementing a SAR process.
>
> **Recommendation 2:** Privacy-related training and technical assistance should continue to be provided to fusion centers and agencies participating in the ISE-SAR EE, as well as agencies not participating in the NSI.
>
> **Recommendation 3:** The Terrorism Liaison Officer (TLO) programs proved to be very beneficial in providing continuation training to field personnel. Support and training for the development of TLO programs should be enhanced and expanded.

INSTITUTIONALIZATION OF THE SAR PROCESS

ANALYTIC TOOLS AND PROCESSES

> ***Lesson Learned:* Although it was not originally part of the project plan, agencies participating in the ISE-SAR EE expressed the need for common analytic tools to be developed and/or identified and made available to all users accessing the data in the Shared Spaces, allowing for additional analysis of ISE-SAR information.**

Background: The analysis of information derived from suspicious activity reports is key to identifying potential threats. There was recognition that additional analytic tools would be beneficial; however, because of the limited time frame for this project, not all aspects could be fully developed. Although each participating agency can analyze its own data or search data from other participating agencies through the ISE-SAR search tool, there are currently no tools available to allow analysis of all SARs. Additionally, there is no process to ensure that all SARs collected nationwide are being analyzed. Typically, agencies conduct detailed analysis of information that relates directly to their jurisdiction but do not have the time or resources to conduct nationwide analysis of incoming information.

> **Recommendation 1:** Conduct research and identify analytic tools that can operate in the distributed environment. These tools would need to simultaneously protect the confidentiality and privacy of the information contained within the shared space. The proposed program management office should consider the adoption and provision of these tools to enhance the capability of the search.

> **Recommendation 2:** Create a capability at the national level that would be responsible for analyzing on a national basis all SARs entered into the ISE-SAR Shared Spaces. This capability would also provide analysis and feedback to the agencies participating in the NSI.

NETWORK CONFIGURATION

> ***Lesson Learned:* Because the ISE-SAR Shared Space servers and applications were not considered a "production" system by most of the site information technology staff, site system and network administration responsibilities were not clearly defined.**

Background: The Virtual Private Network (VPN) approach to the ISE Shared Spaces connectivity was generally effective. However, because the ISE Shared Spaces configuration was considered to be a pilot, had demilitarized zone (DMZ) components, and was time-limited, in many cases separate subnetworks were established for the ISE-SAR EE equipment for security reasons. At the beginning of the project, most participating agencies showed a concern about a VPN access to their internal networks. While this offered desirable security protection to the site information technology (IT) facility, it also led to a "one-off" situation, and site IT staff did not always monitor the subnet for performance or outages on a scheduled basis. Staff at the NCIRC.gov site most often were the first to recognize subnet problems and had to advise fusion center staff. These outages caused some problems with participating agencies' ability to fully search all servers in the project.

> **Recommendation:** Reconfigure the ISE-SAR EE network architecture at each site to "elevate" its status as a production system, and as necessary, integrate the ISE-SAR Shared Spaces into existing network monitoring processes currently installed in the centers.

Background Checks

> ***Lesson Learned:* As a result of the site visits, it was determined that there was no consistent background check process that applied to all participating agencies and contract personnel involved in the ISE-SAR EE.**

Background: While not necessarily required by the project, the Technical Deployment Team requested that each site "clear" contractor staff who would be involved in on-site installation and test activities, as well as postdeployment remote access to a site's ISE-SAR Shared Spaces equipment and data via the NCIRC.gov portal. The requirement for background checks was not due to the nature of ISE-SAR EE data (which is unclassified) but the potential access to a fusion center's internal network that hosts the Shared Spaces environment along with other systems.

None of the contractor staff had any prior federal background checks that might suffice the fusion centers' specific requirements. As a result, each fusion center site required some level of background check before the deployment staff could begin work. Some sites required only limited personal information and ran local checks in their jurisdiction, while others completed full investigations requiring fingerprints and FBI background checks for the ten contractor staff members assigned to the project. In only one case did a fusion center accept the background check performed by another agency.

Participating agencies were also asked to accept existing state and local agency background checks as being sufficient for allowing other agencies to view their data in the shared space. Although this did not present a problem in the ISE-SAR EE, it could become a larger issue if the SAR initiative is deployed nationwide.

> **Recommendation:** The proposed program management office (PMO) should coordinate obtaining appropriate background checks for staff working at the sites to implement any future rollout of this project. The clearances protocol should cover all participating agencies as well as the staff for operations and maintenance duties.

OUTREACH

OUTREACH AND AWARENESS

> ***Lesson Learned:* Agencies that develop and institute a SAR process should include outreach and awareness programs to better inform law enforcement, the general public, privacy advocates, and private sector entities regarding the types of information that should be reported.**

Background: Various outreach and public awareness programs have been developed by the agencies involved in the ISE-SAR EE. The purpose of these programs is to support agencies in successfully implementing a comprehensive SAR process while engaging law enforcement agencies, private sector entities, and the public. These programs clearly identify the types of behavior that should be reported and information that adheres to appropriate privacy and civil liberties protections. These outreach and awareness efforts assist in mitigating many concerns about improper police activities.

Some of the programs that have been developed to assist in outreach efforts include the *Safeguarding America: It All Starts With You* DVD and associated material, a joint effort by DOJ and DHS; BJA's Communities Against Terrorism (CAT) program;[31] the Los Angeles Police Department's iWATCH program;[32] and fusion center tip lines and Web sites. Additionally, fusion centers have utilized their Fusion Liaison Officer (FLO) programs as a link to engage public safety and private sector entities and organizations and increase awareness of suspicious activity and what to report to law enforcement. The New York State Police developed a Field Intelligence Officer (FIO) program that is designed to enable local agencies to forward terrorism and other criminal information to the New York State Intelligence Center (NYSIC). FIOs are trained in all aspects of intelligence, including privacy/civil liberties concerns and requirements of the NSI. The Las Vegas Metropolitan Police Department, the Arizona Counter Terrorism Information Center, and others used videos to inform the public about behaviors that should be reported to law enforcement. A public awareness campaign was found to be extremely useful in getting the public and private sector businesses to report relevant and useful information concerning possible criminal activity. Many of the centers worked with privacy advocates when developing their local policies concerning suspicious activity reporting.

> **Recommendation 1:** Agencies engaged in a SAR program should further engage and train their liaison officers to assist in public, private sector, and law enforcement outreach and awareness opportunities. Providing additional training to FLOs utilizing the *Safeguarding America* DVD and providing additional

[31] The Communities Against Terrorism program was created to assist law enforcement in the development of partnerships with community members to make them aware of potential indicators of terrorism activities. Templates of flyers containing potential indicators have been created for law enforcement to distribute to specific industries.
[32] More information about the iWatch program can be found at www.iwatchla.org.

outreach material to the officers to interact with the public and private sector will provide greater awareness of behaviors indicative of potential terrorism activity.

Recommendation 2: Agencies should develop and implement an awareness program for other law enforcement agencies that are engaged in the end-to-end SAR process. This program would assist agencies in the development of a statewide strategy for both the gathering and dissemination of SARs, as well as identify the types of behaviors of which law enforcement officers should be aware. Agencies that have instituted liaison officer programs may use the TLOs to assist in these outreach opportunities.

Recommendation 3: Agencies engaged in a SAR program should consider an active public awareness program to inform the public of specific needs of law enforcement and to build communities of trust. This may include the development and use of tip lines, Web sites, e-mail addresses, and various types of outreach materials, such as the iWATCH and the CAT programs.

Recommendation 4: Law enforcement agencies and fusion centers engaged in a SAR program should develop and implement a private sector awareness program. This program may utilize the CAT program and tenets of the *Safeguarding America* DVD, as well as incorporate TLO programs to assist in these outreach efforts.

Recommendation 5: Resources should continue to be made readily available to distribute as educational tools, such as the *Safeguarding America* DVD and the CAT material, to state and local fusion centers to assist in outreach and awareness efforts. Engagement with other stakeholders and privacy advocates should be conducted on both a national and local basis.

SAR Technical Process

System Deployment Planning

***Lesson Learned:* Agencies must have certain system standards in place to ensure the seamless sharing of information.**

Background: The ISE-SAR EE deployment team followed normal IT business practices and defined a “standard” template to plan each system deployment. The template included a task plan, activities, timelines, and roles and responsibilities. The average deployment time was approximately three weeks. In addition, a preoperational “checklist” was used to ensure that everything was in order technically before each system went live. A host of center management processes and staffing issues unexpectedly impacted the schedule and delivery of the systems. For example, after one center agreed to participate in the ISE-SAR

EE, it then had to formally request permission from a state IT resources board to commit resources. Unfortunately, the board met only once per month. As another example, after agreements were made to reimburse center staff for labor costs to support the installation and testing of hardware and software, the agency's legal counsel requested that a formal memorandum of understanding (MOU) be drafted and approved to document the agreement (to cover about 24 hours of work) before the work could begin. As a final example, the deployment team was advised by another center that according to its state Department of Public Safety, the NCIRC.gov site would have to comply with FBI Criminal Justice Information Services (CJIS) IT Security Standards and submit a 40-page assessment of mandatory requirements. Although the BJA team worked through each of the above issues, impacts to schedule and deployment activities were unavoidable.

> **Recommendation:** Significantly expand the planning phase activities, communications plan, documentation, and schedule to account for all of the fusion center-driven overhead requirements. Ensure that all of the stakeholders, especially senior leadership, are identified and agree to the plan before actual deployment resources are scheduled or significant work begins. In addition to senior leadership, these stakeholders need to include agency management/oversight groups, IT security, center legal/privacy resources, system and network administrative staff, and key end-users.

SITE SYSTEM SOFTWARE AND HARDWARE

> ***Lesson Learned:* A single Shared Spaces site software and hardware solution may not be the best method for implementing a Shared Space technology.**

Background: To support the accelerated schedule for the ISE-SAR EE infrastructure, a Microsoft-based architecture was selected (Windows Server 2003/2008, MS SQL Server 2005/2008, .NET Framework V3.5, IIS Server ASP.NET V3.5, etc.) for ISE-SAR EE sites. Although this configuration matched the skills of the development team, it was not the best or preferred technology fit for several of the sites. For example, of the 14 sites participating in the ISE-SAR EE,[33] 5 sites would have preferred a different operating system (e.g., UNIX), a different relational database management system (RDBMS) (e.g., Oracle), or a different programming environment (e.g., JAVA). In several instances, site IT staff assigned to support the fusion center were familiar with, but not fully competent, in the selected technologies.

Key components of the software architecture require knowledge of Extensible Markup Language (XML) and the National Information Exchange Model (NIEM), specifically the Logical Entity eXchange Specifications (LEXS) formats for Search and Retrieval (SR) and Publish and Disseminate (PD). It was assumed that site IT staff would at some point be able to provide necessary system, network, and database administration services as the project

[33] These 14 sites include the 12 sites, eGuardian, and DHS.

moved forward, replacing contractor staff who managed the initial deployment. As with system software, site IT staff may not have had an opportunity to become proficient in XML or familiar with NIEM and LEXS.

Early on in the ISE-SAR EE, a decision was made to select a standard, economical hardware and software configuration that provided adequate CPU power and RAM and disk storage but also minimized RDBMS license costs. Since most IT centers use rack-mounted equipment, suitable midlevel Dell, HP, and IBM servers were selected. Each center was given some leeway to request modifications to the standard configuration to match existing site standards or preferences. This flexibility was greatly appreciated by the site IT management and helped solidify their acceptance of the ISE-SAR EE. Unfortunately, because of the enterprise nature of the ISE-SAR EE, in terms of internal and external users, CPU-based licensing was required for the RDBMS (MS-SQL Server). Consequently, single CPU servers were purchased for each site for the evaluation period. With the exception of DHS, the FBI (eGuardian), and the Washington, DC, Metropolitan Police Department, who opted for a single-server configuration, all sites requested two servers—a Web server and a database server.

> **Recommendation 1:** The proposed program management office should evaluate the best method of deploying operating systems and examine the pros and cons of other programming languages.
>
> **Recommendation 2:** Specific training courses or targeted technical assistance should be identified to help site staff improve their technical system administration capabilities.
>
> **Recommendation 3:** To support more robust usage, particularly from external users, a second CPU and additional memory should be added to both servers. In order to support traditional system redundancy and higher system availability requirement, the proposed program manager's office should evaluate the need for backup servers.

Data Mapping to the ISE-SAR Functional Standard

> ***Lesson Learned:* Legacy data concerning SAR information at the participating agencies was not in compliance with the ISE-SAR Functional Standard.**

Background: Since the ISE-SAR Functional Standard was developed with input from selected fusion center subject-matter experts, there was a general sense that legacy databases at fusion centers contained most of the information reflected in the standard. At the state level, this assumption was generally true. At the local level, however, there was significant variability from the ISE-SAR Functional Standard since major city urban area fusion centers selected for the ISE-SAR EE had very little of the data enumerated in the ISE-SAR Functional Standard. For those sites that did have fairly comprehensive data, the key

ISE-SAR fields describing "observed behavior," threats, and privacy controls were absent or incomplete. As a result, searches issued by users against other Shared Space databases usually resulted in few or no hits. Compounding the issue was the situation in which one fusion center provided only SARs associated with critical infrastructure incidents. However, data about subjects or vehicles associated with the suspicious activity was not included in the ISE-SAR because the legacy system was designed for another purpose.

> **Recommendation 1:** Evaluate legacy systems at each of the potential future sites and determine whether common vendor products might be candidates for technology improvements to better support the ISE-SAR Shared Spaces data requirements. If found, facilitate meetings with the vendor(s) to evaluate options that might benefit multiple fusion center participants.

> **Recommendation 2:** Deploy the SAR Vetting Tool (SVT) as a bridge between a center's existing RMS or other database used for SARs so that key fields necessary for effective information sharing can be populated or augmented by fusion center staff before ISE-SARs are stored at that center's shared space. This common tool should continue to be supported by the proposed program manager's office.

Lack of Structured Data in Legacy SAR Records

> ***Lesson Learned:* Structured data was not available at most participating agencies for the population of the Shared Space data fields.**

Background: This problem impacts many records management systems in use today and reflects the reliance of most agencies on paper forms used by frontline officers to record details of suspicious behavior as well as any other incident that the officer may be documenting. Even if online systems provide specific fields to capture names, vehicles, and other descriptive structured data, users of those systems frequently just enter a free-text narrative of the incident. This tendency defeats initiatives to improve the mapping of data and frustrates users trying to search multiple Shared Spaces using structured fields. Having to search long strings of narrative text takes time and often results in the retrieval of records that have no true relationship to the actual subject of the search.

> **Recommendation 1:** At the analyst level, enforce data quality standards and request that structured data fields be updated as necessary (e.g., suspicious activity codes, subject names, location data, threat codes) even if the information is also included in a narrative description. The SVT could be used to support this task. In practice, the number of ISE-SARs that might require additional quality checks and data entry is quite low and does not represent an excessive burden to any fusion center participating in this initiative. The proposed program manager's office should provide support to accomplish this recommendation.

Recommendation 2: As part of a technology refresh cycle, examine new technology that might support more powerful text recognition and search algorithms to be applied to each shared space database upon the ingest of ISE-SAR records that would significantly improve the speed and quality of search operations.

SITE SHARED SPACE DATABASE DESIGN

Lesson Learned:* *The database design at each site may not be robust enough to support a wider deployment to users nationwide.

Background: Because of the pilot nature of the ISE-SAR EE, the common ISE-SAR Shared Spaces database structure was organized based upon the ISE-SAR Functional Standard but normalized to improve efficiency from a search perspective (search fields were limited). However, the database was fully compliant in terms of the NIEM-based content and format within the LEXS-SR standard. This was accomplished by building the LEXS/NIEM record upon data ingest into the Shared Spaces repository so that if queried by a remote NCIRC.gov user, the CPU time necessary to build query results would be minimized. Although this approach worked for the limited-use ISE-SAR EE, additional analysis is necessary to support a production environment.

Recommendation 1: Verify the database design, broaden searchable parameters, conduct performance modeling and tuning activities, and perform some level of stress testing, with particular focus on sites that are hosting the SAR Vetting Tool (SVT) application on the ISE-SAR Shared Spaces Database server.

Recommendation 2: Modify the database schema to include all information exchange package documentation (IEPD) fields to provide for attachments and other desired meta-data that will improve the robustness of ISE-SAR records maintained at each site.

Recommendation 3: Include indicators on each IEPD data element that identify it as a “privacy field” based on the IEPD and augmented by state or local statute or policy.

Recommendation 4: Conduct a review of the database schemas for all systems that will feed into the shared space to ensure compliance with the ISE-SAR Functional Standard.

Deployed Shared Space Applications

***Lesson Learned:* No common process for extracting, transforming, and loading legacy data was available.**

Background: For the ISE-SAR EE, various approaches were taken to import data from legacy systems into the Shared Spaces database. These approaches generally included both reusable components and custom components to support the overall extracting, transforming, and loading (ETL) process. Primarily, two approaches were used: (1) processing an input file containing candidate records with a traditional ETL script and (2) using a database replication approach in which the source database pushed an extract to a staging area on the Shared Spaces database for subsequent processing and loading in the Shared Spaces repository. A third approach was created for processing records from the SVT. Two additional approaches were discussed but not implemented in the pilot: a Web service option to allow legacy systems to push candidate SARs to the Shared Spaces and an approach involving a direct query of a legacy database from the Shared Spaces to “pull” records designated as candidates for sharing with ISE-SAR EE members.

Recommendation 1: Create an interface toolkit that fusion center IT staff or other law enforcement agencies might use which contains various proven and documented applications to process SARs into a Shared Spaces database.

Recommendation 2: Provide the capability to ingest attachments as part of the ISE-SAR record, if available from the legacy system.

Recommendation 3: Reevaluate the current Shared Spaces database “smash and replace” approach to see whether other options might be possible that still preserve the integrity of the Shared Spaces but improve the timeliness of ISE-SARs being made available to the user community. Other options could include Add, Update, Hide, and Purge features that would act upon individual SAR records being pushed to the Shared Spaces. This approach may better support situations in which multiple legacy systems are feeding a single Shared Space database, such as the situation envisioned by DHS.

Recommendation 4: Design and implement an automated approach to provide feedback to users who may have retrieved SAR records from a site’s Shared Space on earlier searches that a previously viewed SAR has been purged from that site’s Shared Space.

Recommendation 5: Evaluate the feasibility of a subscription-based alerting capability that would provide two basic functions.

1. Alert users when they add a new ISE-SAR to their Shared Space that a possible related SAR exists in another fusion center's Shared Space.

2. Allow an analyst at a fusion center to request notification when any fusion center adds an ISE-SAR to its Shared Space that meets basic criteria established by that user.

While the "smash and replace" technique discussed above in Recommendation 3 complicates the design of this alerting capability, the ability to receive notifications automatically without the need to manually search the Shared Spaces periodically could provide significant benefits to the analyst community.

System Deployment Process

***Lesson Learned:* Preplanning readiness and postdeployment checklists were beneficial to the installation of systems at each site.**

Background: Overall, the deployment of computer systems and software at most of the ISE-SAR EE sites went surprisingly well, primarily due to a series of readiness check telecoms in the weeks and days leading to the on-site visit. In every case, site personnel agreed to install the servers and VPN in their facility and support connectivity and application testing. In addition, on most occasions, IT staff also loaded the server system and database software. Some delays were experienced at sites where the fusion center relied upon state or city IT for support and additional coordination was necessary. The process and sequence of tasks was proven to be effective.

Recommendation 1: Document the process and include templates for future use, including a more extensive checklist to cover unanticipated issues and/or constraints both before and after system deployment.

Recommendation 2: It is imperative that specific points of contact for all facets of the Shared Space support be provided and maintained. This will assist not only with the setup of the Shared Space for that location but also in addressing any issues arising in the everyday operation and ability to connect to that location.

Use of Existing Report Forms

***Lesson Learned:* Modification of existing law enforcement reporting forms eases the implementation of the ISE-SAR EE project in the participating agencies.**

Background: One of the major challenges for agencies when implementing a SAR process within an agency is getting the reported suspicious activity from the patrol officer or other person taking the initial report to the unit charged with analyzing the information. Rather than creating a new form or implementing a new process, the agencies modified currently used forms and processes, which made the process more acceptable to the officers initially taking the information.

The Los Angeles Police Department (LAPD) modified its existing Investigative Report used by officers to report crimes as previously described in the report.

The Washington, DC, Metropolitan Police Department initiates a SAR whenever a crime or incident report in the field is tagged as involving suspicious activity. This cataloging occurs when a box on the report labeled "Suspicious Activity" is checked. As Terrorist Incident Prevention Program (TIPP) forms and crime/incident reports are reported to MPD and identified as suspicious, they are immediately forwarded to the Intelligence Fusion Division (IFD) for review and analysis by a trained analyst.

> **Recommendation:** Agencies implementing a SAR process within their agency should review current processes and modify existing forms and processes to simplify internal reporting.

Review of Legacy SAR Data

> ***Lesson Learned:* Legacy SAR data should be carefully reviewed before it is shared in the ISE-SAR Shared Spaces.**

Background: The three initial agencies to place data into the ISE-SAR Shared Spaces had legacy SAR systems that contained several years' worth of existing data. The New York State Intelligence Center, the Virginia Fusion Center, and the Florida Fusion Center all loaded their legacy data into the ISE-SAR Shared Spaces system. In an effort to test the system, a comprehensive review was not conducted on the existing legacy data to ensure that all the data met the four-step process required by the ISE-SAR Functional Standard. After reviewing the legacy data tagged for sharing in the ISE-SAR Shared Spaces, it was determined that a comprehensive review needed to be completed on each individual SAR contained within the legacy systems.

> **Recommendation:** Agencies that have a legacy SAR system with stored data should complete the four-step process required by the ISE-SAR Functional Standard before tagging the data to be included in the ISE-SAR Shared Spaces.

INTERFACE WITH THE FBI'S EGUARDIAN AND DHS'S SHARED SPACE

> ***Lesson Learned:* Building interfaces to the FBI's eGuardian and DHS's Shared Space allowed for a single search interface for local, state, and federal users to access all SAR data and to operate with a common understanding and process.**

Background: The ISE-SAR Shared Space concept was designed to allow the systems to share information while allowing the submitting agencies to maintain control of their data, and all agencies would be able to implement the processes and policies enumerated in the ISE-SAR Functional Standard. One of the project challenges was how to share information with the FBI and DHS without having to utilize different systems or processes.

The solution was twofold: build Shared Space servers for use by the FBI and DHS to allow them to share their data with other users from a single interface and build a utility into eGuardian that allows state and local agencies to share data with eGuardian via the Shared Spaces user interface. Users who place SAR data into their Shared Space server can tag the data to be uploaded into eGuardian, which allows the SAR information to be shared with the FBI's Joint Terrorism Task Forces.

> **Recommendation:** The FBI and DHS should continue to support the interface with the Shared Space environment to allow continued ease of sharing SAR data with all law enforcement agencies.

NCIRC.GOV PORTAL USER INTERFACE

> ***Lesson Learned:* During the ISE-SAR EE, it was determined that the User Search functionality may need to be evaluated and enhanced to ensure that it can meet the technical and functional requirements of any future national rollout of this project.**

Background: As with other facets of the ISE-SAR EE software architecture, the user interface evolved as the project moved forward. Functional and relatively easy to use with a small number of records in the Shared Spaces, the user interface was designed to quickly permit information sharing activities between participating sites. However, to allow for an early deployment of Shared Space search capabilities, user interface functions were constrained when compared to other similar search tools used by law enforcement agencies, such as "read-only" restrictions, lack of analytics or geospatial visualization, lack of attachments, lack of role-based access mechanisms, and limited workflow and query results navigation.

Although the SAR User Search functionality is accessed through the NCIRC portal, it is not the only application or information source available on the portal. Recommendations in this document refer only to the SAR User Search functionality.

Recommendation 1: A group of subject-matter experts, to include analysts, should be utilized to establish firm user interface requirements, conduct a gap analysis against the ISE-SAR EE user interface, and document an enhancement plan for the user interface.

Recommendation 2: Upon completion of the gap analysis, evaluate the desirability of providing a Shared Space Search LEXS-SR-based Web service capability to allow existing fusion centers to conduct searches of ISE-SARs using existing legacy records management systems or case management systems instead of having to physically log on to the NCIRC site. This option, though technically feasible under the LEXS-SR standard, introduces possible privacy and civil liberties concerns that need to be considered.

Recommendation 3: Evaluate the use of commercial or government off-the-shelf technology or portal tools to assist in the integration of additional functional capabilities, with particular focus on the user-interface challenges of federated searches against numerous databases (potentially up to 72). Other capabilities should include the integration of analytical tools, inclusion of attachments in query results (images, documents, video and/or audio, etc.), storing retrieved results (perhaps only temporarily in a personal queue or file), screen personalization, and other techniques to avoid information overload.

Recommendation 4: Provide a report generation capability so that users can create various reports based upon the results of ISE-SAR Shared Space searches. This capability would allow users to tag individual retrieved records to be included in a report. Consideration should be given to making these reports "read only" to preserve the ownership of the data for the contributing agency.

Recommendation 5: Provide a capability to search audit logs based on various criteria—such as monitoring of system use, enforcement of security and privacy policies, and performance management—and produce a series of formatted reports. This feature would be restricted to management users.

Case 3:17-cv-07357-RS Document 70-3 Filed 05/12/21 Page 160 of 301

LEVERAGING PROMISING PRACTICES

The agencies involved in the Information Sharing Environment-Suspicious Activity Reporting Evaluation Environment (ISE-SAR EE) are professional and respected law enforcement agencies. A significant component of the project was the ability to observe and codify critical enabling activities of these agencies and adopt the promising practices for use where appropriate. During the course of this project, an initial analysis of four major city police departments in Los Angeles, California; Boston, Massachusetts; Chicago, Illinois; and Miami-Dade, Florida, revealed a number of promising practices regarding the gathering, processing, analysis, and sharing of SARs. These promising practices were instrumental in the foundation of the project and were shared through the ISE-SAR EE user group to be replicated as the project was implemented. Additionally, a number of promising practices were documented and shared in professional journals in the law enforcement community. Below are some of the significant promising practices identified during the course of the Evaluation Environment.

These promising practices were discussed at all user group meetings and conference calls, as well as shared in the monthly newsletter to all participating agencies. Many of the promising practices were discussed and refined and later adopted by many of the users. All partners agreed that this was critical to establishing common practices and procedures for handling SAR information.

EXECUTIVE LEADERSHIP

Critical to the success of any program is the support from the agency's executive leadership. However, it takes more than just a word of encouragement or a statement of support; there must also be an active commitment to ensure that the agency's members, the public, and other government policymakers are informed and supportive of the operation. Executive leadership should visibly and regularly support the adoption and implementation of an agency SAR process. Without the agency leadership's continued sponsorship and a sense of importance, it will be increasingly difficult to knit together all the process pieces over time.

The Los Angeles Police Department's (LAPD) leadership took an active role in developing a comprehensive program to collect, analyze, and distribute suspicious activity information related to terrorism. The chief of police at the time of the initiation of the ISE-SAR EE shared the lessons learned from LAPD with other agencies nationwide. LAPD frequently provided staff members to cross-train other SAR agencies regarding their behavior codes and SAR processes. Presentations were made by LAPD representatives to police organizations such as the International Association of Chiefs of Police (IACP) and the Major Cities Chiefs Association (MCCA), as well as members of Congress and officials in the White House. These efforts were a major impetus in the development of the NSI. LAPD developed an agency-wide General Order, amended its incident report to simplify the reporting of suspicious information, created a SAR Unit with the responsibility to analyze the information, and communicated to the organization the importance of the SAR process. All of its efforts created a synergy that led to other innovative concepts for developing and analyzing terrorism-related information.

The director of the Miami-Dade Police Department provided a SAR brief on two separate occasions to the local Chiefs of Police Association. This was part of a larger process to obtain support from various law enforcement and other government agencies in the South Florida area. The Miami-Dade Fusion Center has trained various county government departments—including fire, emergency medical services, aviation, and public works—on the process of the SAR program and how to report suspicious activity to the fusion center. The director has also supported the creation of the South Florida Virtual Fusion Center, which provides a platform for all agencies in the South Florida area to participate in the sharing of terrorism-related information throughout the region.

The chief of police of the Seattle Police Department and the sheriff of the Las Vegas Metropolitan Police Department were principal participants in the efforts of the MCCA to develop recommendations for a nationwide SAR process. The MCCA, through its Intelligence Commanders Group, helped spearhead the SAR effort among law enforcement agencies in the country's major cities. Without this initiative, efforts to establish a nationwide process for sharing of SAR information would have been greatly hampered.

The chief of police of the Washington, DC, Metropolitan Police Department was often called upon to represent the interests of law enforcement agencies nationwide in articulating policies needed to ensure that suspicious activity information was being collected and evaluated throughout the country. The chief represented local law enforcement agencies nationwide before Congress and the White House. The police department also had a major role in the supporting preparations for the Inauguration of a new President and was able to test many of the concepts being developed by the project. The lessons learned from those efforts were shared with project participants to better develop their own policies.

Shared Space Concept

At the onset of discussions concerning the sharing of terrorism-related suspicious activity, there was concern by many of the state and local law enforcement agencies regarding the impact of state and local laws, rules, and regulations governing the sharing of information. There was a concern about the agency's ability to maintain control of the information if the information were placed in a data warehouse. Consequently, the concept of Shared Spaces was built to provide both the ability to share SAR information and ensure that the originating agency would retain control of the information developed by its agencies. This concept allows participating agencies to select the information they are willing and able to share and place it in a "shared space" server. Although other technology solutions could have been employed, the shared space servers were developed to be maintained by the originating agency but made accessible for search by a common user interface available to all agencies involved in the project. The following are the agreed-upon attributes that were keystones to developing the shared space:

- The data contained in ISE-SAR Shared Spaces is not intended for use in statistical research and/or reports. Participants are not able to download the shared data in order to ensure that outdated data will not be stored in systems outside of the participating agency's system.
- The ISE-SAR Shared Spaces database is not a criminal intelligence system or database.
- The data in ISE-SAR Shared Spaces is managed and maintained (controlled) by the submitting agency, which is operating under individual state and local jurisdictional laws and policies.
- Data in ISE-SAR Shared Spaces is accessible by authorized ISE-SAR EE participants in fusion centers, law enforcement agencies, Joint Terrorism Task Forces (JTTFs), and Federal Bureau of Investigation (FBI) Field Intelligence Groups via the Sensitive But Unclassified (SBU) networks that provide secure communication.
- Vetting of data for inclusion in the ISE-SAR Shared Spaces should include contact with the local JTTF/National JTTF and the Terrorist Screening Center (for Violent Gang and Terrorist Organization File queries) in order to determine whether current investigative activity is ongoing.
- The query provides the opportunity for a search of all selected ISE-SAR Shared Spaces, to include eGuardian and the U.S. Department of Homeland Security (DHS) Shared Space servers as resource availability allows.
- The user interface utilizes commonly accepted, secure Internet-based technologies.
- Items presented in the initial results list displays submitting organization, contact information, and ISE-SAR information.
- Selection of a record from the query results list retrieves the specific ISE-SAR identified in that selection.
- An audit log is used to capture search transactions at a central query site and agency database.
- User access to the ISE-SAR distributed search is provided utilizing the secure government networks: Regional Information Sharing Systems Secure Intranet (RISSNET), Homeland Security Information Network (HSIN), and Law Enforcement Online (LEO).
- Shared-space ISE-SAR systems provide a uniform data representation of agency data based on the ISE-SAR Functional Standard.

- A capability is provided to allow agencies to forward designated SARs to the eGuardian system from the shared space environment.

The SAR Vetting Tool

In developing the ISE-SAR Shared Spaces concept, it was anticipated that SAR information could be extracted from each agency's legacy database and submitted to the ISE-SAR Shared Spaces. However, it was determined that many of the participating agencies did not have a separate SAR database that could be utilized to analyze SAR information before it was shared with the other agencies. Several agencies had the data in multiple databases, and others used paper processes to analyze and store the information. To this end, the ISE-SAR EE technical team developed a SAR Vetting Tool (SVT) for use by the participating agencies that did not have a sufficient legacy system to support the sharing of information in the Shared Spaces environment. This is a technology that can continue to be refined and utilized as this concept is implemented nationwide. Significant development assistance for the SVT was received from the police departments of Boston, Massachusetts; Miami-Dade, Florida; and Chicago, Illinois. These agencies outlined the specifications needed for this type of tool and were instrumental in the technical team's implementation of the SVT.

This tool was developed using common database standards and protocols, which allowed for quick development and deployment. Using the input from analysts from the participating agencies, the team developed a method to import data from multiple systems, allow for manual information input, and ultimately track the vetting of the information to ensure compliance with the ISE-SAR Functional Standard. Now developed and deployed, the SVT can easily be replicated and distributed to additional participants.

Use of National Information Exchange Model (NIEM) and Logical Entity eXchange Specifications (LEXS)

The National Information Exchange Model (NIEM) is a partnership of DOJ and DHS. The model was built from the foundational elements of the Global Justice XML Data Model and its companion documents, training, and technical support mechanisms. It is designed to develop, disseminate, and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations, as well as support the day-to-day operations of agencies throughout the nation. NIEM enables information sharing, focusing on common processes and definitions for information exchanged among organizations as part of their current or intended business practices. This model and its associated business processes were developed by more than 50 state and local participants.

DOJ established the Law Enforcement Information Sharing Program (LEISP) to achieve the Department's vision of creating relationships and methods for sharing criminal information routinely and securely across jurisdictional boundaries. The LEISP developed the Logical

Entity eXchange Specifications (LEXS), which is a family of Information Exchange Package Documents that implement NIEM for many common types of law enforcement information exchanges. LEXS specifies how law enforcement information should be packaged and delivered to information sharing applications and how partnering applications can implement federated search capabilities.

All of the applications utilized in the ISE-SAR EE were built utilizing these common data sharing standards. The ISE-SAR Shared Spaces database, the SVT, and the FBI's eGuardian system all utilize these standards, which allow for the ease of sharing law enforcement information. Because these standards were utilized during development, these systems can now easily be used to accomplish additional information sharing based on these common standards.

Leveraging Existing Secure but Unclassified Networks

Critical to the success of any law enforcement information sharing system is the ability to provide security for the information during storage and transmission. When access protocols for the shared space concept were designed, it was determined that access to information needed to be provided over a secure network that would protect the information and provide for user authentication. Three SBU networks were identified as being suitable for this function: the DOJ-supported RISSNET; the FBI-supported LEO; and DHS-supported HSIN. Each of the participating agencies had access to all three networks.

Access to the Shared Space query tool user-interface is supported using all three of the secure networks. This is the first time a single application was accessible by all three networks. Participating law enforcement agencies were concerned about the creation of another system requiring another set of usernames, passwords, and credentialing. The creation of an interface among the three SBU networks to a single application made for an easy and common method for user access and authentication to the system.

Development of Privacy Policy Templates and Technical Assistance

Central to the design of this project was adherence to the ISE Privacy Guidelines. Many agencies had policies in place that were designed to guard the privacy and civil liberties of individuals. However, it was determined that a more comprehensive privacy framework concerning safeguards for the sharing of suspicious activity reports would be needed for use by all participating agencies. Aimed at protecting privacy rights and civil liberties, these safeguards were intended to avoid the gathering, documenting, processing, and sharing of information such as race, ethnicity, national origin, or religious preference that has no reasonable relation to the criminal activity.

The project team provided subject-matter experts to review the privacy policies for each of the pilot sites. The reviews were made to ensure that the policies were consistent with the applicable requirements of the ISE Privacy Guidelines. Additionally, technical assistance was provided to all sites to assist in the development of the policies. As a result, all participating agencies are utilizing privacy policies that are common and acceptable by all participants.

Development of a SAR Training Program

Training was recognized as critical to the successful implementation of the Nationwide SAR Initiative. The ISE-SAR Functional Standard outlines a new set of protocols and standards that need to be utilized by law enforcement before SAR information can be shared among the agencies nationwide. Therefore, three levels of training were designed and implemented to ensure that agency personnel at all levels had a clear understanding of what information was to be collected and shared in the ISE-SAR EE. Additionally, it was important to reinforce the need to protect individuals' civil rights and civil liberties. A collaborative design method was established utilizing the MCCA, the IACP, and the Bureau of Justice Assistance (BJA) to develop the three different levels of training and deliver to all the participating agencies.

Participating agencies also developed training to meet their local needs. The Los Angeles Police Department built regional awareness of SARs by providing training to local law enforcement partners, including the Los Angeles Port Police, the Los Angeles Unified School District Police, the Los Angeles Airport Police, and the City of Long Beach Police. All command staff were trained on the agency's Special Order, with follow-up briefings and PowerPoint presentations at general staff meetings. LAPD developed a training framework for the training of every officer in the development and submission of SAR reports. Training programs—including e-learning, PowerPoint presentations, and roll call presentations—were developed and provided to all command staff, new recruits, and civilian and sworn personnel before the implementation of the SAR process.

All officers of the Houston Police Department have undergone a four-hour training course on terrorism indicators and have been trained on identifying suspicious activity. The training course includes privacy protections, and the need for a criminal nexus when reporting suspicious activity. The Houston Regional Information Service Center (HRISC) has conducted a terrorism indicator training program for private sector personnel, including oil industry officials.

Analyst Professional Development

The analytic function is a critical component of the Nationwide SAR Initiative. The ISE-SAR Functional Standard calls for a four-part analysis and vetting process to ensure that information developed by a law enforcement agency concerning potential terrorism activities meets the criteria to be shared in the ISE-SAR Shared Spaces. Although most law enforcement agencies have long had well-developed training programs for sworn officers, developing high-level training programs for criminal intelligence analysts is a more recent development.

The Florida Department of Law Enforcement (FDLE) previously developed a six-week law enforcement analyst training program that has been delivered to more than 400 state, local, and federal law enforcement intelligence analysts in the state of Florida. The course delivers training in the following areas:

- Intelligence Analysis and the Intelligence Process
- Analysis and Analytical Processes
- Data Management and Analysis
- Effective Briefings and Teamwork
- Crime-Specific Investigations and Analysis

An important component of the Analyst Academy Program is the continuing education opportunities. The department took the BJA-developed analyst training course and delivered it to more than 100 Analyst Academy graduates representing 36 state, local, county, and federal agencies.

The New York State Intelligence Center (NYSIC), working with DHS, developed an analyst professional development program that includes analytic training as well as a mentoring program. The department created an analyst development workbook that allows the agency to track the professional development of its analysts to ensure they have received the appropriate level of training needed to conduct the analytic process.

Utilization of Roll Call Training and E-Training Programs

Law enforcement agencies have long used roll call training as a method of delivering important information to patrol officers without having to take them away from their normal patrol duties. Although it varies in different agencies, roll call training is generally a brief training delivery that emphasizes a particular issue determined to be important by the agency command. Agencies are increasingly using some form of electronic training to fulfill this training need. This method of training provides an excellent way for patrol officers to understand the tenets of the Nationwide SAR Initiative and their critical role in the process.

The Miami-Dade Police Department provided in-person roll call training to all districts and shifts. The training was provided on the SAR effort by the commander of the Homeland Security Bureau. This provided the bureau the opportunity to answer all questions and to stress the importance of the street officers providing the information according to department protocols. The officers were also informed of privacy concerns and the need for the suspected information being reported to be based upon the activities identified in Part B of the ISE-SAR Functional Standard.

The Washington, DC, Metropolitan Police Department had the task of providing training to its own officers and the visiting out-of-area officers who would be participating in law enforcement details associated with the 2009 Presidential Inauguration. The department developed a roll call training stressing the behaviors to be reported to the fusion center. The training was delivered via an online system due to the need to provide the training to thousands of officers in a short period of time.

The Chicago Police Department disseminates suspicious activity alerts, warnings, and notifications via intelligence bulletins to all law enforcement officers, as well as selected managers of critical infrastructure and other government agencies. The distribution of these reports includes the command staff, the Deployment Operations Center's Web site, roll call distribution in each district office, the LEO Special Interest Group, Homeland Security State and Local Intelligence Community of Interest, and RISSNET.

Liaison Officer Programs

It is important that fusion centers and agency intelligence bureaus have appropriately trained officers from other sections and departments who are trained in the intelligence process to assist in the collection and reporting of information needed for the intelligence process. Many agencies have developed formalized programs to select and train the officers who become an extension of the fusion center or intelligence bureau. Called Terrorism Liaison Officers (TLOs), Intelligence Liaison Officers, or Field Intelligence Officers, each performs an important role in the ISE-SAR process.

The state of Arizona has developed an extensive cadre of TLOs throughout the state who are both law enforcement and other emergency response personnel. These individuals serve as primary contacts with local agencies to develop and report suspicious activity information. These TLOs may enter information directly into the center's database, which promotes the development of a SAR within the fusion center.

The Chicago Police Department has a TLO program consisting of officers selected from all 25 districts and units, one per watch—approximately 80 members of the department. These officers meet quarterly, have organized training programs with guest speakers, and keep lines of communication open with the department's Deployment Operations Center. These officers also function as distribution points for information to be delivered to the street officers in the department.

LAPD has a highly developed TLO program within the department. Every division office has at least two officers trained for that function. In addition, the department has trained a number of TLOs to interact with other government agencies to assist the Counter Terrorism and Criminal Intelligence Bureau in the implementation of the SAR process within their own agencies and in the community. TLOs are responsible to liaise with officers at their assigned LAPD division, as well as with other government agencies and local business partners within their area of responsibility. The TLOs are utilized to provide feedback to the officers and/or local agencies or business partners who originally submitted the SAR data. In addition, the Bureau Commander provides personalized e-mails and written commendations in response to SAR reports that have been received.

NYSIC has developed a Field Intelligence Officer program consisting of 1,600 officers, representing 85 percent of the state's law enforcement agencies. These officers also deliver training to the business community through the department's Operation Safeguard program using tools developed by BJA, such as the *Safeguarding America—It All Starts With You* video training for first responders and the Communities Against Terrorism program. An example of the success of the program is a report of suspicious activity that was provided by a business that was a recipient of the training:

> *In May of 2009, an employee noticed something unusual while working at a self-storage facility. A group of suspicious-looking men had begun to meet around an outdoor storage unit. They aroused suspicion because they met frequently—as much as 20 or 30 times in the span of a few days. They were also very careful to conceal their property by backing their SUV right up to the storage unit door. The self-storage facility had been visited by local law enforcement in the past and had been provided information on indicators and warnings of suspicious activity as part of the New York State's Operation Safeguard outreach program. The employee contacted the local police department to report the suspicious activity observed. He also provided them with information on the vehicle and renter. The police department ran checks and found that the New York FBI Joint Terrorism Task Force (JTTF) had an active investigation and the individuals associated with the storage unit were currently under surveillance. Two weeks after the employee's report, the New York JTTF arrested four men on a number of terrorism charges, including charges arising from a plot to detonate explosives near a synagogue and to shoot military planes with Stinger surface-to-air guided missiles. The employee's information demonstrated the effectiveness of the Operation Safeguard efforts to help prevent terrorist attacks in New York State.*

COMMUNITY OUTREACH

Incorporating the community into the SAR process is very important to build trust and support for the agency's SAR program. There is a need to clearly identify the types of information that should be reported to law enforcement by the community and to stress the importance of adhering to appropriate privacy and civil liberties protections. These outreach and awareness efforts should assist in mitigating many concerns about improper police activities.

FDLE has developed several methods of reaching out to the public. The state has developed the BusinesSafe Web site for use by private industry in the state of Florida to inform them of terrorism-related concerns and to provide a method for supplying information to the Florida Fusion Center. FDLE's Computer Crime Center maintains a "Secure Florida" Web site to provide information about cyber security to the public and the state's business community.

HRISC has an outreach program with the public and has conducted community meetings, trained members on the Crime Stoppers program, and coordinated with the Houston-area JTTF, which operates a tip hotline that the public may use to report suspicious activity. HRISC also works with the U.S. Attorney's Office and the Anti-Terrorism Advisory Council to provide outreach to the private sector and has provided training to human trafficking/ smuggling enforcement groups. Special training has been provided to the area's petrochemical industry because of its major presence and potential to be a target of a terrorist attack.

LAPD introduced the SAR program to the community through Community Forums and meetings, and there is a unit within LAPD that specifically deals with community outreach. The program educates the public on what suspicious activities are, the behaviors and indicators of suspicious activity, and the need to report suspicious activity. The program introduces a Web site (www.iWATCHLA.org) for national application to be used for the reporting of suspicious activity. The Web site is the central site/host for a network of informational reports on past terrorist-related acts, terrorism indicators, case studies, and other such educational tools currently available through open source networks. The Web site provides links nationwide to local law enforcement agencies and notifications to various sectors.

LAPD has also developed media commercials to explain how the SAR program works and the need to report information concerning terrorism to the police department. LAPD TLOs also share in the responsibility to make presentations to community groups and other interested sectors concerning the reporting of suspicious activity. The American Civil Liberties Union was involved with the development of the iWATCH program and provided comments on the script of the Public Service Announcement. Informational flyers have also been developed for release at the community trainings, and a DVD was developed that relates to the reporting of suspicious activity and contains all the information found on the Web site.

NYSIC works closely with the New York Office of Homeland Security, which maintains a public Web site (http://www.security.state.ny.us) to conduct community outreach. NYSIC uses the "If you see something, say something" program to inform the public as to what actions they should take if they see suspicious activity. Additionally, the Operation Safeguard initiative was created to inform the private sector on suspicious activities that should be reported to law enforcement and the state's Field Intelligence Officers.

The Seattle Police Department is heavily involved in the Northwest Warning, Alert and Response System Web site (NW-WARN), which is designed to provide real-time alerts and warnings to both government and private sector partners. Information developed by the fusion center and determined to be important for distribution to the other partners is distributed over this closed system. The Web site provides the capability for those partners to provide SARs and other crime-related information to the fusion center.

The Washington, DC, Metropolitan Police Department has a robust community and business community outreach program. The department conducted a Homeland Security Emergency Management seminar, which was a public and private sector event that attracted 100 people. The representatives discussed how to recognize and report suspicious activity. The department has also distributed the SAR tip information to storage facilities, pharmacies, and several hotels to help these entities understand how to recognize and report suspicious activity. Billboards on buses have also been utilized to explain how to report SARs.

The Arizona Counter Terrorism Information Center (AcTIC) has developed a DVD for distribution to the public and first responders, titled *8 Signs of Terrorism*, which educates the public about what to look for and report regarding terrorism-related suspicious activity. The center also maintains a public Web site (http://cid.dps.state.az.us) that provides information for the public and explains the operation and mission of the state fusion center: "The mission of the AcTIC is to protect the citizens and critical infrastructures of Arizona by enhancing intelligence and domestic preparedness operations for all local, state, and federal law enforcement agencies. Mission execution is guided by the understanding that the key to effectiveness is the development and sharing of information between participants to the fullest extent as is permitted by law or agency policy."

Based on the experiences gleaned from this project, BJA and PM-ISE developed the Building Communities of Trust project. This project focuses on developing relationships of trust between police, fusion centers, and the communities they serve, particularly immigrant and minority communities, so that the challenges of crime control and prevention of terrorism can be addressed. Effective crime control and the prevention of terrorism require meaningful sharing of information among police agencies and between the community and police. Underlying information sharing are a number of important federal initiatives that seek to support an effective information sharing environment, reflecting full transparency and protection of privacy rights and civil liberties of all people. This initiative seeks to explore the intersection of three critical partners—the community, local law enforcement, and fusion centers—in our nation's framework to improve information sharing and protect our local communities. The knowledge about communities that comes from trust-based relationships between law enforcement and the local community is critical, because it allows law enforcement officers and analysts to distinguish between innocent cultural behaviors and behavior indicative of criminal activity.

The project stressed the importance of providing a robust outreach program. The ISE-SAR EE outreach reached a multitude of agencies and organizations, including:

- 2008 and 2009 National Fusion Center Conference: Presentations, Exhibits, and Hands-on-Lab Demonstrations
- 2007–2009 Regional Fusion Center meetings: Presentations and Resource Materials
- 2008–2009 Global Justice Information Sharing Initiative Advisory Committee: Semiannual Status Updates
- CICC: Quarterly Status Updates
- PM-ISE Leadership: Quarterly Status Updates
- NIEM Program Management Office: Periodic Status Update
- 2008–2009 IACP Annual Conference
    - Major Cities Chiefs Executive Committee: Presentations and Resource Material
    - Railroad Police Section: Presentation and Resource Material
    - University and College Committees: Presentation and Resource Material
    - Police Investigative Operations Committee: Presentation and Resource Material
    - Intelligence Coordination Panel: Presentation and Resource Material
    - Homeland Security Committee: Presentation and Resource Material
    - Criminal Justice Information Systems Committee: Presentation and Resource Material
    - Hands-on-Lab Demonstration of the SVT and SAR Search Tool
    - Facilitation of Breakout Panel regarding ISE-SAR EE
- Other National Law Enforcement Organizations:
    - Major Cities Chiefs Association: Presentations and Resource Materials
    - Major County Sheriffs' Association: Presentations and Resource Materials
    - National Sheriffs' Association: Presentations and Resource Materials

These outreach opportunities were often led by state and local participants who were able to share their experiences, promising practices, and lessons learned to a large population of the law enforcement community.

Institutionalization of Processes for the Handling of SAR Information

It is important that consistent processes be developed nationwide to ensure consistency in the collection and sharing of SAR information. Internal agency policies are very important in successfully implementing an agency-wide process to ensure that all agency members understand their role in gathering and analyzing suspicious activity reports. Written policies should be very specific as to the internal flow of SAR information and to reinforce the need to respect civil rights and civil liberties concerns when gathering, analyzing, and disseminating SARs.

The Arizona Counter Terrorism Information Center (AcTIC) has a policy to explain its use of the center's Suspicious Activity Reporting System. After an entry is made, it is electronically sent to an investigative supervisor, who reviews the information for investigative content and assigns it to an investigator/analyst. The Watch Center Supervisor reviews all SAR report entries daily for completeness and potential terrorism nexus and continuously monitors and assesses situational awareness to determine if suspicious activity is present in any reporting coming in to the center. The SAR Gatekeeper reviews all entries daily for the standardized behavior-specific activities, and if they are present, the entry is coded as a SAR and prepared to be pushed to the ISE-SAR Shared Spaces.

The Houston Police Department's General Order No. 800-07, Criteria for Submitting Incident Reports, has a section on suspicious activity. The General Order requires all information to be initially reported to the department's Criminal Intelligence Division, where it is analyzed to determine the type of information it contains and where the information should be routed within the department. By this process, the Houston PD is able to take an "all crimes" approach to monitoring suspicious activity and ensure that terrorism-related suspicious activity is properly monitored and forwarded for appropriate follow-up. All terrorism-related information is routed to the fusion center. The fusion center has a process in place to review all SAR data consistent with the agency's privacy framework. A fire program is now being added to this routing process so that information from the fire department will be routed to the fusion center.

LAPD modified its existing Investigative Report used by officers to report crimes. Three simple changes were made: the addition of a check box to identify as a SAR report, a check box for distribution to the Counter Terrorism and Criminal Intelligence Bureau (CTCIB) Major Crimes Division (MCD), and a check box for "Involved Party (IP)" information. Modifying an existing report that officers were familiar with simplified the introduction of the SAR process throughout the department. All SARs are forwarded to the MCD SAR Unit for processing and analysis. The SAR Unit is the centralized unit responsible for updating all incoming SARs with the SAR modus operandi codes, tracking for status, vetting, and investigative assignment. Vetting includes informing the FBI of those SARs that meet the criteria. A SAR is first reported by a line officer and reviewed by a supervisor. Both officer and supervisor have been trained in recognizing the behaviors and indicators that terrorists may exhibit. If the supervisor feels the SAR meets the criteria, it will then be sent to the MCD's SAR Unit, where it is further vetted and moved to the ISE-SAR Shared Spaces. Following initial vetting, the SAR Unit at the MCD makes a determination whether to forward the information to the regional fusion center and/or to the JTTF.

LAPD developed audit and management tools to evaluate the current SAR reporting process and continues to modify the program, as well as enhance training, based on emerging trends and lessons learned during the SAR process. The LAPD audit process includes both internal and external audits. An internal audit is conducted daily by the SAR Unit to ensure that all reported SARs are received and that all activity which indicates that a SAR should be reported does result in a SAR. The SAR process was added to the external audit schedule of the Inspector General's Office and the semiannual internal audit schedule of LAPD. LAPD Management Tools include reports to help identify emerging trends and to identify gaps.

The Seattle Police Department's Criminal Intelligence Bureau (CIB) initially receives information from officers within the Seattle Police Department in the form of information reports; field interview reports; and other reporting mechanisms. After review by the CIB, the reports are taken to the state fusion center, where they are further analyzed and distributed to the appropriate agency for follow-up investigation. This process has allowed the Seattle PD to merge its procedures for the handling of suspicious activity with those of the state fusion center, allowing for an efficient and streamlined effort.

The Virginia State Police has a Standard Operating Procedure in place concerning the SAR process within the agency. All employees of the Virginia State Police were provided with Information Bulletin 2009–35, explaining suspicious activity reporting procedures for the Virginia Fusion Center. The directive goes on to explain the types of information and types of activities that should be reported to the fusion center, as well as the appropriate forms for reporting the information.

The Southern Nevada Counter-Terrorism Center has developed outreach materials that assist the community with recognizing the signs of terrorism. Because of the unique jurisdictional challenges faced by the tourism and casino industry, Nevada has developed a specialized liaison program. This outreach program focuses on hotel staff, including valet attendants, private security, bell captains, and housekeeping. In this effort, the Las Vegas Police Department (LVPD) is providing software (Trapwire) to several hotel/casino sites in its city so that they can report suspicious activity. There are 14 sites currently involved. The casinos/hotels populate a node at their site with suspicious incidents that have been observed and reported, and they also enter proprietary data (which is not shared). The suspicious incidents are then shared with the other sites involved in the project and with LVPD.

USING SAR INFORMATION IN AGENCY DECISION MAKING

It is important that terrorism-related suspicious activity be shared with other law enforcement agencies in the ISE-SAR Shared Spaces. It is equally important that the gathering agency utilize the information when making decisions on resource deployment and asset allocations. Many law enforcement agencies have formalized processes for utilizing information developed from the SAR program in the agency's decision-making process.

The Boston Police Department and the Boston Regional Intelligence Center (BRIC) utilize the excellent relationships that have been built with the surrounding Urban Areas Security Initiative (UASI) regional partners and have a general agreement with the seven participating UASI cities—Quincy, Brookline, Cambridge, Revere, Everett, Summerville, and Chelsea—to jointly implement a regional SAR initiative. The key component of the information sharing initiative is daily conference calls with these agencies and components of the Boston Police Department in which information is shared and then utilized in the daily decision-making and resource allocation processes.

LAPD has a computerized statistics process whereby the agency's information analysis process feeds the agency's decision-making process. Information from the SAR program is analyzed and provided to LAPD commanders, who utilize that information to make decisions on officer deployments and assignments. The department has developed a crime-mapping program that includes information from the SAR initiative that allows the department's command staff to understand its crime environment and supports the decision-making process.

DEVELOPMENT OF THE TERRORISM INDICATORS DATABASE

In order for law enforcement agencies to collect the correct information concerning activities that may have a nexus to the planning of a terrorist attack, it is important that they understand the indicators from previous terrorist attacks that were part of the planning process. An analysis has to be conducted of previous terrorist attacks so that law enforcement can document those activities to provide a basis for gathering information concerning the indicators of future terrorist attacks.

BJA's State and Local Anti-Terrorism Training (SLATT) Program has long maintained information on both domestic and international terrorist events that affect the United States. As a part of this project, the database was enhanced to include information concerning the activities enumerated in the ISE SAR Functional Standard, Appendix B, relating to suspicious activities that can be shared in the ISE-SAR Shared Spaces. The information available in the

Terrorist and Criminal Extremist Events Database is available in four formats—chronological, by topic, search engine, and geospatial.

> The *Calendar of Terrorist and Criminal Extremist Events* is a chronology of antigovernment, terrorist, and criminal extremist activities that occurred either in the United States or involved a U.S. interest from January 1997 to recent time. These listings illustrate a broad spectrum of activities from large-scale acts of terrorism to local acts of harassment and intimidation. They also highlight violent political attacks carried out by terrorist and extremist groups, cite the more significant criminal violations perpetrated by extremists, and include activist-related court decisions.
>
> The *Terrorist and Criminal Extremist Incidents* lists are categorized by topic, searchable, and arranged in chronological order, starting with the most recent events. An explanation of the content included on each list is presented with the data.
>
> The *Suspicious Activity Search* allows searches to be conducted on multiple data fields, including dates, locations, precursor terrorist indicators, affected infrastructure type, and/or group affiliation.
>
> The *Geospatial Search* allows events to be mapped and reviewed by a variety of criteria, including date, location, precursor terrorist indicator, affected infrastructure type, and/or group affiliation in relation to distance from a specified location.

The SLATT project relied on the LAPD research of an extensive set of behavior-specific codes for the reporting of suspicious activity. These codes provided the method for documenting behavioral indicators that have a potential nexus to terrorism. LAPD used the codes to train its personnel in the recognition of suspicious activity. The process continued to mature as LAPD conducted research to develop patterns and determine the frequency of use with the codes. For this initiative, additional subject-matter experts from state and local agencies reviewed the LAPD codes as well as those identified in the Functional Standard. Throughout the project, these behavior codes were consistently mapped and validated to ensure that they are representative of the current terrorism threat environment.

Appendices

APPENDIX ONE: PROJECT PARTICIPANTS

PROJECT SPONSORS AND PARTNERS:

- U.S. Department of Justice (DOJ), Bureau of Justice Assistance (BJA), http://www.ojp.usdoj.gov/BJA
- Federal Bureau of Investigation (FBI), http://www.fbi.gov
- U.S. Department of Homeland Security (DHS), http://www.dhs.gov
- Program Manager, Information Sharing Environment (PM-ISE), http://www.ise.gov
- Major Cities Chiefs Association (MCCA), http://www.majorcitieschiefs.org
- DOJ's Global Justice Information Sharing Initiative (Global), Criminal Intelligence Coordinating Council (CICC), http://www.it.ojp.gov/global
- U.S. Department of Defense (DoD), http://www.defenselink.mil/policy/sections/policy_offices/hd/index.html
- International Association of Chiefs of Police (IACP), http://www.theiacp.org
- Major County Sheriffs' Association (MCSA), http://www.mcsheriffs.com

PROJECT PARTICIPANTS:

- Arizona Counter Terrorism Information Center (AcTIC)/Arizona Department of Public Safety
- Boston Regional Intelligence Center/Boston Police Department
- Chicago Police Department
- Florida Fusion Center/Florida Department of Law Enforcement
- Houston Regional Intelligence Service Center/Houston Police Department
- Los Angeles Police Department
- Miami-Dade Police Department
- New York State Intelligence Center (NYSIC)/New York State Police
- Washington State Fusion Center/Seattle Police Department
- Southern Nevada Counter-Terrorism Center/Las Vegas Metropolitan Police Department
- Virginia Fusion Center/Virginia State Police
- Washington Regional Threat and Analysis Center/Washington, DC, Metropolitan Police Department

Appendix Two: Project Timeline

ISE-SAR Evaluation Environment

Timeline

Illustrated below is a comprehensive timeline highlighting documents developed, meetings, site visits, training, technology, and other significant milestones throughout the ISE-SAR Evaluation Environment (ISE-SAR EE). Not captured below are the ad hoc planning efforts and countless conference calls that went into the development of a standardized SAR process and the ISE-SAR EE. A special thank-you is extended to all the partners at the state, local, and federal levels that helped make this project a success in such a short period of time.

ISE-SAR EE Publications	
Documents	**Date**
SAR for Local and State Entities IEPD v1.0	January 22, 2008
ISE-SAR Functional Standard, Version 1.0	January 25, 2008
ISE-SAR Functional Standard and Evaluation Environment: Initial Privacy and Civil Liberties Analysis, Version 1	September 2008
Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project (SAR Report)	October 24, 2008
SAR Process Implementation Checklist	November 2008
ISE-SAR Segment Architecture	December 2008
Nationwide SAR Initiative (NSI) CONOPS	December 23, 2008
ISE-SAR EE Implementation Guide, Version 1.0	January 9, 2009
ISE-SAR Functional Standard, Version 1.5	May 21, 2009
NSI Activity Summary	Monthly

Law Enforcement Associations' SAR Resolutions	
Associations	**Date**
Major Cities Chiefs Association (MCCA) SAR Resolution	June 10, 2008
Major County Sheriffs' Association SAR Resolution	June 29, 2008
International Association of Chiefs of Police SAR Resolution	November 11, 2008
National Sheriffs' Association SAR Resolution	January 31, 2009

ISE-SAR EE Related Meetings	
Event	**Date**
PM-ISE hosted a State and Local LE SAR Meeting—Washington, DC	February 11, 2008
SAR Executive Steering Committee Meeting—Baltimore, MD	May 6, 2008
SAR Pilot Expansion Project Meeting—Washington, DC	June 2, 2008
SAR Pilot Expansion Project Technology and Mapping Meeting—Washington, DC	June 2–3, 2008
MCCA Intelligence Commanders Meeting—Las Vegas, NV	July 8–9, 2008
SAR Working Group Meeting—Washington, DC	July 30, 2008
Dialogue on Privacy and Civil Liberties—Washington, DC	September 3, 2008
Criminal Intelligence Coordinating Council (CICC) Meeting: CICC unanimously approves the *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project* (SAR Report)—Bethesda, MD	September 9, 2008

ISE-SAR EE Related Meetings	
Event	**Date**
SAR Working Group Meeting—Washington, DC	September 11, 2008
SAR Pilot Project Meeting—St. Louis, MO	September 16–17, 2008
SAR Working Group Meeting—Washington, DC	October 21, 2008
DOJ's Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC) Meeting: GAC unanimously approves the SAR Report—National Harbor, MD	October 23, 2008
SAR Working Group Meeting—Washington, DC	December 2–3, 2008
SAR Working Group Meeting—Washington, DC	January 29, 2009
SAR Working Group Meeting—Washington, DC	March 25, 2009
SAR Team Meeting—Washington, DC	June 1, 2009
ISE-SAR EE User Group Meeting—Bethesda, MD	June 2, 2009
MCCA Intelligence Commanders Meeting—Baltimore, MD	August 18–19, 2009
ISE-SAR EE User Group Meeting—Washington, DC	September 16–17, 2009

ISE-SAR EE Site Visits/Assessments

Event	Date
Initial project site visit to Los Angeles Police Department by SAR Team	April 1, 2008
Initial project site visit to Chicago Police Department by SAR Team	April 3, 2008
Initial project site visit to Boston Police Department by SAR Team	April 9, 2008
Initial project site visit to Miami-Dade Police Department by SAR Team	April 24, 2008
Initial project site visit to New York State Police by SAR Technical Team	June 16, 2008
Initial project site visit to Florida Department of Law Enforcement by SAR Technical Team	June 19, 2008
Initial project site visit to Virginia State Police by SAR Technical Team	June 24, 2008
"As-Is" conference call with Washington, DC, Metropolitan Police Department	November 4, 2008
"As-Is" site visit to Los Angeles Police Department	December 4, 2008
"As-Is" site visit to Chicago Police Department	December 16, 2008
"As-Is" site visit to Boston Police Department	December 17, 2008
"As-Is" site visit to Las Vegas Metropolitan Police Department	January 13, 2009
"As-Is" site visit to Houston Police Department	January 15, 2009
"As-Is" conference call with Miami-Dade Police Department	February 18, 2009
"As-Is" site visit to Florida Department of Law Enforcement	February 19, 2009
"As-Is" site visit to Seattle Police Department	February 24, 2009
"As-Is" conference call with New York State Police	April 23, 2009
"As-Is" conference call with Virginia State Police	May 1, 2009
"As-Is" site visit to Arizona Department of Public Safety	July 23, 2009
ISE-SAR EE Final Assessment conference call with Arizona Department of Public Safety	September 28, 2009
ISE-SAR EE Final Assessment conference call with Miami-Dade Police Department	September 28, 2009

ISE-SAR EE Site Visits/Assessments	
Event	**Date**
ISE-SAR EE Final Assessment conference call with Florida Department of Law Enforcement	September 30, 2009
ISE-SAR EE Final Assessment conference call with Las Vegas Metropolitan Police Department	September 30, 2009
ISE-SAR EE Final Assessment conference call with Houston Police Department	October 8, 2009
ISE-SAR EE Final Assessment conference call with Washington, DC, Metropolitan Police Department	October 8, 2009
ISE-SAR EE Final Assessment conference call with Virginia State Police	October 9, 2009
ISE-SAR EE Final Assessment conference call with New York State Police	October 13, 2009
ISE-SAR EE Final Assessment conference call with Seattle Police Department/Washington State Fusion Center	October 13, 2009
ISE-SAR EE Final Assessment conference call with Chicago Police Department	October 14, 2009
ISE-SAR EE Final Assessment conference call with Los Angeles Police Department	October 16, 2009
ISE-SAR EE Final Assessment conference call with Boston Police Department	November 12, 2009

ISE-SAR EE Training	
Agency and Event	**Date**
Arizona Department of Public Safety	
Chief Executive Officer Briefing	June 4, 2009
SAR Analyst/Investigator Training delivered to Arizona Department of Public Safety	July 23, 2009
Line Officer Training	TBD

ISE-SAR EE Training	
Agency and Event	**Date**
Boston Police Department	
SAR Analyst/Investigator Training	February 3–4, 2009
Chief Executive Officer Briefing	February 12, 2009
Line Officer Training	TBD
Chicago Police Department	
SAR Analyst/Investigator Training	March 3, 2009
Chief Executive Officer Briefing	March 19, 2009
Line Officer Training	TBD
U.S. Department of Homeland Security	
SAR Analyst/Investigator Training delivered to Federal Air Marshals Service	June 16, 2009
Florida Department of Law Enforcement (FDLE)	
SAR Analyst/Investigator Training to FDLE—Miami	January 26, 2009
SAR Analyst/Investigator Training delivered to FDLE—Tallahassee (funded by FDLE)	June 5, 2009
SAR Analyst/Investigator Training delivered to FDLE—Tampa (funded by FDLE)	June 23, 2009
SAR Analyst/Investigator Training delivered to FDLE—Orlando (funded by FDLE)	June 25, 2009
Line Officer Training delivered to FDLE—Tallahassee (final pilot)	August 6, 2009
Chief Executive Officer Briefing	September 15, 2009
Houston Police Department	
SAR Analyst/Investigator Training	March 5, 2009
Chief Executive Officer Briefing	April 23, 2009
Line Officer Training	TBD
Las Vegas Metropolitan Police Department	
Chief Executive Officer Briefing	March 12, 2009
SAR Analyst/Investigator Training	April 7, 2009
Line Officer Training	TBD

ISE-SAR EE Training	
Agency and Event	**Date**
Los Angeles Police Department	
Chief Executive Officer Briefing	February 26, 2009
SAR Analyst/Investigator Training	July 21, 2009
Line Officer Training	TBD
Miami-Dade Police Department	
SAR Analyst/Investigator Training	January 26, 2009
Chief Executive Officer Briefing	February 19, 2009
Line Officer Training	TBD
New York State Police	
SAR Analyst/Investigator Training	March 18, 2009
Line Officer Training (pilot)	May 2009
Line Officer Training (pilot)	June 2009
Chief Executive Officer Briefing	September 24, 2009
Seattle Police Department	
SAR Analyst/Investigator Training	May 14, 2009
Chief Executive Officer Briefing	May 28, 2009
Line Officer Training	TBD
Virginia State Police	
SAR Analyst/Investigator Training	April 2, 2009
Line Officer Training (pilot)	June 9, 2009
Chief Executive Officer Briefing	October 29, 2009
Washington, DC, Metropolitan Police Department	
Line Officer Training	December 2008
SAR Analyst/Investigator Training	December 12, 2008
Chief Executive Officer Briefing	December 18, 2008

ISE-SAR EE Privacy Policy	
Privacy Policies determined to be consistent with the applicable requirements of the ISE Privacy Guidelines	Date
Miami-Dade Police Department	May 6, 2009
Florida Department of Law Enforcement	May 6, 2009
Virginia State Police	May 6, 2009
Boston Police Department	May 12, 2009
New York State Police	May 12, 2009
Chicago Police Department	July 13, 2009
Houston Police Department	August 13, 2009
Los Angeles Police Department	September 1, 2009
Washington State Fusion Center	October 27, 2009

ISE-SAR EE Technology Milestones	
Event	Date
ISE-SAR EE Shared Space Install Completed at New York State Police	August 27, 3008
ISE-SAR EE Shared Space Install Completed at Florida Department of Law Enforcement	September 19, 2008
ISE-SAR EE Shared Space Install Completed at the Virginia State Police	September 24, 2008
ISE-SAR EE Shared Space Install Completed at Washington, DC, Metropolitan Police Department	December 17, 2008
ISE-SAR EE Shared Space and SVT Install Completed at Miami-Dade Police Department	February 23, 2009
ISE-SAR EE Shared Space and SVT Install Completed at Chicago Police Department	March 13, 2009
ISE-SAR EE Shared Space and SVT Install Completed at Boston Police Department	March 29, 2009
ISE-SAR EE Shared Space and SVT Install Completed at Houston Police Department	April 24, 2009

ISE-SAR EE Technology Milestones

Event	Date
ISE-SAR EE Shared Space and SVT Install Completed at Las Vegas Metropolitan Police Department	May 19, 2009
Chicago Police Department went "live" and was able to utilize the ISE-SAR EE Shared Spaces	July 22, 2009
ISE-SAR EE Shared Space Install Completed at U.S. Department of Homeland Security	July 30, 2009
Completed ISE-SAR EE eGuardian Interface	August 15, 2009
ISE-SAR EE Shared Space and SVT Install Completed at Los Angeles Police Department	September 24, 2009
ISE-SAR EE Shared Space Install Completed at eGuardian	October 16, 2009
Houston Police Department went "live" and was able to utilize the ISE-SAR EE Shared Spaces	November 30, 2009 (estimated)
Los Angeles Police Department went "live" and was able to utilize the ISE-SAR EE Shared Spaces	November 30, 2009 (estimated)
ISE-SAR EE Shared Space and SVT Install Completed at Seattle Police Department	December 3, 2009 (estimated)
ISE-SAR EE Shared Space Install Completed at Arizona Department of Public Safety	December 19, 2009 (estimated)

APPENDIX THREE: ACRONYMS AND ABBREVIATIONS

BJA	Bureau of Justice Assistance
CFR	Code of Federal Regulations
CICC	Criminal Intelligence Coordinating Council
CTISS	Common Terrorism Information Sharing Standards
CUI	Controlled Unclassified Information
DHS	U.S. Department of Homeland Security
DoD	U.S. Department of Defense
DNI-U	Director of National Intelligence–Unclassified
DOJ	U.S. Department of Justice
EAF	Enterprise Architecture Framework
EE	Evaluation Environment
FBI	Federal Bureau of Investigation
FI	Field Interview
FIG	Field Intelligence Group
Global	Global Justice Information Sharing Initiative
HSIN	Homeland Security Information Network
IACP	International Association of Chiefs of Police
IEPD	Information Exchange Package Document
ISE	Information Sharing Environment
JTTF	Joint Terrorism Task Force
LEISP	Law Enforcement Information Sharing Program
LEO	Law Enforcement Online
LEXS-PD	Logical Entity eXchange Specifications–Publication and Discovery
LEXS-SR	Logical Entity eXchange Specifications–Search and Retrieval
MCCA	Major Cities Chiefs Association
MCSA	Major County Sheriffs' Association
MO	Modus Operandi
NCIRC	National Criminal Intelligence Resource Center
N-DEx	National Data Exchange Program
NIEM	National Information Exchange Model

NSIS	*National Strategy for Information Sharing*
ODNI	Office of the Director of National Intelligence
PIA	Privacy Impact Assessment
PIN	Priority Information Need
PGC	[ISE] Privacy Guidelines Committee
PM-ISE	Program Manager, Information Sharing Environment
RISSNET	Regional Information Sharing Systems Secure Intranet
RMS	Records Management System
SAR	Suspicious Activity Reporting
TSC	[FBI] Terrorist Screening Center
VPN	Virtual Private Network
XML	Extensible Markup Language

APPENDIX FOUR: PARTICIPATING AGENCY ASSESSMENTS

ARIZONA COUNTER TERRORISM INFORMATION CENTER

SAR PROCESS REPORT—POST-IMPLEMENTATION PHASE

Following the conclusion of the Information Sharing Environment-Suspicious Activity Reporting Evaluation Environment (ISE-SAR EE), a discussion was held with the Arizona Department of Public Safety's (ADPS) Arizona Counter Terrorism Information Center (AcTIC) to document the implementation efforts conducted during the ISE-SAR EE. The results of the discussion are detailed below.

EXECUTIVE LEADERSHIP

ADPS has the lead role for the operation of AcTIC. Colocated with AcTIC are components of the U.S. Department of Homeland Security (DHS), the Joint Terrorism Task Force (JTTF), and various police departments, sheriffs' departments, and other emergency response agencies around the state. It was noted that prior to the ISE-SAR EE, AcTIC had no standard operating procedure (SOP)/General Order regarding the SAR process.

During the ISE-SAR EE, command staff and senior management were briefed on the ISE-SAR EE. ADPS command staff attended the Major Cities Chiefs Association's Chief Executive Officer Briefing in June 2009, in which nine personnel from seven agencies participated. The commander of AcTIC has been assigned to the SAR process development project; the primary responsibility of the commander is to implement a formal SAR process within AcTIC. The day-to-day implementation has been tasked to a lieutenant within AcTIC. During the ISE-SAR EE, a SAR SOP had not been developed; however, command staff indicated that there is a plan to develop a SAR SOP.

SAR BUSINESS PROCESS

Prior to the ISE-SAR EE, AcTIC had developed a SAR process and collaborated with other law enforcement agencies to develop policies and procedures concerning the reporting of suspicious activity. SARs are received by the center via phone calls directly to the center, e-mails, and electronic postings, using the NC4 TIP system software operated by AcTIC. The center operates a 24-hour watch center, which is the initial entry point for SAR information into the center. However, some SAR information is received from local agency case management systems, such as the Phoenix, Arizona, Police Department. All SAR information is eventually entered into the NC4 TIP system.

The state of Arizona has developed an extensive cadre of Terrorism Liaison Officers (TLOs) throughout the state who are both law enforcement agents and other emergency response agents. These individuals serve as the primary contacts with local agencies to develop and report SAR information. The TLOs may enter the information directly into the NC4 TIP system or call the center. The TLO program is central to the center's ability to quickly receive suspicious activity information that is reported to law enforcement and other emergency response agencies throughout the state. These officers have been specially trained and serve as liaisons to the respective agencies as well as to the public. Prior to the ISE-SAR EE, AcTIC had a highly developed analytic section to conduct analysis of information received at the center. This section is very successful because of the center's large joint operation, and information can quickly be analyzed and assigned for investigation and follow-up.

Prior to the ISE-SAR EE, AcTIC had submitted a privacy policy during the DHS/U.S. Department of Justice (DOJ)-sponsored Fusion Center Privacy Policy Development Technical Assistance.[34] AcTIC was a late addition to the ISE-SAR EE, and it is currently reviewing and modifying, as necessary, its current privacy policy to ensure that it includes the SAR process and meets the applicable requirements of the ISE Privacy Guidelines.

During the ISE-SAR EE, AcTIC was in the process of developing a standard operating procedure (SOP) on SARs. In addition, it is also in the beginning stages of adopting the behavior-specific codes identified in the ISE-SAR Functional Standard. During the ISE-SAR EE, the NC4 TIP system was modified to include SAR information fields for transition without reentering information. SAR data is retrievable in the system and covers the response to and referrals and final disposition of SARs. AcTIC has developed a multilayer review process for the vetting of SARs and moving them to the ISE-SAR Shared Spaces. An AcTIC TIP must have two field values completed to trigger submission into the ISE-SAR Shared Spaces:

(1) Under the "Basic Info" tab within the Information Sharing and Analysis Center (ISAC) area, the "Status" color code must be one of the following: green, yellow, orange, or red. This field is completed by the TIP initiator and/or responsible supervisor.

(2) Under the "Classified/Threat Assessment" tab and within the subreport labeled "Target of Suspicious Activity" in the ISAC area, the drop-down tab "PIIR/SIIR" must have a "SAR" field selection. This field is to be completed only by the AcTIC SAR Gatekeeper.

Once both field values are completed, the selected TIP data fields are automatically pushed to the Arizona ISE-SAR Shared Spaces and the TIP database is synchronized daily at midnight. Any updates to the TIP database are copied and pasted at this time. After an NC4

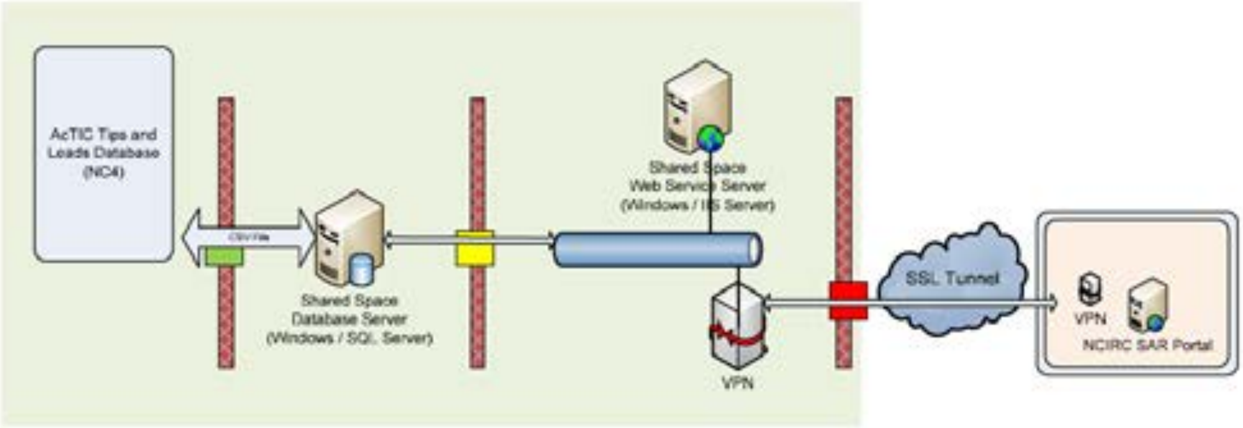
[34] The Fusion Center Privacy Policy Development Technical Assistance course is offered through the DHS/DOJ Fusion Process Technical Assistance Program and Services.

TIP entry is made, it is electronically sent to an investigative supervisor who reviews the information for investigative content and assigns it to an investigator/analyst. The Watch Center Supervisor reviews all NC4 TIP entries daily for completeness and potential terrorism nexus. Daily, the gatekeeper reviews all NC4 TIP entries for the standardized behavior-specific points, and if they are present, the NC4 TIP is coded as a SAR and pushed to the ISE-SAR Shared Spaces.

Currently, access to the ISE-SAR Shared Spaces is restricted to the Watch Center supervisory staff and the Situational Awareness Unit. Participants with access to the ISE-SAR Shared Spaces must sign a nondisclosure agreement. All queries on the information within the ISE-SAR Shared Spaces must be completed for law enforcement purposes only and must have a criminal nexus. At this time, there is no formal process for notifying the source agency if there in an error in content; however, this issue will be addressed in the SOP.

SAR Technical Process

Prior to the ISE-SAR EE and for several years, AcTIC and other partner agencies have collected and managed SARs using the Tips and Leads application offered by NC4 Corporation. During the ISE-SAE EE, AcTIC decided on a novel approach of using an existing report generation capability on the NC4 system to generate a comma-separated values (CSV) file containing all of the SAR fields that AcTIC has decided to submit to its shared space. The CSV file is processed by an extract, transform, and load routine and loads all the SARs into the AcTIC Shared Spaces database.


AcTIC Tips and Leads Database (NC4)
CSV File
Shared Space Database Server (Windows / SQL Server)
Shared Space Web Service Server (Windows / IIS Server)
VPN
SSL Tunnel
VPN
NCIRC SAR Portal

Training

Prior to the ISE-SAR EE, AcTIC had developed numerous training programs for state of Arizona and fusion center personnel to train them on the SAR process as well as terrorism-related information. In addition, AcTIC developed a high-level training program for its TLOs within the state. This training has developed into a model for other states and fusion centers for the training of its TLOs.

During the ISE-SAR EE, ADPS participated in the Chief Executive Officer Briefing and the SAR analyst/investigator course. During the SAR analyst/investigator course in the Phoenix area in July 2009, 28 personnel were trained from 10 law enforcement agencies. ADPS plans to utilize the line officer training once it is made available nationwide.

Institutionalization of the SAR Process

Prior to and during the ISE-SAR EE, AcTIC had a process to handle SARs. This process has been institutionalized with the local, state, and federal agencies because of the colocation of critical components of each of those agencies in the center. The center has implemented a software solution to ensure that all SAR information leads are followed through with appropriate investigative activity.

AcTIC analyzes all SARs and utilizes the all-crimes approach to identify emerging trends and behavior patterns. The SAR process is modified to meet the needs as new information is received and new patterns and priority information needs are identified. Special reports, alerts, warnings, and notifications based on the analysis of SARs, crime, and arrest activity are developed and shared externally with regional partners, local law enforcement, and security personnel at critical infrastructure/key resource locations.

Outreach to the Public

Prior to and during the ISE-SAR EE, the center had developed a DVD for distribution to the public and first responders titled *8 Signs of Terrorism*, which educates the public about what to look for and report regarding terrorism-related suspicious activity. The center also maintains a public Web site (http://cid.dps.state.az.us) that provides information for the public and explains the operation of the state fusion center. In addition, ADPS has a highly developed TLO program that provides outreach to the public and first responder agencies in the state.

Partnering With Other Agencies and Connecting to Information Sharing

AcTIC has healthy partnerships with the various state and local government agencies and public safety offices and agencies in the region. Components of DHS, the Federal Bureau of Investigation's (FBI) JTTF, the Phoenix Police Department, the Maricopa County Sheriff's Office, the Phoenix Fire Department, and other emergency response agencies are colocated at the center. The TLO program is utilized extensively by AcTIC for outreach to the private sector as well as other government agencies. AcTIC has a strong relationship with DHS and the JTTF through colocation at the center.

AcTIC has access to the Regional Information Sharing Systems Secure Intranet (RISSNET), the Homeland Security Information Network, and the FBI's Law Enforcement Online, which allows the sending and receiving of secure e-mail via these secure networks. AcTIC also has access to the state's criminal justice network, participates in a number of regional information sharing initiatives, and operates a public Web site. AcTIC technical staff members are working with the SAR project team to develop the ability to export the records management system data in the National Information Exchange Model format.

Partnering to Develop Geographic Risk Assessments

AcTIC works with federal partners in Arizona as well as its federal headquarters counterparts to develop the information needed to create geographic risk assessments. The primary responsibility for these assessments rests with AcTIC. The center also works with federal agencies to develop information needs based on risk assessments as well as other reviews and analyses of SARs.

Project Recommendations From the Arizona Counter Terrorism Information Center

- There is no need for a national program office.
- If nationwide standards are to be established and maintained, it is recommended that a national training program for this project be created.
- A national users group should be established for this project that will assist with vetting changes, identifying lessons learned and success stories, networking, and identifying challenges.
- There is a need for ongoing technical support for the Nationwide SAR Initiative.
- A national legal office for this initiative should be established to protect the data being collected and to address concerns raised by the American Civil Liberties Union and other privacy advocates.
- Agencies should receive training, technical support, and funding for the servers during this initiative.

BOSTON, MASSACHUSETTS, POLICE DEPARTMENT

SAR PROCESS REPORT—POST-IMPLEMENTATION PHASE

Following the conclusion of the Information Sharing Environment-Suspicious Activity Reporting Evaluation Environment (ISE-SAR EE), a discussion was held with the Boston, Massachusetts, Police Department's (BPD) Boston Regional Intelligence Center (BRIC) to document the implementation efforts conducted during the ISE-SAR EE. The results of the discussion are detailed below.

EXECUTIVE LEADERSHIP

Currently, BPD has no General/Special Order relating to SAR; however, the agency superintendent fully supports the SAR process, and the department is in the development stage of issuing a SAR General/Special Order. The order will be released in conjunction with the department-wide online SAR training. The BPD command staff received the Major Cities Chiefs Association's Chief Executive Officer Briefing in February 2009, in which 46 command staff personnel from 8 law enforcement agencies participated. During the ISE-SAR EE, a deputy superintendent within BRIC was assigned primary responsibility for implementation of the SAR process throughout BRIC and BPD.

SAR BUSINESS PROCESS

Prior to the ISE-SAR EE, BPD had a check box on its incident reports that allowed officers to identify a potential SAR. Once this box is checked, the information is flagged for BRIC to review. Each district in the department files its SARs with BRIC, and BRIC assigns a detective to serve as the formal reviewer of all SARs submitted to the center. As part of the business process, the detective reviews all SARs that have a potential terrorism-related nexus within the first 24 hours. If a SAR is deemed to be terrorism-related, the detective forwards the SAR to the Joint Terrorism Task Force (JTTF). After the SAR is analyzed by BRIC personnel, action is taken to either respond to the SAR, refer it to the investigative unit or JTTF, or take no further action and close the report. Feedback on the SAR's disposition is provided to the submitting officer.

BRIC can access all of BPD's automated systems through a data warehouse and can retrieve SAR data from any of the systems. BRIC utilizes an automated search capability for information in the records management system (RMS), computer-aided dispatch, intelligence systems, and field interview card process to identify reports that have certain terrorism-related behaviors requiring additional analysis. In addition, discussion has occurred between BRIC and the Massachusetts Commonwealth Fusion Center[35] about standardizing the SAR process between the two agencies. Additional jurisdictions participating in the Urban Areas Security Initiative (UASI) have agreed to send their SARs to BRIC; BRIC and BPD will then serve as the regional "vetting authority" and send all appropriate SARs to the ISE-SAR Shared Spaces.

During the ISE-SAR EE, BPD did not adopt the behavior-specific codes detailed in the ISE-SAR Functional Standard but reviewed its own codes and can classify its activities based on the Functional Standard. BRIC developed and implemented a privacy policy regarding the reporting of suspicious activity that meets the applicable requirements of the ISE Privacy Guidelines. During the ISE-SAR EE, BRIC developed a multilayer review for the vetting of SAR information. Once a potential SAR is identified and the box is checked, the report is electronically sent to a data warehouse, where an analyst in BRIC vets the information and adds any value to the report. If the analyst deems the report to contain terrorism-related information, it is reviewed by a supervisor for final approval. If the supervisor designates the information as an ISE-SAR, it is manually entered into the ISE-SAR Shared Spaces via the SAR Vetting Tool (SVT). In order to protect the information within the ISE-SAR Shared Spaces, it was determined that access to the ISE-SAR Shared Spaces would be limited to personnel within BRIC that have attended the analyst/investigator and privacy training. It is BRIC policy that all queries on the information within the ISE-SAR Shared Spaces be for law enforcement purposes only and must have a criminal nexus.

SAR Technical Process

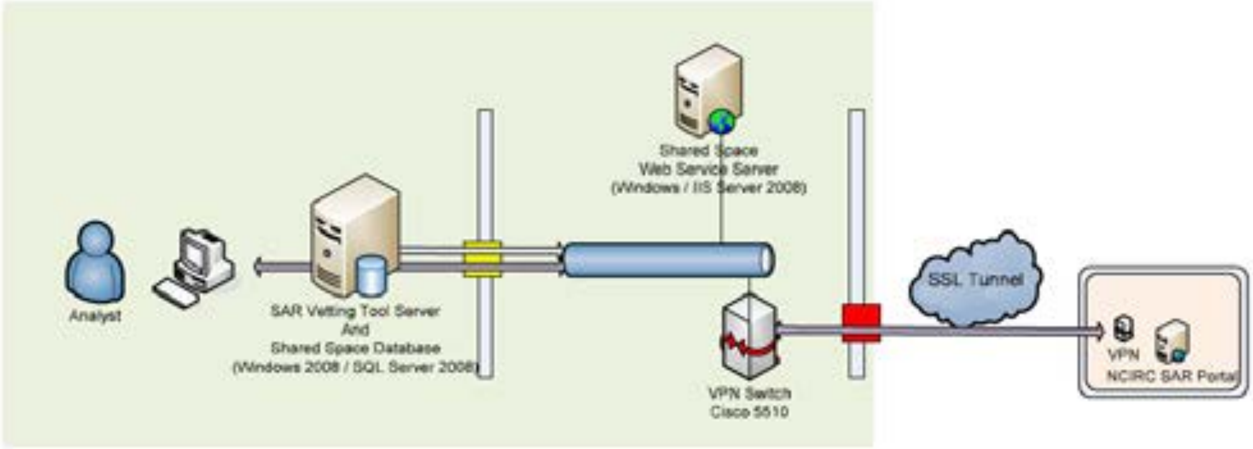
Prior to the ISE-SAR EE, BRIC's technical process included an in-house-designed data warehouse solution with an interface to the Environmental Systems Research Institute, Inc. (ESRI), geographic information system software application. Each night, all incident data, including potential SARs, is loaded into the warehouse solution. BRIC analysts can then search the warehouse for new incident records that may support ongoing investigations, including general crimes, gang violence, and terrorist activities. Using the ESRI tools, analysts can also track crime patterns and trends on map background for use in daily briefings and investigative reports.

Once BRIC analysts determine that incident data (terrorism or criminal indicators) is important to an intelligence case, data from the data warehouse solution and/or RMS is exported to an intelligence case management system. This type of system is also used by the Massachusetts Commonwealth Fusion Center. Plans are under way to connect the two systems to provide effective data exchange between the two centers.

During the ISE-SAR EE, BRIC requested the use of the SVT to augment existing legacy system data and act as a bridge between the legacy system and the Shared Spaces database. The

[35] The state-designated fusion center, as determined by the Federal Bureau of Investigation (FBI) and the U.S. Department of Homeland Security (DHS).

SVT application and database were installed on the ISE-SAR Shared Spaces Server as an economical approach to share hardware and MS-SQL resources. The common architecture is described below.



Training

Prior to the ISE-SAR EE, the department had not developed nor implemented agency-wide training on the SAR process. BPD was developing SAR training independent of the ISE-SAR EE. This training will focus on homeland security and violent street crime and will be applicable to personnel outside of the department, including university police, public school police, parking enforcement, and code inspectors. BPD was using portions of the State and Local Anti-Terrorism Training (SLATT) Program instruction material in its in-service training and preservice curriculum in the academy.

During the ISE-SAR EE, BPD and BRIC participated in the Chief Executive Officer Briefing and the analyst/investigator course. During the SAR analyst/investigator course in the Boston area in February 2009, 24 personnel were trained from 10 law enforcement agencies. BPD plans to utilize the line officer training once it is made available nationwide. In addition, BPD continued its efforts to develop online SAR line officer training. It is anticipated that the training will be finalized in November 2009 and made available to line officers in December 2009.

Institutionalization of the SAR Process

Prior to and during the ISE-SAR EE, several efforts were under way in BRIC to institutionalize the SAR process. While there is no formal liaison officer program within BRIC, officers in each of the BPD districts and surrounding agencies work closely with BRIC. The commander for BRIC conducts audits of the intelligence and SAR files, and the SAR reports are reviewed and analyzed on a regular basis. BRIC regularly compares its information needs against the current jurisdictional trends and modifies its SAR process as needed. SAR review is also a part of BRIC's alert and notification process, with alerts and notifications sent out to distribution lists maintained by BRIC. These distribution lists include BPD's district offices and participating UASI agencies, and BRIC conducts daily conference calls with those entities to ensure that all information is shared on a timely basis.

Outreach to the Public

Prior to and during the ISE-SAR EE, BPD conducted citizen academies in order to inform the public on terrorism behaviors and how to report suspicious activity. In addition, there are monthly forums that are held with the Middle Eastern community groups within the city. BPD is partnering with the state, local, and federal agencies for the Building Communities of Trust program. Currently, the department conducts approximately 5,000 community outreach programs a year for all crime types, including terrorism.

Partnering With Other Agencies and Connecting to Information Sharing

Prior to and during the ISE-SAR EE, BRIC and BPD had various information sharing initiatives in place. External stakeholders in the Boston area are informed of and support BRIC's operations. BRIC has excellent relationships with the surrounding UASI regional partners and has a general agreement with the seven participating UASI cities—Quincy, Brookline, Cambridge, Revere, Everett, Summerville, and Chelsea—to jointly implement a regional SAR initiative. It was also indicated that several cities outside of the UASI region may elect to join the BPD SAR initiative.

BRIC can access the Regional Information Sharing Systems Secure Intranet (RISSNET), the FBI's Law Enforcement Online (LEO), and the Homeland Security Information Network and is able to send and receive secure e-mails through RISSNET and LEO. BRIC can also access the state's criminal justice network. Although BRIC works closely with the Massachusetts Commonwealth Fusion Center (a state fusion center representative is staffed in BRIC), the two are not directly connected; therefore, information sharing is not automated.

In addition, formal training develops partnerships among public safety, the private sector, and BRIC. After the formal training is completed, BRIC will meet with public safety and private sector personnel on an ad hoc basis depending on the emerging trends throughout the city. BRIC has access to independent e-mail alert systems within the financial and hotel industries and hospitals throughout the city. Alerts can immediately be sent out over these systems, and the information is quickly disseminated by personnel within the industries.

Partnering to Develop Geographic Risk Assessments

Prior to and during the ISE-SAR EE, BRIC worked with DHS and the FBI to develop risk assessments and information needs, and all terrorism-related SAR activity is reported to the JTTF. Many local-area agencies, as well as state and federal agencies, are represented, in some capacity, in BRIC and participate in the development of these assessments.

Project Recommendations From the Boston Police Department

- There is a need for some form of governing body, such as a national program office, to monitor the Nationwide SAR Initiative (NSI) and take the lead in the coordination efforts between agencies at all levels of government.
- There should be a national training program to assist agencies in the development and/or delivery of SAR-related training.
- If it can be made affordable, there is tremendous value in the creation of a national users group for the NSI. A national users group would bring agencies together so they can form relationships and discuss issues, best practices, and lessons learned regarding the NSI.
- There is a need for ongoing technical support in order for the technology to evolve with the project.
- A national legal office should not be created. Multiple legal resources already exist for law enforcement agencies at all levels of the government.
- A "daily digest" should be created for the ISE-SAR Shared Spaces. This capability would allow agencies to monitor the SARs that are being submitted to the ISE-SAR Shared Spaces on a daily basis and could save the time and effort it takes to conduct multiple searches.
- An appropriate threshold should be clearly defined for entering a SAR into the ISE-SAR Shared Spaces. During the ISE-SAR EE, there seemed to be a disparate amount of SARs being entered between the agencies. BPD wants to avoid the entry of information into the ISE-SAR Shared Spaces that is not of value and avoid large volumes of information being "dumped" into the system.

Chicago, Illinois, Police Department

SAR Process Report—Post-Implementation Phase

Following the conclusion of the Information Sharing Environment-Suspicious Activity Reporting Evaluation Environment (ISE-SAR EE), a discussion was held with the Chicago, Illinois, Police Department (CPD) to document the implementation efforts conducted during the ISE-SAR EE. The results of the discussion are detailed below.

Executive Leadership

Prior to the ISE-SAR EE, CPD did not have a policy regarding the collection and analysis of suspicious activity information. The command staff in CPD's Deployment Operations Center had been briefed on the initiative and had attended conferences and training events in which the SAR process implementation was discussed. CPD command staff and senior management had shown their full support for this effort.

During the ISE-SAR EE, CPD command staff received the Major Cities Chiefs Association's Chief Executive Officer Briefing in May 2009, and 36 command staff personnel from approximately 31 law enforcement agencies participated. Currently, there is no separate policy for the collection and analysis of SAR information; however, there is a comprehensive policy on the handling of information reports. As the project matures, the chief of the Counterterrorism and Intelligence Division (CID) will be responsible for drafting a SAR policy. A commander from CID has been assigned to the SAR process development project; the primary responsibility of the commander is to implement a formal SAR process at CPD.

SAR Business Process

Prior to the ISE-SAR EE, CPD utilized an "information report" to collect data regarding suspicious activity. CPD forwarded all of the information reports containing terrorism-related issues to CID. Based on its analysis and investigation, CID made a determination as to the disposition of these reports. The disposition included either referral for full investigation or referral to another agency for its review. A database was designated to document and track the reported terrorism-related suspicious activity information. CID is responsible for providing feedback to the officers who submit the suspicious activity.

Prior to the ISE-SAR EE, CPD had not adopted the behavior-specific codes listed in the ISE-SAR Functional Standard. All terrorism-related information reports were vetted within 24 hours and a report provided to the on-duty lieutenant in CID. After the lieutenant's review, relevant terrorism-related information reports were forwarded to the Illinois Statewide Terrorism and Intelligence Center, the U.S. Department of Homeland Security's (DHS) National Operations Center (NOC), and the Federal Bureau of Investigation's (FBI) Joint

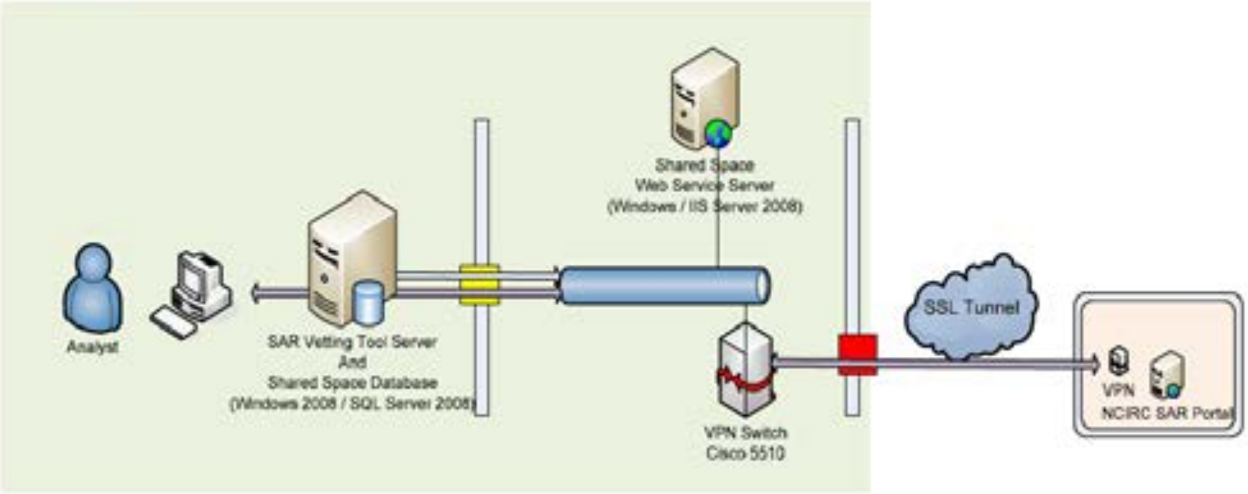
Terrorism Task Force (JTTF) for further vetting. Prior to the ISE-SAR EE, the department was using the eGuardian system to submit terrorism-related SARs to the JTTF.

During the ISE-SAR EE, CPD continued to use the same SAR mechanisms that were used prior to the ISE-SAR EE. However, CPD created a multilayer review process for reviewing and vetting SARs and moving them to the ISE-SAR Shared Spaces. The department requested use of the SAR Vetting Tool (SVT) to input its SAR data for ultimate migration to the ISE-SAR Shared Spaces. CID adopted the behavior-specific codes illustrated in the ISE-SAR Functional Standard and developed and implemented a privacy policy regarding the reporting of suspicious activity that meets the applicable requirements of the ISE Privacy Guidelines. In order to protect the information within the ISE-SAR Shared Spaces, it was determined that access to the ISE-SAR Shared Spaces would be limited to personnel within CID, and by policy, all queries on the information within the ISE-SAR Shared Spaces is for law enforcement purposes only and must have a criminal nexus. It was indicated that if SAR information is identified as having an error, CID will immediately contact the source agency and rectify the error.

SAR Technical Process

Prior to the ISE-SAR EE, the center of CPD's information technology infrastructure was the Citizen Law Enforcement Analysis and Reporting (CLEAR) system. Initially deployed in April 2000, the CLEAR system is the foundation for a growing set of integrated CLEAR applications used by CPD officers and civilians in and around the Chicago area. Handling thousands of queries daily, the CLEAR system supports all law enforcement and investigative functions within CPD.

During the ISE-SAR EE, CPD requested the use of the SVT to augment existing legacy system data and act as a bridge between the legacy system and the Shared Spaces database. The SVT application and database was installed on the ISE-SAR Shared Spaces Server as an economical approach to share hardware and MS-SQL resources. The common architecture is described below.



TRAINING

Prior to the ISE-SAR EE, CPD had developed a five-day terrorism training program and was in the process of training all of its officers. CID continuously monitors all incoming terrorism-related information in order to identify new trends and emerging issues. The results of this analysis are provided to the training bureau.

During the ISE-SAR EE, CPD continued its efforts to train all officers in its five-day terrorism awareness program, and SAR-related training has been provided to all Terrorism Liaison Officers (TLOs) within the department. It was indicated that CID continually monitors all incoming SARs and evaluates those for new trends and emerging issues. The results of the analysis are provided to the Training Bureau. In addition, CPD participated in the Chief Executive Officer Briefing and the SAR analyst/investigator course. During the SAR analyst/investigator course in the Chicago area in March 2009, 21 personnel were trained from three law enforcement agencies. CID plans to utilize the line officer training once it is made available nationwide.

INSTITUTIONALIZATION OF THE SAR PROCESS

Prior to and during the ISE-SAR EE and continued throughout the ISE-SAR EE, CPD maintained a robust TLO program within the department. Officers are selected from 25 districts, one per watch, and include approximately 80 members. TLOs meet quarterly and have organized training programs with guest speakers. CPD disseminates suspicious activity alerts, warnings, and notifications via intelligence bulletins to all law enforcement officers, as well as selected managers of critical infrastructure and other government agencies. The audience for these reports includes the command staff, the Deployment Operations Center's Web site, roll call distribution in each district office, the Law Enforcement Online (LEO) Special Interest Group, Homeland Security State and Local Intelligence Community of Interest, and the Regional Information Sharing Systems Secure Intranet (RISSNET).

OUTREACH TO THE PUBLIC

Prior to and during the ISE-SAR EE, CPD had an aggressive outreach program to the community. The Chicago Alternative Policing Strategy is used to educate the public and business community regarding activities of CPD. A weekly bulletin is distributed to the business community, and posters are provided in public areas such as mass transit utilizing the "See something—Say something" concept. Additionally, officers are assigned to the downtown business district to implement the department's homeland security strategy.

PARTNERING WITH OTHER AGENCIES AND CONNECTING TO INFORMATION SHARING

Prior to and during the ISE-SAR EE, CPD had developed partnerships with other public safety agencies and utilizes the TLO program to maintain and enhance relationships with its partners. Additionally, the mayor of Chicago and city council committees are briefed on a regular basis concerning homeland security activities.

As noted during the site visits, CPD is a member of RISSNET, LEO, and the Homeland Security Information Network and can send and receive secure e-mails via RISSNET and LEO. CPD can access the Illinois criminal justice network and operates several city and regional information systems that are accessible by CID. CPD had a working relationship with the state fusion center; however, there is no direct electronic connectivity.

Partnering to Develop Geographic Risk Assessments

Prior to and during the ISE-SAR EE, CPD indicated that it had developed threat assessments and special assessments using data from the FBI, DHS, and CPD information reports. Although it does not have a formal information needs process, CPD works closely with the FBI, DHS, and U.S. Immigration and Customs Enforcement to gain relevant information and to provide that information to relevant partners. To determine and coordinate information needs, CPD staff members noted that they regularly work with the JTTF as well as the NOC and incorporate these information needs as appropriate. They also explained that the Human Intelligence Squad is responsible for developing information needs and managing human assets. These efforts provide additional feedback to CPD for further evaluation and analysis.

Project Recommendations From the Chicago Police Department

- There needs to be some federal-level coordination; however, the initiative is primarily a local-agency issue.
- Training on SAR should be handled at the local level.
- A national users group would be beneficial to help local agencies coordinate their activities.
- There is a need for ongoing technical support for the current technology that has been deployed for the ISE-SAR Shared Spaces.
- There is no need for a national legal office; legal issues for the Nationwide SAR Initiative are mostly a local concern.

Florida Department of Law Enforcement

SAR Process Report—Post-Implementation Phase

Following the conclusion of the Information Sharing Environment-Suspicious Activity Reporting Evaluation Environment (ISE-SAR EE), a discussion was held with the Florida Department of Law Enforcement's (FDLE) state-designated Florida Fusion Center (FFC) to document the implementation efforts conducted during the ISE-SAR EE. The results of the discussion are detailed below.

Executive Leadership

Prior to the ISE-SAR EE, FDLE had no specific General/Special Order relating to SAR; however, it has several other investigative procedures that cover the receipt and documentation of SAR information. FDLE is currently completing an Intelligence Procedures Manual that will address the handling of SAR information by all FDLE and FFC personnel. The FFC Standard Operating Procedures Manual, as well as the InSite Operating Guidelines, addressed the receipt of domestic security and terrorism tips; these manuals have been updated to reflect the ISE-SAR process.

During the ISE-SAR EE, the FDLE command staff and senior management were briefed on the initiative and have shown their full support for this effort. Throughout the project, the FFC Director personally briefed the command staff as well as other state agencies' command staffs. FDLE utilized the Major Cities Chiefs Association's Chief Executive Officer Briefing to train more than a dozen law enforcement officials. During the project, the command staff attended conferences and meetings in which the SAR process implementation was discussed. As part of the SAR process planning development, a director was assigned to the project. The primary responsibility of the director is to implement a SAR process throughout FDLE, including the FFC.

SAR Business Process

Prior to the ISE-SAR EE, FDLE had a robust process for the collection of SARs. The FFC serves as the intake point for the collection of domestic security tips and suspicious activity data within the state. Law enforcement agencies throughout the state can electronically enter SARs into FDLE's Florida Intelligence Site (InSite[36]). Before this initiative, tips/SARs were initially reviewed by analysts within the Counter-Terrorism Intelligence Center (CTIC)[37] to determine their disposition, forwarded to appropriate agencies, and used to produce intelligence products, as necessary.

[36] InSite is the statewide intelligence system.
[37] CTIC is a component of the FFC.

During the ISE-SAR EE, the FFC modified InSite to capture and retrieve suspicious activity data utilizing the ISE-SAR Functional Standard list of behaviors and indicators to determine whether an entry is an ISE-SAR. It is standard policy that tips/SARs entered into InSite receive an initial vetting by a local supervisor who will approve the report for entry. These supervisors can assign these tips/SARS for review and investigation. As tip/SAR information is entered into InSite, analysts within the CTIC, immediately upon receipt, conduct initial vetting of each SAR received and move the SAR to the ISE-SAR Shared Spaces. If, during the review process, information is determined to have errors in the content or found to be incomplete, a formal process exists through which the source agency is contacted by the analyst for follow-up. All tips/SARs entered into InSite are reviewed every 90 days to determine their dispositions and to ensure that they have been fully investigated.

During the ISE-SAR EE, the FFC developed and implemented a privacy policy regarding the reporting of suspicious activity that met the applicable requirements of the ISE Privacy Guidelines. In order to protect the information within the ISE-SAR Shared Spaces, the FFC determined that only fusion center personnel would be allowed access to the ISE-SAR Shared Spaces. By policy, all queries on the information within the ISE-SAR Shared Spaces are for law enforcement purposes only and must have a criminal nexus. To ensure the protection of individual rights, the FFC has adopted internal operating policies and/or procedures that are in compliance with applicable laws and regulations protecting privacy, civil rights, and civil liberties, including but not limited to the U.S. Constitution and state, local, and federal privacy, civil rights, civil liberties, and legal requirements applicable to the FFC.

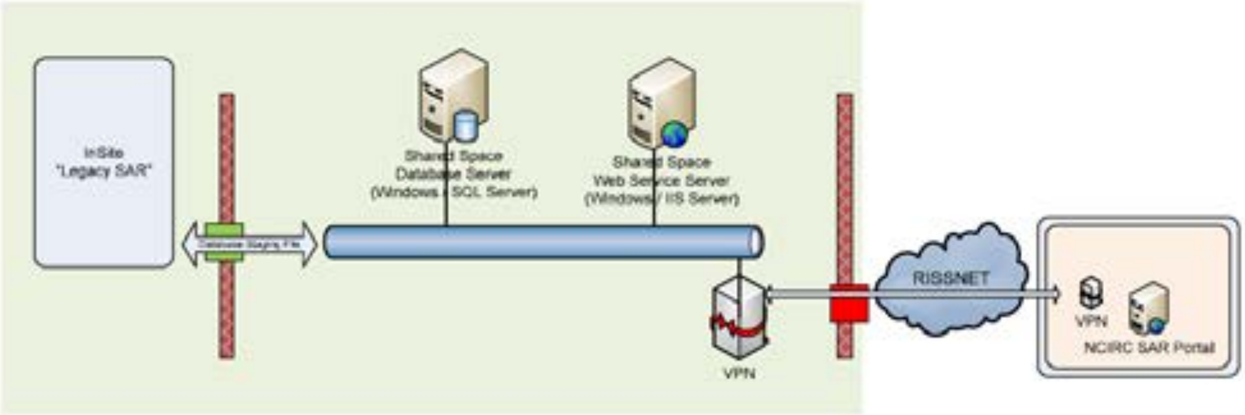
Prior to the ISE-SAR EE, all trained InSite users—including personnel from FDLE, FFC, the state's urban area fusion centers, and the Joint Terrorism Task Force (JTTF)—also had electronic access to the Florida data via InSite and could retrieve SAR data for further follow-up. When appropriate, information is forwarded to the Regional Domestic Security Task Force (RDSTF) and the JTTF. The Federal Bureau of Investigation (FBI) has access to InSite, which contains FDLE's tips and leads (SARs) as well as intelligence information. Unfortunately, the fusion center has no way to determine which SARs have been actioned by the FBI. The assignment of an FBI analyst to the FFC to assist with this follow-up process and analysis on InSite and eGuardian of SARs with a nexus to Florida would have been beneficial. During the ISE-SAR EE, FDLE maintained its partnerships with the previously mentioned agencies.

SAR Technical Process

FDLE uses an intelligence system called InSite that is provided by ACISS Systems, Inc. InSite has multiple modules, including a case management application that is used to track SARs. SARs are flagged for submission to the Shared Spaces by analysts at the FFC. Unlike the Virginia Fusion Center and the New York State Intelligence Center, FDLE information technology staff recommended a database replication technique using MS-SQL Utilities to "push" candidate SARs to a staging area database on the Shared Space Server. A specialized routine would then process the staged records and load the Shared Space repository.

As indicated above, the deployment of the Shared Space Servers in FDLE is slightly different from the standard deployment.

1. The virtual private network (VPN) connection between FDLE and the National Criminal Intelligence Resource Center portal is over the Regional Information Sharing Systems Secure Intranet (RISSNET) rather than the Internet.
2. The firewall between the database and Web servers was not required.



TRAINING

FDLE conducts numerous training events throughout the state of Florida; however, no specific training on the reporting of suspicious activity existed before the ISE-SAR EE. A brief description of the reporting of suspicious activity was mentioned in the required InSite training material.[38]

During the ISE-SAR EE, FDLE coordinated several SAR training events, including the Chief Executive Officer Briefing, the SAR analyst/investigator training, and the line officer training.[39] FDLE utilized the Bureau of Justice Assistance SAR analyst/investigator training within the state of Florida to target additional intelligence analysts. The analyst/investigator training was conducted throughout the state and had 103 attendees, representing 36 state, local, county, and federal agencies. The FFC indicated that additional training will be made available during agent in-service classes and that all SAR training is evaluated by the attendees.

[38] Individuals who have access to InSite are required to receive training on the system.

[39] The line officer training is under development, and the FFC worked with the International Association of Chiefs of Police during the pilot phase of the training.

The FFC is currently working with a vendor to develop training for all Florida law enforcement personnel on its SAR process. The training will include behaviors and indicators of terrorist activity and will also stress the importance of protecting privacy, civil liberties, and civil rights. To accomplish the long-term goal of training all Florida law enforcement personnel and fusion center partners, the FFC is seeking to deliver this as a Web-based training. Once developed, this training can quickly and efficiently be delivered to all applicable entities.

Institutionalization of the SAR Process

Prior to the ISE-SAR EE, the SAR process was not institutionalized agency-wide. However, since the inception of the ISE-SAR EE, the FFC has numerous initiatives under way to institutionalize the process. The FFC has an Intelligence Liaison Officer (ILO) program in partnership with 12 state agencies to assist in the gathering of suspicious information. Additionally, the RDSTFs have developed intelligence liaison officers within their regions.

The FFC has implemented quantitative measures to gauge the effectiveness of the SAR process; however, there are no performance metrics for qualitative data. The FFC currently reviews all SAR data in the InSite system for quality control purposes. To fully integrate critical infrastructure and key resources (CIKR) into the SAR process, the FFC coordinated its efforts with the FBI and the U.S. Department of Homeland Security (DHS) to develop alerts, warnings, and notifications and other relevant reports for CIKR entities. The center currently has a list of coordinated information needs that have been developed with DHS.

Outreach to the Public

Prior to the ISE-SAR EE, FDLE had instituted multiple outreach initiatives throughout the state of Florida and, due to the ISE-SAR EE, began including the SAR process information in its community outreach. FDLE has previously divided the state into seven regions to maximize regional support for local law enforcement. To harness this regional landscape for outreach efforts, each of the RDSTFs was tasked with outreach efforts in its respective region.

The FFC continues—as it has in the past—to post information to the public Web site and has an extensive e-mail notification system to reach out to stakeholders within the state. Additionally, FFC has provided further public outreach through the delivery of training and has developed a public Web site for business owners that describes how these owners can have a “safe business.” The Computer Crime Center maintains a “Secure Florida” Web site to provide information about cyber security. The FFC has provided each RDSTF and regional office with the *Safeguarding America—It All Starts With You* DVD to identify the types of suspicious activity the public should be aware of.

Partnering With Other Agencies and Connecting to Information Sharing

Prior to the ISE-SAR EE, the FFC had developed strong partnerships with other agencies and engaged in various forms of information sharing. During the ISE-SAR EE, partnerships became stronger because of the time devoted to the project and the additional collaboration required to make this initiative a success. To ensure comprehensive information sharing, the FFC has engaged in various efforts to demonstrate its current information sharing efforts and expand on these efforts. The FFC has worked closely with other state fusion centers, homeland security officials, and the JTTF. The FFC has regularly conducted domestic security briefings to the Florida Legislature and routinely provides briefings to the state's homeland security advisor. The center has also provided high-level and general situational awareness information within the state to FDLE command staff in preparation for legislative committee meetings.

The FFC has partnered with numerous public safety agencies—including the Florida Fire Chiefs' Association, the Florida Sheriffs Association, the Florida Chiefs of Police Association, the Florida Division of Emergency Management, and the Florida Department of Health—in an effort to effectively share information. The FFC continues to work with other organizations and agencies in its information sharing efforts, including the Nationwide SAR Initiative (NSI) partners, Southern Shield, and the Law Enforcement Intelligence Unit.

The FFC has access to numerous information sharing networks, including RISSNET, Law Enforcement Online (LEO), and the Homeland Security Information Network (HSIN). The FFC can send and receive secure e-mails and has access to the state criminal justice networks, databases, and regional intelligence databases. Access to these systems allows for comprehensive information sharing with all of the FFC's constituents.

Partnering to Develop Geographic Risk Assessments

Prior to the ISE-SAR EE, the FFC worked with the FBI and DHS in the development of geographic risk assessments, which were mostly driven by special events in Florida (e.g., the Super Bowl). However, the FBI does not provide these assessments routinely to the state. The FFC has instituted a production calendar plan for the regular development of coordinated risk assessments with federal, state, and local agencies and fusion centers. Once the risk assessments are complete, a process will be developed to understand and address the identified information needs, to task the RDSTFs with gathering information related to these needs, and to incorporate them into the SAR process.

Although FDLE and the FFC have a process for developing geographic risk assessments with federal agencies, during the ISE-SAR EE, there has been no additional emphasis placed on this effort.

Project Recommendations From the Florida Department of Law Enforcement

- ➢ The FFC believes that there needs to be a national program office for the NSI that is a strong, centrally coordinated effort. The office should not be divvied out to multiple federal agencies.

- A national training program is recommended to maintain consistency in the collection of SAR information. The center suggested the creation of a train-the-trainer program, with template teaching materials, so that the states could train their own regions and jurisdictions.
- A small national users group for the initiative was suggested. The group should meet regularly and should be divided into subgroups to deal with policy/legal issues, training, and technology.
- There needs to be continual technical support for the applications developed by the project.
- There needs to be legal assistance to help develop policies for participating agencies. However, the legal office should not be so large that it creates problems for the state and local agencies. The legal assistance could be handled by two or three full-time subject-matter experts.
- The FFC commented that there are no policy, technical, or legal issues that it could not overcome.
- The privacy policy template was very helpful in developing the FFC privacy policy.

HOUSTON, TEXAS, POLICE DEPARTMENT

SAR PROCESS REPORT—POST-IMPLEMENTATION PHASE

Following the conclusion of the Information Sharing Environment-Suspicious Activity Reporting Evaluation Environment (ISE-SAR EE), a discussion was held with the Houston, Texas, Police Department's (HPD) Houston Regional Intelligence Service Center (HRISC) to document the implementation efforts conducted during the ISE-SAR EE. The results of the discussion are detailed below.

EXECUTIVE LEADERSHIP

Prior to the ISE-SAR EE, HPD Chief Harold Hurtt issued General Order No. 800-07 regarding "Criteria for Submitting Incident Reports" on June 12, 2007.[40] The order includes a section on suspicious activity and lists 13 behaviors that officers are required to report, if observed. The command staff/senior management had been briefed on HPD's SAR policy.

During the ISE-SAR EE, Chief Hurtt gave his full support to the SAR initiative and has been a nationwide leader in the development of SAR policy. Chief Hurtt and other members of the HPD command staff attended the Major Cities Chiefs Association's (MCCA) Chief Executive Officer Briefing (CEOB) held in April 2009, which included 30 participants from 27 law enforcement agencies. In addition, the entire HPD command staff has been fully briefed on the ISE-SAR EE and the SAR process. The commanding officer of the Criminal Intelligence Division (CID) has been assigned primary responsibility for handling and processing SARs, and a CID lieutenant has been assigned to implement the ISE-SAR EE efforts within the HRISC.

SAR BUSINESS PROCESS

Prior to the ISE-SAR EE, HPD had a robust process for the reporting of suspicious activity. HPD's reporting process for suspicious activity requires that all officers complete an "Investigation CID" report (information report) concerning any suspicious activity that is identified in the General Order. If a suspect identified in an information report is in custody or suspicious circumstances require additional investigative assistance, the involved officer will contact CID. For reports forwarded to HRISC, the center will attempt to contact the officer who submitted the information report; however, no formal process was in place.

CID is the intake point for all information reports and immediately reviews the reports to identify any behaviors and indicators associated with terrorist activity. Within 24 hours, all terrorism-related SARs are forwarded to HRISC, which is designated as the primary entity to analyze SAR data within the department. Prior to the ISE-SAR EE, the HRISC did not use the

[40] A copy of the General Order is available upon request.

behavior-specific codes identified in the ISE-SAR Functional Standard for SAR data but tracks the suspicious activity in similar categories that can be translated to the codes.

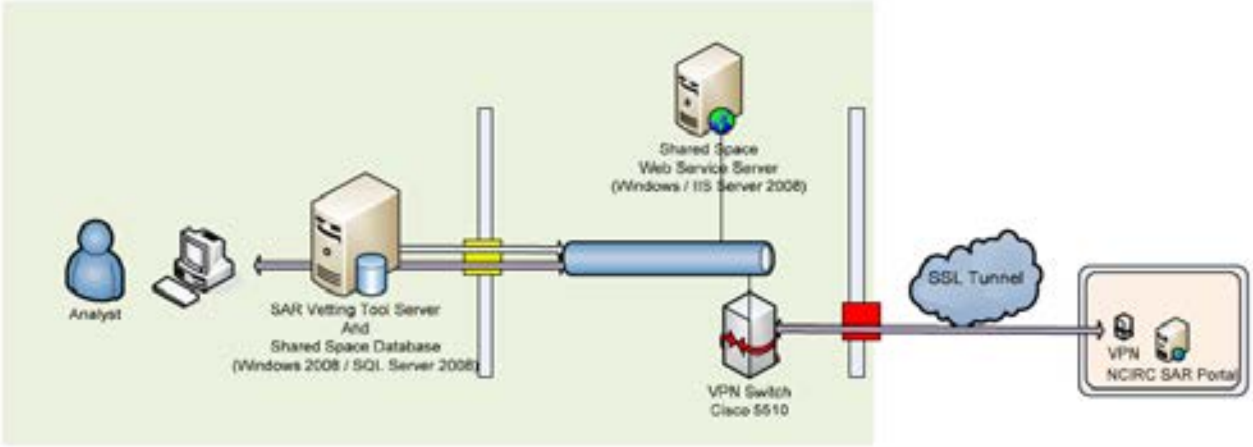
All SARs are also forwarded to the Joint Terrorism Task Force (JTTF), which is given the "right of first refusal" for follow-up activity relating to the SAR. If the JTTF chooses not to follow up, the SARs are then investigated by HRISC. HRISC also downloads all Terrorist Screening Center (TSC) reports from Law Enforcement Online (LEO) daily and compares the reports with local information. HRISC creates weekly summaries based on the TSC reports and sends those summaries to appropriate federal, state, and local agencies.

During the ISE-SAR EE, HPD adopted the behavior-specific codes specified in the ISE-SAR Functional Standard. The command staff decided that they would continue to use their previous "Investigative CID" report because of its comprehensiveness and familiarity to the officers. The department has created a "tips and leads" form for the fire department and other government agencies so that suspicious activity information can be routed to HPD. The department continues to use its current records management system (RMS); however, it is reviewing and planning for a new system that will include new forms for SARs.

During the ISE-SAR EE, HPD enhanced its multilayer review process to enter SARs into the ISE-SAR Shared Spaces. The department utilizes its previous vetting process but implemented a final supervisory approval before a SAR is entered into the ISE-SAR Shared Spaces. This will ensure that multiple trained personnel have reviewed the information for accuracy and completeness before submission. This continual review is in place to prevent any erroneous information from entering the ISE-SAR Shared Spaces. If an error is ever detected, the source agency or individual is contacted and the information is corrected. The CID and HRISC developed and implemented a privacy policy regarding the reporting of suspicious activity that met the applicable requirements of the ISE Privacy Guidelines. Access to the ISE-SAR Shared Spaces is limited based upon the individual's role within the HRISC, and by policy, all querying of SAR information must have a criminal nexus and be for legitimate law enforcement purposes.

SAR Technical Process

Prior to the ISE-SAR EE, HPD utilized an RMS as the central location for all HPD officers' information reports. CID conducts daily searches in the RMS system and identifies any terrorism-related reports to forward to HRISC. Once forwarded to HRISC, the reports are entered and maintained electronically in an internally developed SAR database. During the ISE-SAR EE, HRISC requested that the SAR Vetting Tool (SVT) augment existing legacy system data and act as a bridge between the legacy system and the ISE-SAR Shared Spaces database. The SVT application and database were installed on the ISE-SAR Shared Spaces Server as an economical approach to share hardware and MS-SQL resources. The common architecture is described below.



TRAINING

Prior to the ISE-SAR EE, all HPD officers had undergone a four-hour training course on terrorism indicators and trained on identifying suspicious activity. The training course includes privacy protections, 28 Code of Federal Regulations (CFR) Part 23, and the need for a criminal nexus when reporting suspicious activity. As new trends emerge and lessons learned are identified, the training programs will be modified and enhanced as necessary. Additionally, officers receive updates from the fusion center concerning current activities.

During the ISE-SAR EE, HPD maintained its current terrorism indicator and identifying suspicious activity training during in-service and recruit training. In addition, HPD participated in the CEOB and the SAR analyst/investigator course.[41] The SAR analyst/investigator course was delivered in March 2009, and 32 individuals received the training from 8 agencies in the Houston area.

INSTITUTIONALIZATION OF THE SAR PROCESS

Prior to the ISE-SAR EE, yearly audits were conducted on SAR data to determine relevance and to ensure that the data meets agency purge requirements. SARs are reviewed for emerging trends and behaviors to determine priority information needs within the department, and SAR information is used in the development and issuance of alerts, warnings, and notifications. HPD also works closely with agencies such as the U.S. Department of Homeland Security (DHS), the JTTF, and the Texas Department of Public Safety (DPS) to determine additional information needs. Assessments are conducted within the department to determine the effectiveness of the SAR process.

During the ISE-SAR EE, HPD continued the previously mentioned institutionalization efforts and began developing a Terrorism Liaison Officer (TLO) program with other agencies in the Houston area. HPD is currently using the TLOs that have been trained to assist the fusion center with providing tips and leads within their respective sectors.

[41] The CEOB was previously discussed in the Executive Leadership section.

Outreach to the Public

Prior to the ISE-SAR EE, HRISC had an outreach program with the public and has conducted community meetings, trained members on the Crime Stoppers program, and coordinated with the Houston-area Federal Bureau of Investigation's (FBI) tip hotline. The hotline can be used to report suspicious activity. HRISC also works with the U.S. Attorney's Office and the Anti-Terrorism Advisory Council (ATAC) to provide outreach to the private sector and has provided training to human trafficking/smuggling enforcement groups.

During the ISE-SAR EE, HPD continued its outreach efforts and is developing an iWATCH program based upon the lessons learned from the Los Angeles, California, Police Department.

Partnering With Other Agencies and Connecting to Information Sharing

Prior to the ISE-SAR EE, HPD worked with MCCA, the FBI, DHS, and the Texas DPS to collaborate on fusion center issues and policies. External stakeholders, including members of Congress, have been briefed on the SAR process, and educational outreach has been provided to public safety and the private sector entities.

HRISC is a member of the Regional Information Sharing Systems Secure Intranet (RISSNET), LEO, and the Homeland Security Information Network and has the ability to send and receive secure e-mails primarily through the LEO e-mail system. HRISC has access to the state's criminal justice network, and a Texas DPS representative who can access the state's intelligence database is assigned to the center. HRISC has access to eGuardian but does not input information into the system. HRISC also posts information to a special-interest group on LEO.

During the ISE-SAR EE, HPD continued its previous partnerships and efforts to connect to information sharing systems. HPD officers work with the public health and private sector industries on identifying suspicious activity.

Partnering to Develop Geographic Risk Assessments

Prior to the ISE-SAR EE, multiple assessments were being conducted in the Houston area. HRISC works closely with DHS, the JTTF, the U.S. Attorney's Office, and the ATAC to develop geographic risk assessments. Threat assessments are completed with the FBI and other local agencies within the 13-county Urban Areas Security Initiative, and these assessments drive HPD information needs. Critical infrastructure assessments are completed by another agency within the city of Houston.

During the ISE-SAR EE, HPD continued its partnerships in the development of information needs and risk assessments.

Project Recommendations From the Houston Police Department

HPD felt that there is no need for a national program office; however, there is a need for national consistency in how SAR information is handled because every jurisdiction is unique.

There is a need for consistent SAR training nationwide. The fundamentals are already in place with the CEOB, SAR analyst/investigator course, and the line officer training.

A national users group would be helpful as the project expands nationwide to share best practices and to develop methods for the best use of the information.

There is a need for nationwide analysis of the data that is being gathered by agencies around the country.

There is a continuing need for technical support as information systems change and agencies need assistance in purchasing compatible systems.

There is a need for reporting tools to be used in order to conduct analysis of the agency's information.

There is a need for a national legal office, since there are many difficult legal issues that agencies face as they try to share information.

Las Vegas, Nevada, Metropolitan Police Department

SAR Process Report—Post-Implementation Phase

Following the conclusion of the Information Sharing Environment-Suspicious Activity Reporting Evaluation Environment (ISE-SAR EE), a discussion was held with the Las Vegas, Nevada, Metropolitan Police Department's (LVMPD) state-designated fusion center, the Southern Nevada Counter-Terrorism Center (SN/CTC), to document the implementation efforts conducted during the ISE-SAR EE. The results of the discussion are detailed below.

Executive Leadership

Prior to the ISE-SAR EE, LVMPD had no General/Special Order related to SAR; however, Sheriff Douglas Gillespie had been a principal participant in the creation of the Major Cities Chiefs Association's (MCCA) SAR process. During the ISE-SAR EE, the command staff was briefed on the Nationwide SAR Initiative (NSI) and the implementation of the SAR process, which was a priority of the sheriff. There is a plan to develop a standard operating procedure (SOP), but it has not been implemented yet. As part of the LVMPD SAR process planning development, a lieutenant was assigned to implement a SAR process throughout LVMPD, including SN/CTC.

During the ISE-SAR, the LVMPD received the MCCA's Chief Executive Officer Briefing in March 2009, and 24 command staff personnel from approximately 8 law enforcement agencies participated.

SAR Business Process

Prior to the ISE-SAR EE, SN/CTC served as the intake point for the collection and receipt of SARs and provides "real-time" monitoring of all LVMPD reports. The field interview reports and information reports used by LVMPD were not modified to report SAR data, but all reports were reviewed by district supervisors for suspicious activity. If a report is deemed to contain suspicious activity, it is forwarded to SN/CTC for immediate investigation. All SARs are reviewed and a decision is made whether to respond, refer, determine unfounded, or take other action, including investigative action. Feedback to the reporting officer is a routine internal operating procedure. Computer-aided dispatch (CAD) data is also reviewed by SN/CTC for potential suspicious activity.

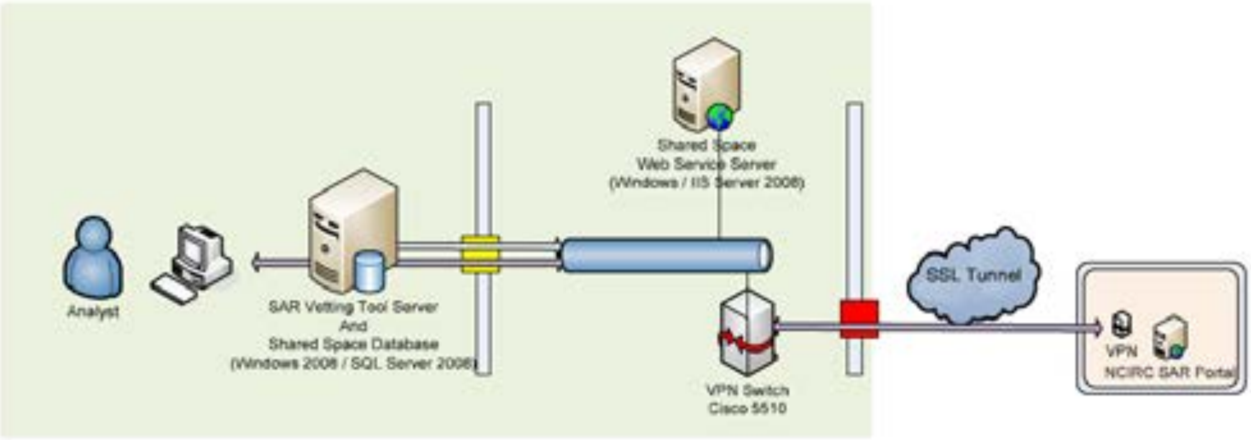
During the ISE-SAR EE, LVMPD adopted the behavior-specific codes specified in the ISE-SAR Functional Standard. The department is in the beginning stages of developing a formalized, policy-driven SAR process within the agency. There is a plan to evaluate and simplify the reporting process and develop an internal multilayer review and vetting process to identify ISE-SARs and a procedure for moving SARs to the ISE-SAR Shared Spaces. The new processes and procedures will be included in the yet-to-be-developed SOP. SN/CTC has not modified the basic report and is creating a data warehouse of police databases to access the SAR information. In addition, SN/CTC is developing a search tool to allow for the review of police reports for SAR data. During the ISE-SAR EE, SN/CTC utilized the SAR Vetting Tool (SVT) for storing terrorism-related SARs. Currently, SN/CTC is establishing a Web site to enable direct SAR reporting from the public and other agencies. The center is also in the process of staffing a 24-hour homeland security hotline as another form of reporting SARs.

During the ISE-SAR EE, SN/CTC developed a privacy policy regarding the reporting of suspicious activity; however, due to departmental review processes the policy has not been finalized. It is anticipated that once finalized, the policy will meet the applicable requirements of the ISE Privacy Guidelines. In order to protect the information within the ISE-SAR Shared Spaces, it was determined that only personnel within the fusion center would be allowed access to the SVT and ISE-SAR Shared Spaces. By policy, all queries on the information within the ISE-SAR Shared Spaces is for law enforcement purposes only and must have a criminal nexus.

SAR Technical Process

Prior to the ISE-SAR EE, the SN/CTC SAR technical process utilized a records management system and a CAD system to collect, store, and retrieve SAR data. SAR data determined to have a potential link to terrorist activity was not stored separately. Prior to the ISE-SAR EE, LVMPD was developing a computer system—the All Data Virtual Information Sharing Environment (ADVISE)—that will allow for the collation of SAR data within the department. ADVISE will also allow for real-time gathering, processing, analyzing, reporting, and sharing of department-wide SAR data.

During the ISE-SAR EE, LVMPD requested the SVT to augment existing legacy system data and act as a bridge between the legacy system and the Shared Spaces database. The SVT application and database were installed on the ISE-SAR Shared Spaces Server as an economical approach to share hardware and MS-SQL resources. The common architecture is described below.



Training

Prior to the ISE-SAR EE, LVMPD developed a terrorism training program based on the behaviors and indicators learned from prior terrorist attacks around the world, including the London bombings, the World Trade Center attacks, and the train bombings in Spain. LVMPD also utilizes a very robust Terrorism Liaison Officer (TLO) program. The TLOs receive a four-hour training class and are assigned to LVMPD district offices. The TLOs are responsible for the implementation of the terrorism training program within the department. In the department's academy, officers receive training on SN/CTC and its operations. The training emphasizes privacy protections and the observation of behaviors relating to precursor activities of terrorist attacks. However, prior to the ISE-SAR EE, no specific training on the SAR process existed.

During the ISE-SAR EE, LVMPD participated in the Chief Executive Officer Briefing and the analyst/investigator course. During the SAR analyst/investigator course in the Las Vegas area in April 2009, 35 personnel were trained from 10 law enforcement agencies. In addition, SN/CTC is currently developing a training program for line officers and will train officers based upon the SAR process, which will be defined in the SOP. The agency will develop a mechanism to capture feedback on the value of the information being collected.

Institutionalization of the SAR Process

Prior to the ISE-SAR EE, SN/CTC had numerous initiatives under way that will aid in the institutionalization of the SAR process once it is formalized within the department. In addition to LVMPD officers, the TLO program includes other first responders, such as fire representatives and the private sector. SN/CTC is also working to involve the university campus police in the TLO program.

Prior to the ISE-SAR EE, no audits were being conducted on SAR data and no processes were in place to determine the effectiveness of the SAR system; however, once implemented, the ADVISE system will allow for audits and performance analysis.

Prior to the ISE-SAR EE, the SAR process and priority information needs were interconnected within LVMPD. The emerging trends, behaviors, and indicators from SAR data drove the identification and enhancement of the department's information needs. SN/CTC also works with the Federal Bureau of Investigation (FBI) and the U.S. Department of Homeland Security (DHS) to determine information needs and to develop crime and terrorism alerts and advisories and homeland security threat assessments. SAR information received by SN/CTC is the primary driving force behind the issuance of alerts and warnings.

During the ISE-SAR EE, SN/CTC continued its efforts to institutionalize the SAR process throughout the department.

Outreach to the Public

Prior to the ISE-SAR EE, SN/CTC had a very aggressive outreach program. When SN/CTC first opened in January 2008, the media was invited to the center and was provided a full briefing on the center's operations.[42] Since the center became operational, numerous public documents and publications have been produced to explain terrorism indicators and the purpose of the center. More than 60,000 *Seven Signs of Terrorism* DVDs and *If You See Something, Say Something* CDs have been produced and distributed to the public. The center also has an online SAR form[43] that the public can access and use to submit "all-crimes, all-hazards" suspicious activity. Additionally, the center is developing a Web site and a statewide toll-free terrorism hotline.

During the ISE-SAR EE, SN/CTC continued its robust outreach program and is currently developing an iWatch program similar to the program initiated by the Los Angeles Police Department. Additionally, due to the unique characteristics of Las Vegas, LVMPD is focusing its outreach on hotel staff—valet attendants, security, bell captains, and housekeeping as well as the casinos.

Partnering With Other Agencies and Connecting to Information Sharing

Prior to the ISE-SAR EE, SN/CTC held on-site briefings and invited external stakeholders—including congressional delegates—to the center to learn about SN/CTC activities and operations. Outreach opportunities and partnerships have also been developed with multiple agencies through the utilization of the TLO program and public media outlets.

The center can access the Regional Information Sharing Systems Secure Intranet (RISSNET), Law Enforcement Online, and the Homeland Security Information Network and through these networks, as well as through the Homeland Security Data Network, has the ability to send and receive secure e-mail. SN/CTC has representation from DHS, the FBI's Joint Terrorism Task Force, and other law enforcement entities within the center. However, SN/CTC does not have access to eGuardian. The center can also access the state's criminal justice network and the regional intelligence system. The Nevada State Fusion Center was not fully operational at the time of the site visit, but once the state's center has information sharing capability, SN/CTC will pursue a relationship with the center.

During the ISE-SAR EE, SN/CTC continued its aforementioned partnerships in order to maintain connectivity with other fusion centers.

Partnering to Develop Geographic Risk Assessments

Prior to the ISE-SAR EE, SN/CTC noted that there is no formal process in place for the center to work with federal agencies to develop geographic risk assessments, but the center

[42] The LVPD press release is available at http://www.lvmpd.com/news/pdfs/2008/011808release.pdf.
[43] The SAR form is available at http://www.lvmpd.com/pdf/SAR_form.pdf.

receives risk assessments from DHS and the FBI when requested and does coordinate to develop information needs. SN/CTC has developed vulnerability assessments for critical infrastructure and key resources in the Las Vegas area and has also developed threat assessments on specific events, such as highly publicized sporting events.

During the ISE-SAR EE, SN/CTC continued its aforementioned partnerships in the development of information needs and risk assessments. In addition, SN/CTC participates in a multilogo assessment with federal agencies. SN/CTC indicated that threat assessments from the federal agencies are so general as to not be able to develop specific information needs. It is the responsibility of the local fusion center to take the general threat assessments and enhance them to fit its specific jurisdiction.

Project Recommendations From the Las Vegas Metropolitan Police Department

- There is a need for an NSI national program office only as it relates to consistency, funding, and coordination nationwide.
- There is a need for an NSI national training program that can illustrate the value of the initiative to agencies. A national training program will also provide more exposure of the program to agencies nationwide.
- There is a need for an NSI national users group for the purpose of having a good feedback loop and to define performance matrix.
- There is a continued need for ongoing NSI technical assistance.
- There is a need for a general domestic security officer to address all national matters relating to fusion centers, including the NSI.
- There needs to be improvement on marketing efforts to make sure the general public, legislatures, and others are fully informed about the SAR initiative.

LOS ANGELES, CALIFORNIA, POLICE DEPARTMENT

SAR PROCESS REPORT—POST-IMPLEMENTATION PHASE

Following the conclusion of the Information Sharing Environment-Suspicious Activity Reporting Evaluation Environment (ISE-SAR EE), a discussion was held with the Los Angeles, California, Police Department (LAPD) to document the implementation efforts conducted during the ISE-SAR EE. The results of the discussion are detailed below.

EXECUTIVE LEADERSHIP

Prior to the ISE-SAR EE, Chief William Bratton issued Special Order 11 on March 5, 2008, titled "Reporting Incidents Potentially Related to Foreign or Domestic Terrorism." With the release of the Special Order, the SAR process was formalized within LAPD. After the order was issued, all command staff and personnel were trained on the processes noted in the order.

During the ISE-SAR EE, LAPD—in partnership with the Major Cities Chiefs Association (MCCA)—hosted a Chief Executive Officer Briefing in February 2009 with 51 attendees from 26 law enforcement agencies. In addition, LAPD provides continuous training on the SAR process to all new executive leadership within the department.

SAR BUSINESS PROCESS

Prior to the ISE-SAR EE, LAPD had an extremely robust process for the collection of SARs and was used as a national model when developing the ISE-SAR EE. LAPD developed data collection codes (modus operandi [MO] codes) for the reporting of suspicious activity. The purpose of the MO codes is to provide a standardized method to document behavioral indicators that may have a potential nexus to terrorism and to provide the ability to analyze the data by date, time, and location, just as is done with crime codes. LAPD also uses the codes to train its personnel on how to recognize suspicious activity. LAPD conducted research to develop patterns and determine the frequency of use of the codes. In addition to the development of the MO codes, LAPD modified its existing Investigative Report used by officers to report crimes. Three changes were made: (1) the addition of a check box to identify the report as containing suspicious activity, (2) the addition of a check box for distribution to the Counter-Terrorism and Criminal Intelligence Bureau (CTCIB) Major Crimes Division (MCD), and (3) "Involved Party (IP)" information. Modifying the existing report allowed LAPD to simplify the introduction of the SAR process within the department and was instrumental in the institutionalization of the SAR process.

Once an Investigative Report is identified as containing suspicious activity, it is forwarded to the MCD SAR Unit for processing and analysis. The MCD SAR Unit serves as the centralized unit responsible for updating all incoming Investigative Reports with either the SAR check box or CTCIB-MCD check box marked. The unit is also responsible for tracking, vetting, and assigning MO codes and investigative responsibility for all SAR reports. During the vetting stage, SARs that met certain criteria (as determined by the SAR Unit) were sent to the Federal Bureau of Investigation's (FBI) Counterterrorism 6 (CT-6) Unit.[44]

Investigative Reports written by LAPD officers that contain SAR information are forwarded within 24 hours to the SAR Unit at CTCIB's MCD for initial vetting by trained personnel and appropriate response. A process is in place to forward SARs to the Joint Regional Intelligence Center (JRIC), which serves as the Los Angeles-area fusion center. Following initial vetting of the information, the MCD SAR Unit makes a determination on whether to forward the information to JRIC and/or to the Joint Terrorism Task Force (JTTF). Information is forwarded to JRIC electronically and uploaded to JRIC's system using Memex software.

For SARs maintained by LAPD, further vetting takes place to determine investigative responsibility within MCD. If a SAR is found to be erroneous or does not meet a certain level of quality, the report is categorized as Unfounded and feedback is provided to the source agency or citizen. The SAR Unit maintains an up-to-date record of all SARs, including who has investigative responsibility for the SAR, the current status of each SAR, the number of unfounded reports, which reports are shared with JRIC and/or the JTTF, and which reports are submitted to the ISE. Due diligence is given to each and every SAR report. The SAR Unit provides a timely, consistent flow of SAR data and terrorism-related information to the Terrorism Liaison Officers (TLOs), who are assigned on a geographic basis to all LAPD divisions. The TLOs' responsibility includes communicating with the officers at their assigned LAPD division and liaising with other government agencies and local business partners within the TLOs' area of responsibility. The TLOs are also utilized to provide feedback to the officers and/or local agencies or business partners that submit SAR data to the department. The bureau commander also sends e-mails and written commendations to the entities that submit a SAR to the department highlighting excellent work.

LAPD had an existing records management system, known as the Consolidated Crime and Analysis Database (CCAD), which housed all crime and arrest data. CCAD was modified to include SARs and SAR MO codes. CCAD allows for the immediate retrieval of all SAR and crime data and stores the data indefinitely, allowing for reach-back capabilities. During the ISE-SAR EE, LAPD replaced its 30-year-old Crime Mapping Database (CMDB) system with the Crime Analysis Mapping System (CAMS). CAMS allows for the analysis and mapping of SAR data. LAPD also developed a procedure for moving SARs to the ISE SAR Shared Spaces. SARs that meet the behavior-specific codes outlined in the ISE-SAR Functional Standard are entered into the SAR Vetting Tool (SVT) by trained analysts in the SAR Unit and moved to the

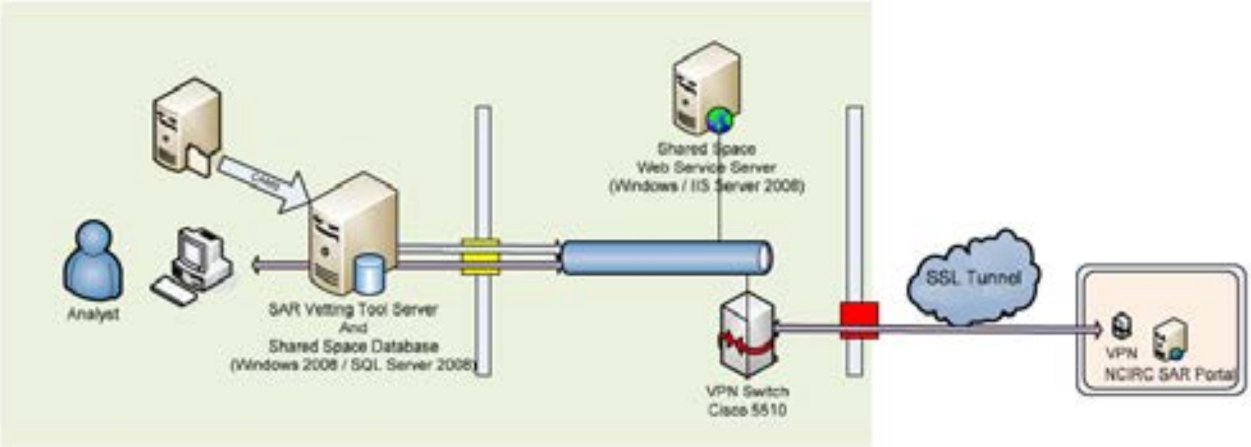
[44] This is a regionally based FBI counterterrorism squad located in a command center in Norwalk, California, and is responsible for protecting seven counties and 18 million people. The CT-6 Unit was created in May 2004 after a series of reported threats diverted too much manpower from other counterterrorism investigators.

ISE-SAR Shared Spaces. Only a few personnel within the SAR Unit have access to the ISE-SAR Shared Spaces, however, and MCD plans to expand the access list. It is department policy that querying and use of the ISE-SAR Shared Spaces be for legitimate law enforcement purposes.

Prior to the ISE-SAR EE and the formalization of the SAR process within the department, LAPD had a long-standing privacy policy that was adjusted to include SAR processes. LAPD consulted with the department's legal section and the city attorney's office to help in that adjustment. LAPD also consulted with the American Civil Liberties Union (ACLU) and the department's Office of the Inspector General, as well as regional private sector groups. LAPD met regularly with ACLU representatives to continue communication and information flow. During the ISE-SAR EE, LAPD submitted its privacy policy documents for the purposes of participation in the ISE-SAR EE; the policy was reviewed and determined to be consistent with the applicable requirements of the ISE Privacy Guidelines.

SAR Technical Process

LAPD captures all incident data, including SARs, in CCAD, which is then downloaded to CAMS. Based on flags in CAMS, an extraction routine pulls SARs from CAMS and loads the SVT. Once in the SVT, LAPD analysts can then review the basic information and augment specific SARs with other information it may possess and then elect to "push" the SAR to its ISE-SAR Shared Spaces. Although the network options and hardware equipment varied at each site, the essential applications were the same. In the common architecture, the decision was made to leverage existing hardware and database software resources to colocate the SVT with the Shared Spaces database application and have both applications separated from the Web server by a security firewall. LAPD has moved one step further by adding a legacy database to feed the SVT with SAR incident data as shown in the diagram below.



Training

Prior to the ISE-SAR EE, LAPD developed a framework for the training of each officer involved in the development and submission of SARs. Training programs—including e-learning, a training film, PowerPoint presentations, and roll call presentations—were created and delivered to all command staff, new recruits, and civilian and sworn personnel prior to the implementation of LAPD's SAR process. Additionally, ongoing TLO training will be included in roll call training efforts. Training focuses on the importance of privacy and civil liberties protections; the gathering of suspicious activity through behavior-based policing, including behaviors and/or incidents known to be exhibited in terrorism-related suspicious activity; the mechanism for reporting SARs (standardization); the processing of SARs within the department; steps taken in the analysis of SAR data; and the appropriate sharing of suspicious activity within and outside the department.

During the ISE-SAR EE, LAPD continued its robust training throughout the department. In addition to agency training, in July 2009, LAPD participated in the SAR analyst/investigator training, in which 53 individuals from eight law enforcement agencies were trained. The outstanding level of SAR information being received by the SAR Unit has been a testimony to the multiple training efforts conducted throughout LAPD.

Institutionalization of the SAR Process

Prior to and during the ISE-SAR EE and since the release of Special Order 11, LAPD has taken numerous steps to institutionalize the SAR process within the department. As previously indicated, LAPD has a highly developed TLO program. Each division office includes at least two officers trained as a TLO. The department also trains designated TLOs to interact with other government agencies; the goal of this training effort is to assist the CTCIB in the implementation and institutionalization of the SAR process among other government agencies and throughout the community. The SAR process is also regularly evaluated and modified, and training is enhanced as a result of identified emerging trends and lessons learned.

LAPD developed internal and external audits as well as management tools that evaluate the current SAR reporting process. Internal audits are conducted daily by the SAR Unit to ensure that a report is filed on all documented SARs. The SAR process was added to the annual external audit schedule of the Inspector General's Office and the semiannual internal audit schedule of LAPD. LAPD's management tools include reports to help identify emerging trends and gaps. Additionally, the CTCIB developed management "at-a-glance" reports that provide the status of all SAR reports and track SAR activity by date, time, and location. The management accountability reports provide a foundation for management decisions as well as the allocation of resources.

LAPD analyzes all SAR reports and utilizes the all-crimes approach to identify emerging trends and behavior patterns. As new information is received and new patterns and priority information needs are identified, the SAR process is modified to meet these needs. The CTCIB also leverages existing technology to develop the management of at-a-glance reports to provide a complete overview of SAR activity in the jurisdiction at all times. Special reports, alerts, warnings, and notifications based on the analysis of SARs, crime, and arrest activity are developed and shared internally within the department and externally with regional partners, local law enforcement, and security personnel at critical infrastructure and key resources locations.

Outreach to the Public

Prior to and during the ISE-SAR EE, LAPD developed and launched the iWATCH[45] program. This program educates the public regarding suspicious activity, including behaviors and indicators of suspicious activity, and the importance of reporting suspicious activity. The program includes a Web site for the reporting of suspicious activity.[46] Since the release of iWATCH in October 2009, the Web site has already received several thousand hits.

In addition, LAPD developed public service announcement (PSA) media commercials to explain how the SAR program works and articulate the need to report information concerning terrorism to the police department. Department TLOs share in the responsibility to present to community groups and interested sectors concerning the reporting of suspicious activity. LAPD also introduced the SAR program to the community through forums, meetings, and the distribution of informational flyers during these events. LAPD developed DVDs about suspicious activity reporting that contain all the information that will be available on the Web site. LAPD also has officers assigned to a tip line—"(877) A-Threat"—that individuals can call to speak with an expert and let them decide whether the activity is suspicious.

During the development of iWATCH, LAPD involved the ACLU in the development of the script for the PSA and, prior to the launch, met again with the ACLU officials to give them a preview of iWATCH and allow them to make comments.

Partnering With Other Agencies and Connecting to Information Sharing

Prior to the ISE-SAR EE, Chief Bratton was very public in informing external stakeholders about LAPD's SAR program to build on its strong partnerships within the region. Several meetings were held to introduce the SAR program to the department's partners, including state and local government agencies and public safety agencies in the region. The TLO program has also been utilized extensively by LAPD for outreach to the private sector as well as other government agencies. LAPD continues to have a strong relationship with the U.S. Department of Homeland Security (DHS) and the JTTF through JRIC. Additionally, LAPD has built a regional awareness of SARs and provides training to local law enforcement

[45] See www.iwatchla.org.
[46] The Web site may be applied nationally for other agencies to utilize in their SAR processes.

partners, including the Los Angeles Port Police, Los Angeles Unified School District Police, Los Angeles Airport Police, and City of Long Beach Police. As previously stated, LAPD provides all vetted SAR information to JRIC, and the information is also provided to the FBI's CT-6 Unit and other agencies as appropriate.

LAPD can access the Regional Information Sharing Systems Secure Intranet (RISSNET), the FBI's Law Enforcement Online, and the Homeland Security Information Network and can send and receive secure e-mail via these secure networks. LAPD can also access the state's criminal justice network; can participate in a number of regional intelligence databases, including regional information sharing systems; and has a direct connection to the regional fusion center as well as the other regional fusion centers within the state of California.[47]

LAPD is actively engaged with nationwide partners as well as federal officials in the development of its SAR program. After LAPD formalized the SAR process within the department, it collaborated with state and local law enforcement agencies, the Office of the Program Manager for the Information Sharing Environment, the ACLU, and members of the MCCA's Intelligence Commanders Group to discuss policies and procedures concerning the reporting of suspicious activity.

During the ISE-SAR EE, LAPD continued its strong partnerships with other agencies throughout the city, regional, state, and national levels.

Partnering to Develop Geographic Risk Assessments

Prior to and during the ISE-SAR EE, LAPD worked with state and federal partners—the FBI; the U.S. Drug Enforcement Administration; the Bureau of Alcohol, Tobacco, Firearms and Explosives; the DHS Federal Air Marshal Service; the California State Board of Equalization;[48] and the U.S. Social Security Administration—in the Los Angeles area to obtain the information needed to develop geographic risk assessments. LAPD has also worked with these federal agencies to develop information needs based on these assessments. However, JRIC (the regional fusion center) has the primary responsibility for the assessments.

Project Recommendations From the Los Angeles Police Department

- A national program office would assist in the nationwide coordination, and local agencies should have heavy involvement.
- There should be a national training program for the SAR process.

[47] All of the regional fusion centers in California are connected to the state fusion center.

[48] The Board of Equalization collects California state sales and use tax, as well as fuel, alcohol, and tobacco taxes and fees that provide revenue for state government and essential funding for counties, cities, and special districts.

- A national users group would be extremely helpful. LAPD received many calls regarding its SAR process from agencies around the country. Having a national users group would assist in reaching out to numerous agencies on a regular basis. The users group should have a strong involvement from local law enforcement agencies.
- There is a need for ongoing technical support.
- There is a need for a national legal office. Given the "new terrain" this project is covering, a legal office could assist with transparency on a national level.
- Agencies need a SAR "ABC Implementation Book" to assist in the implementation of the SAR process.
- There is a need for an inspection/technical assistance team that can assess agencies' current SAR processes and assist with the implementation of a SAR process.
- Every SAR should be treated with the same importance as a crime report to ensure that it receives the attention and proper emphasis needed..

Miami-Dade, Florida, Police Department

SAR Process Report—Post-Implementation Phase

Following the conclusion of the Information Sharing Environment-Suspicious Activity Reporting Evaluation Environment (ISE-SAR EE), a discussion was held with the Miami-Dade Police Department's (MDPD) Homeland Security Bureau (HSB), known as the Miami-Dade Fusion Center (MDFC), to document the implementation efforts conducted during the ISE-SAR EE. The results of the discussion are detailed below.

Executive Leadership

Prior to the ISE-SAR EE, MDPD had no General/Special Order relating to SAR. MDPD had issued a directive on February 27, 2008, regarding the "Handling of Criminal Intelligence." Soon thereafter, another directive was issued on June 28, 2008, regarding "Suspicious Activity Report" (SAR). Subsequent to the directive's issuance, command staff and senior management were briefed on the directive's purpose.

During the ISE-SAR EE, it was decided by command staff that the previously mentioned directives were sufficient to cover the reporting of suspicious activity. Director Robert Parker sent a letter to the Office of the Program Manager for the Information Sharing Environment expressing MDPD's full support of the SAR process and offering MDPD's participation in the Nationwide SAR Initiative (NSI). MDPD command staff is fully aware of the SAR program and the ISE-SAR EE and in February 2009 received the Major Cities Chiefs Association's Chief Executive Officer Briefing, in which 33 command staff personnel from 16 law enforcement agencies participated. As part of the agency's SAR process development, a major was assigned the primary responsibility of implementing the SAR process within MDPD and MDFC.

SAR Business Process

Prior to the ISE-SAR EE, officers' reports were submitted in hard copy to MDPD. If an officer determined that the report included suspicious activity, the report was forwarded to MDFC, which served as the collection point for all SARs within the department. Officers were also encouraged to call MDFC to inform the center of the suspicious activity notated in their reports. MDFC utilized an online form located on the South Florida Virtual Fusion Center[49] to collect SARs from agencies outside the department. Once a report is submitted, it is then assigned to the sector-designated fusion center representative, depending on the information contained in the report. After a SAR is assigned, it is vetted and responded to as appropriate. If the information is found to be reliable, it is posted to the South Florida

[49] The South Florida Virtual Fusion Center is a collaboration site that allows government agencies from the South Florida area to post and share information.

Virtual Fusion Center, and if there is a terrorism nexus, the Joint Terrorism Task Force (JTTF) is notified. If a SAR is deemed to be credible, feedback is provided to the original submitter of the SAR and, depending on the validity of the information, commendations can be issued.

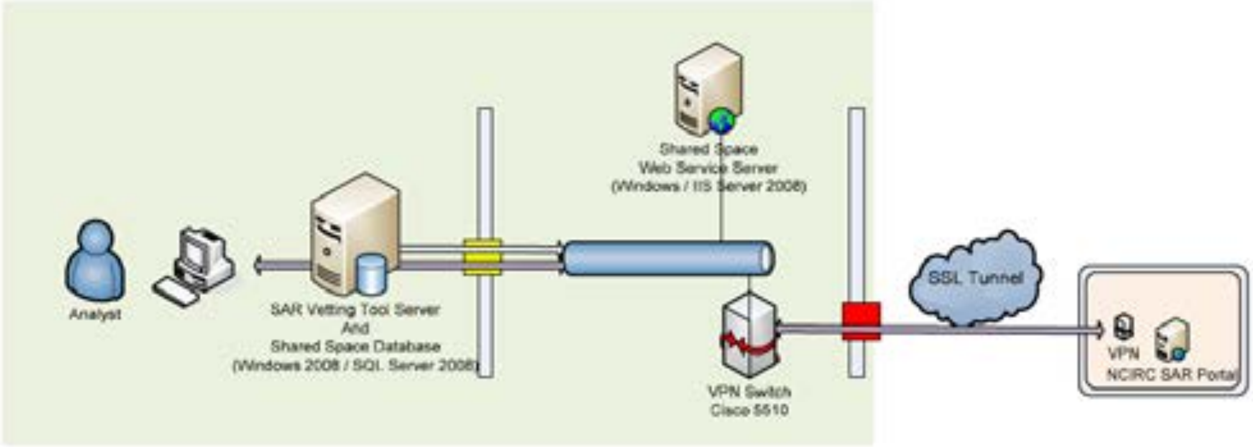
During the ISE-SAR EE, it was decided by MDPD command staff that there would be no changes made to the basic police report. Because MDPD does not have an automated records management system, changing the report would not have affected the SAR collection process. However, the department is working on developing specific radio call signs for suspicious activity. All SARs continue to be forwarded to MDFC, and it has adopted the behavior-specific codes specified in the ISE-SAR Functional Standard. MDFC is utilizing the SAR Vetting Tool (SVT) provided by the NSI to retrieve and analyze SARs.

During the ISE-SAR EE, the center developed a multilayer review and vetting process to identify SARs. Once the initial report is submitted, a field supervisor reviews the report to ensure accuracy and appropriateness of the report. Once it is sent to MDFC, it is immediately reviewed by an analyst and investigative personnel to determine its relationship to terrorism. If the SAR is credible, a detective will deploy to the scene for follow-up. Once the review is complete and analytical value added, the SAR is then reviewed and approved by an MDFC supervisor before entry into the ISE-SAR Shared Spaces. If at any time during the SAR process a report is determined to have an error or incomplete information, the report is immediately dealt with at that time and the submitting agency or officer is notified. All SARs from source agencies are verified, validated, and corroborated. MDFC maintains the same process prior to the ISE-SAR EE for forwarding SARs to local, state, and federal agencies.

During the ISE-SAR EE, MDFC developed and implemented a privacy policy regarding the reporting of suspicious activity that met the applicable requirements of the ISE Privacy Guidelines. In order to protect the information within the ISE-SAR Shared Spaces, it was determined that only personnel within MDFC's Intelligence Operations Center would be allowed access to the SVT and ISE-SAR Shared Spaces. By policy, all queries on the information within the ISE-SAR Shared Spaces is for law enforcement purposes only and must have a criminal nexus.

SAR Technical Process

Prior to the ISE-SAR EE, MDPD did not maintain a database for the collection of SARs. During the ISE-SAR EE, MDPD requested the SVT to augment existing legacy system data and act as a bridge between the legacy system and the Shared Spaces database. The SVT application and database were installed on the ISE-SAR Shared Spaces Server as an economical approach to share hardware and MS-SQL resources. The common architecture is described below.



Training

MDPD conducts numerous training events throughout the greater Miami region; however, no specific training on the SAR process existed before the ISE-SAR EE.

During the ISE-SAR EE, MDPD participated in several SAR training events—including the Chief Executive Officer Briefing, the SAR analyst/investigator course, and agency-developed SAR training. In January 2009, MDPD attended the SAR analyst/investigator course in the Miami area, in which 58 personnel were trained from 26 law enforcement agencies. During a two-month initiative, MDFC provided SAR roll call training to more than 1,100 officers within the department. In addition, MDFC has trained various county government departments—fire, emergency medical services, aviation, and public works—on the process of the SAR program and how to report suspicious activity to the fusion center. It was indicated that the training curriculum is continually revised based upon information that has been analyzed from the gathering of SARs.[50]

Institutionalization of the SAR Process

Prior to the ISE-SAR EE, MDPD had several institutionalization efforts for the SAR process within the department. In addition to the aforementioned directives, line officers received the BJA Pocket Guides for Law Enforcement, and roll call training on terrorism was provided to line officers. County agencies and law enforcement agencies in the region had access to the South Florida Virtual Fusion Center. MDFC is a controlled environment, so it was determined by command staff that no formal audits were needed and qualitative and quantitative measures were made part of the review process. MDFC released alerts, warnings, and notifications as necessary.

During the ISE-SAR EE, MDPD continued its efforts to institutionalize the SAR process throughout the department. The Center has stringent security requirements, and all

[50] For example, training was developed for airport maintenance personnel to look for suspicious activity based upon the analysis of SAR information received.

assigned personnel have received an overview of SOPs, security, and the privacy policy, as well as hard copies of all documents.

Outreach to the Public

Prior to the ISE-SAR EE, MDPD developed *Seven Signs of Terrorism* DVDs and CDs and distributed them to surrounding agencies and private sector entities.[51] The SAR process was presented to community groups and external government stakeholders in the region.

During the ISE-SAR EE, MDPD continued outreach similar to what it was conducting prior to the ISE-SAR EE by continuing to brief community groups; distribute DVDs, bulletins, and brochures to the public; and conduct officer-to-citizen interaction programs. In addition, the Miami-Dade Fusion Center is involved in the joint "Building Communities of Trust" program with the federal government and other local agencies.

Partnering With Other Agencies and Connecting to Information Sharing

Prior to the ISE-SAR EE, MDFC was a U.S. Department of Homeland Security (DHS)-recognized fusion center and has a representative and analyst reports officer from DHS assigned to the center. Additional center personnel include representation from the JTTF; the FBI Field Intelligence Group; Miami-Dade Fire Rescue; the Florida Department of Law Enforcement; the U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives; the Southeast Florida Regional Domestic Security Task Force; Miami-Dade Corrections; the U.S. Transportation Security Administration; and U.S. Immigration and Customs Enforcement. MDFC also partners with surrounding government agencies via the South Florida Virtual Fusion Center.

MDFC can access the Regional Information Sharing Systems Secure Intranet (RISSNET) but does not post information to it to share SAR information. MDFC can also access the state's criminal justice network and intelligence database but does not post intelligence to them. However, information is posted on the Homeland Security Information Network, Law Enforcement Online, and the South Florida Virtual Fusion Center. MDFC is able to send and receive secure e-mail via the Homeland Secure Data Network and has secure communications at the Secret level for fax, phone, and video. It also has an account with the Secret Internet Protocol Router Network.

During the ISE-SAR EE, MDPD continued the previously mentioned partnerships and developed new partnerships by developing a Terrorism Liaison Officer (TLO) program for other public agencies. The mayor, city manager, and county commission have been briefed and are aware of the SAR program and have mandated that agencies work with the TLO

[51] The video is also available on the MDFC Web site at http://www.miamidade.gov/mdpd/BureausDivisions /bureau_Hls.asp.

program. In addition, MDPD has a working relationship with all the major private security operations in South Florida.

Partnering to Develop Geographic Risk Assessments

Prior to the ISE-SAR EE, MDPD worked with the FBI, DHS, the U.S. Department of Defense, and the Bureau of Alcohol, Tobacco, Firearms and Explosives on a continual basis to develop geographic risk assessments. MDFC also works with federal agencies to identify its information needs based on the results of these risk assessments, including assigning two personnel to the FBI's Field Intelligence Group in the development of the risk assessments. It was indicated that most of the assessments in South Florida are conducted by the FBI, and MDPD contributes to the assessments as necessary.

During the ISE-SAR EE, MDPD continued its aforementioned partnerships in the development of information needs and risk assessments.

Project Recommendations From the Miami-Dade Police Department

- There should be a national program to ensure that standards and measurements stay consistent. It should be established so that local agencies have ownership in the sharing of information.
- There is a need for a standard process for the sharing of SAR data from all of the DHS programs.
- There should be a national online training program for ease of delivery nationwide; however, the analyst training should be classroom-based since that is a complicated piece of the project.
- There is a need for a national SAR users group, and the fusion center directors should be involved.
- There must be ongoing technical support for at least three to five years until the systems become stabilized.
- There should be continuous technical assistance support for privacy policies; however, there is no need for a national legal officer for the project.
- It should be understood that the entire privacy policy development is a lengthy and time-consuming process.
- A greater awareness is needed from the local federal special agents in charge concerning the SAR process.
- The NSI needs to stay focused on behaviors and not individuals.

NEW YORK STATE POLICE

SAR PROCESS REPORT—POST-IMPLEMENTATION PHASE

Following the conclusion of the Information Sharing Environment-Suspicious Activity Reporting Evaluation Environment (ISE-SAR EE), a discussion was held with the New York State Police's (NYSP) state-designated fusion center, the New York State Intelligence Center (NYSIC), to document the implementation efforts conducted during the ISE-SAR EE. The results of the discussion are detailed below.

EXECUTIVE LEADERSHIP

Prior to the ISE-SAR EE, NYSP had no specific standard operating procedure (SOP) or General/Special Order relating to the SAR process. However, there is a section in the NYSP Manual under "Article 30D: NYSP Law Enforcement Field Interview Card," on the reporting of suspicious incidents or subjects. The center had also begun implementing a statewide program for the collection of suspicious activity with the creation of Counterterrorism Intelligence Units (CIUs) within each of the troops. No formal training on the SAR process had been conducted for the command staff; however, command officials of NYSP had been briefed on the operations of NYSIC as well as its efforts to obtain and analyze SARs. In addition to the brief, leadership receives daily reports from NYSIC on suspicious activity and has expressed its support of the statewide initiative.

During the ISE-SAR EE, the NYSP command staff, as well as the state's Office of Homeland Security (OHS), was briefed by NYSIC personnel on its efforts in the project. In addition, the center utilized the Major Cities Chiefs Association Chief Executive Officer Briefing to train more than 60 law enforcement officials. As part of the SAR process planning development, a captain was assigned to the project with the primary responsibility to implement a SAR process throughout NYSP, including NYSIC. During the ISE-SAR EE, NYSIC leadership decided that the section on suspicious incidents or subjects in the NYSP Manual was sufficient and no SOP or General Order would be developed.

SAR BUSINESS PROCESS

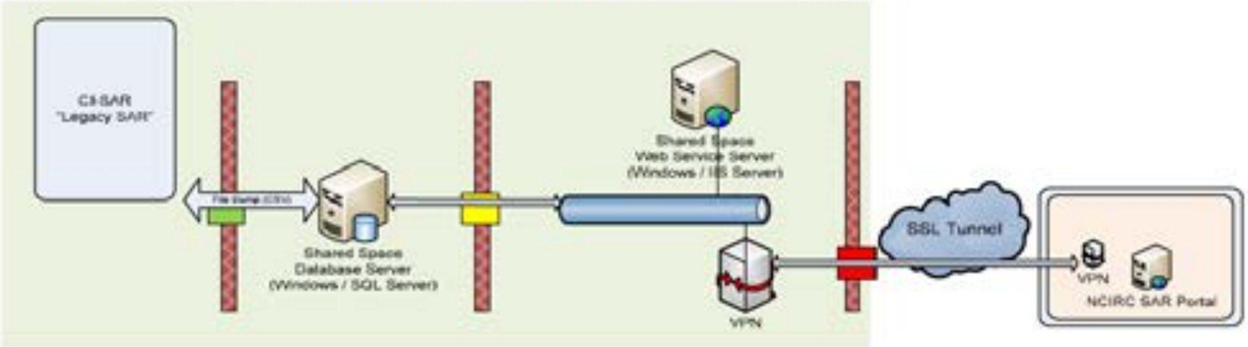
Prior to the ISE-SAR EE, NYSIC had a process in place for gathering and handling SAR information. The center continues to refine its processes and increase the involvement of troopers in the field and other law enforcement agencies in the state. NYSIC also maintains a tip line that gives the public an opportunity to provide information directly to the center. NYSIC includes representatives from the Federal Bureau of Investigation (FBI) and the U.S. Department of Homeland Security (DHS) who assist in the analysis and investigation of SARs. Prior to the ISE-SAR EE, NYSIC was the central collection point for SARs in the state of New York. Once SARs are forwarded to NYSIC, they are reviewed immediately by an analyst to determine whether there is a terrorism nexus and to ensure that an appropriate follow-up investigation is conducted. Additionally, the CIUs assigned in each troop work closely with NYSIC on a variety of intelligence issues, including SARs. The CIUs in each troop work with NYSIC personnel to ensure that all SAR information is forwarded to the center. NYSIC also reviews all field interview cards completed by NYSP troopers to ascertain whether any terrorism-related information is included in the reports.

During the ISE-SAR EE, NYSIC adopted the behavior-specific codes located in the ISE-SAR Functional Standard and developed and implemented a privacy policy regarding the reporting of suspicious activity that meets the applicable requirements of the ISE Privacy Guidelines. In order to protect the information within the ISE-SAR Shared Spaces, it was determined that access to the ISE-SAR Shared Spaces would be limited to command staff and personnel assigned to the Counter Terrorism Center within NYSIC. By policy, all queries on the information within the ISE-SAR Shared Spaces is for law enforcement purposes only and must have a criminal nexus.

It was decided during the project that NYSIC would not modify the current reporting process or the existing offense report, which were in place before the ISE-SAR EE, because both the process and report adequately address the project areas. NYSIC is currently in the process of developing a new intelligence and case management system that will house SAR data. SARs that are currently reported to the center are entered into a tips and leads database, where they receive the initial review by an intelligence analyst. After the analyst reviews the SAR, a supervisor will review and has the final determination to enter the SAR into the ISE-SAR Shared Spaces. If an error is found in the information during any period of the vetting process, it is immediately corrected and the source agency notified. SARs are assigned to the relevant law enforcement agency for follow-up and disposition. All SARs are forwarded to the Joint Terrorism Task Force, which has the first right of refusal to investigate the SAR.

SAR Technical Process

The NYSP and NYSIC are currently engaged in building a new intelligence and case management system to support all fusion center operations. For the ISE-SAR EE effort, they plan to use a critical infrastructure analysis system called CI-SAR as the legacy system. The configuration used is similar to the Virginia Fusion Center solution.



Training

NYSIC conducts numerous terrorism awareness training events throughout the state of New York; however, no specific training on the reporting of suspicious activity existed before the ISE-SAR EE.

During the ISE-SAR EE, NYSP participated in several SAR training events, including the Chief Executive Officer Briefing, the SAR analyst/investigator course, and the line officer training. The line officer training is under development, and NYSIC worked with the International Association of Chiefs of Police during the pilot phase of the training. The analyst/investigator course was conducted in March 2009 and 19 analysts participated. The fusion center indicated that there is a need for follow-up training on internal SAR processes. To address this issue, NYSIC will modify its annual training to incorporate specific examples of activities that can be precursors to terrorism.

Institutionalization of the SAR Process

Prior to the ISE-SAR EE, NYSIC had a very robust program to institutionalize the SAR process throughout the state. NYSIC's existing SAR program is well-developed and provides a process outlining how to receive, review, and analyze suspicious activity information. FBI and DHS representatives are colocated within the center, giving it the ability to conduct additional follow-up investigation and analysis of SAR data. All troopers in the state have been trained in terrorism awareness and are aware of the process for feeding relevant information to NYSIC. The development of a Field Intelligence Officer (FIO) program has been a critical component of the NYSIC SAR process. The FIO program is designed for local agencies so that they have a method of forwarding terrorism and other criminal information to NYSIC. The program is similar to the Terrorism Liaison Officer programs developed in other fusion centers. FIOs are trained in all aspects of intelligence, including privacy/civil liberties concerns and requirements of the Nationwide SAR Initiative. Also important to the institutionalization of the SAR process has been the aforementioned development of CIUs in each of NYSP's troops. These units give NYSIC access to trained individuals in each area of the state to help support statewide intelligence operations. NYSIC also produces alerts, warnings, and notifications that can be sent to law enforcement agencies statewide. In addition, NYSIC works closely with the state's OHS, which has the primary responsibility for distribution of information to the private sector.

During the ISE-SAR EE, NYSIC indicated that it is in the process of developing quantitative and qualitative measures to engage the effectiveness of the SAR process. Currently, it has more quantitative than qualitative data but will develop these evaluation criteria further as the process matures. NYSIC reported that it has trained approximately 1,600 FIOs, which is 85 percent of the state's law enforcement agencies. Currently, its FIO program is focusing on law enforcement and corrections personnel.

Outreach to the Public

In comparison to other ISE-SAR EE sites, NYSIC has a different approach regarding outreach to the public. Before and during the ISE-SAR EE, the OHS has had the primary responsibility for public outreach concerning terrorism-related issues in the state of New York. OHS maintains a public Web site that includes updates concerning terrorism and other awareness information that citizens should be aware of and report to law enforcement.[52] NYSIC supports the operations of OHS and provides information to it that can be made available to the public.

The state utilizes the *Seven Signs of Terrorism* DVD to inform the public of behaviors and suspicious activity that they should report. In addition, NYSIC has a program called "See Something, Say Something" that advises the public on what they should do if they see suspicious activity. The program also explains how to identify suspicious activity.

NYSP also has a program that posts signs on interstate highways and at highway rest stops providing information about terrorism and describing the types of suspicious behavior that citizens should look for. The signs encourage citizens to call the state terrorism tip line if they see something suspicious.

During the ISE-SAR EE, outreach to the public continued through the OHS, with NYSIC providing support to its efforts.

Partnering With Other Agencies and Connecting to Information Sharing

Prior to the ISE-SAR EE, NYSIC had developed strong partnerships and engaged in various forms of information sharing. Members of NYSIC have been leaders in the Northeast Region Fusion Center Group and have worked to develop information sharing protocols among agencies in the region. NYSIC personnel have actively participated in the U.S. Department of Justice's Global Justice Information Sharing Initiative's (Global) Intelligence Working Group as well as Global's Criminal Intelligence Coordinating Council. NYSIC is also developing a Web portal that will provide local law enforcement agencies with an additional opportunity to share information with the center. Additionally, NYSIC shares intelligence electronically with the New York Police Department—the largest metropolitan agency in the state. NYSIC can access the Regional Information Sharing Systems Secure Intranet (RISSNET), Law Enforcement Online, and the Homeland Security Information Network and can send and receive secure e-mail via these secure networks. NYSIC can also access the Federal Protective Service Internet portal and can post intelligence information to the portal to share with other fusion centers.

[52] The New York OHS Web site address is http://www.security.state.ny.us.

During the ISE-SAR EE, NYSIC actively engaged with partners, including the Bureau of Justice Assistance, DHS, the FBI, and OHS in the development of its SAR program. In addition, the Governor's Office was briefed on the goals of the ISE-SAR EE. To ensure communication with public health, NYSIC indicated that two fire officers were assigned to the center and distribute the intelligence products to the emergency medical services and fire communities.

Partnering to Develop Geographic Risk Assessments

Prior to the ISE-SAR EE, the OHS had primary responsibility for the development of risk assessments in the state. NYSIC works closely with OHS to develop the assessments and obtain critical information to analyze and publish as part of the assessments. The colocation of federal law enforcement agencies in the center allows NYSIC to obtain critical federal information to incorporate into the state's assessments. NYSIC works closely with the FBI and DHS to develop priority information needs and is working with them to develop a template for use by fusion centers nationwide to assist in the development of their own priority information needs.

During the ISE-SAR EE, OHS maintained the responsibility of developing geographic risk assessments. Due to this unique circumstance, there has been no additional emphasis placed on this effort. NYSIC continues to work closely with the FBI and DHS to develop priority information needs.

Project Recommendations From the New York State Police

- ➢ Due to the scope of the project, there should be a national program office to assist in the nationwide coordination.
- ➢ To maintain consistency throughout the nation, there should be a national training program; however, every agency is somewhat unique in its training needs.
- ➢ There is a need for a national users group in order to maintain consistency and share lessons learned and issues within the initiative.
- ➢ Due to ongoing changes with information technology systems, there is a need for ongoing technical support to maintain connectivity with the different law enforcement systems.
- ➢ Most of NYSIC's legal issues were at the state level; therefore, there is no need for a national legal office. However, there should be some form of legal assistance available.
- ➢ There is a need for a privacy checklist for analysts to utilize during the initial vetting of the SAR.

Additional Comments

NYSIC personnel indicated that there were no policy, legal, or technical issues that they could not overcome. They suggested that there should be improvements to the search tool for the ISE-SAR Shared Spaces.

SEATTLE, WASHINGTON, POLICE DEPARTMENT

SAR PROCESS REPORT—POST-IMPLEMENTATION PHASE

Following the conclusion of the Information Sharing Environment-Suspicious Activity Reporting Evaluation Environment (ISE-SAR EE), a discussion was held with the Seattle, Washington, Police Department (Seattle PD) to document the implementation efforts conducted during the ISE-SAR EE. The results of the discussion are detailed below.

EXECUTIVE LEADERSHIP

Prior to the ISE-SAR EE, Seattle PD had no General/Special Order regarding SARs. However, Seattle PD had worked closely with the Major Cities Chiefs Association (MCCA) to enhance its current SAR process. Command staff and senior management have been briefed on the Nationwide SAR Initiative (NSI) and support the department's efforts. Additionally, Chief Gil Kerlikowski had served as the President of MCCA, which helped organize the SAR effort among law enforcement agencies in the country's major cities.

During the ISE-SAR EE, Seattle PD worked closely with the Washington State Fusion Center (WSFC) and the local office of the Federal Bureau of Investigation (FBI), which both strongly support the effort to enhance the SAR process among the agencies and the participation of Seattle PD in the initiative. The command staff is fully aware of the SAR program and the ISE-SAR EE and in May 2009 received the MCCA's Chief Executive Officer Briefing, in which 31 command staff personnel from approximately 18 law enforcement agencies participated. During the ISE-SAR EE, the command staff decided that existing policies were sufficient and general enough to cover the reporting of suspicious activity, so a new General Order was not necessary. A deputy chief from the Criminal Intelligence Bureau (CIB) was assigned to the SAR process development project; the primary responsibility of the deputy chief was to implement a SAR process at Seattle PD.

SAR BUSINESS PROCESS

Prior to the ISE-SAR EE, Seattle PD indicated that the department had a process for gathering and handling suspicious information, and it continues to refine this process and increase involvement from line officers and other law enforcement agencies in the area. Seattle PD provides all of its collected suspicious activity information to WSFC. WSFC is colocated with the FBI's Joint Terrorism Task Force to facilitate effective SAR information sharing with both federal and state agencies.

Seattle PD utilizes information reports, field interview reports, and other reporting mechanisms in its SAR process. Officer reports are entered into the department's records management system (RMS). From there, terrorism-related reports are forwarded to CIB, where the reports are printed for review and vetting by CIB personnel. All reports that are determined to be terrorism-related are then "hand-carried" to WSFC for further review.

Prior to the ISE-SAR EE, Seattle PD's SAR process was not formalized and the department did not assign behavior codes to SARs. Once the reports are received by WSFC, they are reviewed and vetted by WSFC analysts along with FBI and U.S. Department of Homeland Security (DHS) personnel.

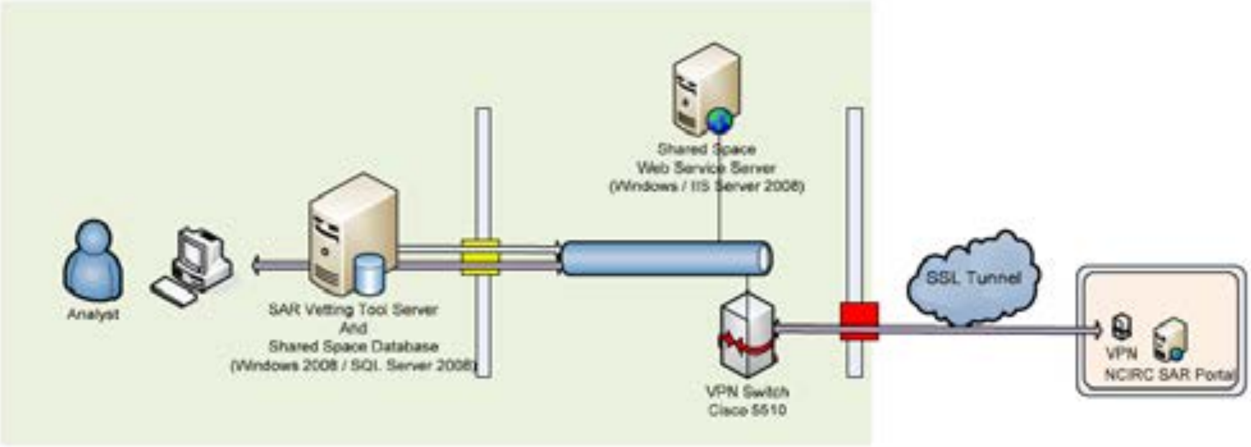
During the ISE-SAR EE, the agency continued to use the same reporting mechanisms that were used prior to the ISE-SAR EE. However, Seattle PD adopted the behavior-specific codes illustrated in the ISE-SAR Functional Standard and developed and implemented a privacy policy regarding the reporting of suspicious activity that meets the applicable requirements of the ISE Privacy Guidelines. In order to protect the information within the ISE-SAR Shared Spaces, it was determined that access to the ISE-SAR Shared Spaces would be limited to command staff and personnel assigned to the fusion center. By policy, all queries on the information within the ISE-SAR Shared Spaces is for law enforcement purposes only and must have a criminal nexus. If SAR information is identified as having an error, the fusion center has an affirmative responsibility to notify in writing the source agency.

During the ISE-SAR EE, a multilayer review process was established to identify ISE-SARs within 24 hours. SARs that are submitted to Seattle PD are reviewed by CIB and then sent to WSFC for review and analysis. Once the fusion center determines that the information has a nexus to terrorism, the ISE-SAR is entered into the ISE-SAR Shared Spaces. During this review process, SARs are assigned to an investigator, and the disposition is tracked utilizing the Fusion Core Solutions application.

SAR Technical Process

Prior to the ISE-SAR EE, the initial information concerning suspicious activity at Seattle PD was reported by officers in either the RMS, if a Seattle PD officer writes an information report, or in a field interview report, if the officer conducts a field interview; CIB can then retrieve the information for analysis. The information in the RMS is not maintained in a manner that allows the information to be exported to the ISE-SAR Shared Spaces. Seattle PD tracks all SARs received by CIB in a spreadsheet. Additionally, the Washington Joint Analytical Center (WAJAC) enters all statewide SAR data received into an agency-developed database and also enters SARs into the FBI's classified eGuardian system.

During the ISE-SAR EE, it was decided by Seattle PD and WSFC that the servers for the ISE-SAR Shared Spaces would be housed at WSFC. Seattle PD and WSFC requested the SAR Vetting Tool (SVT) to augment existing legacy system data and act as a bridge between the legacy system and the Shared Spaces database. The SVT application and database were installed on the ISE-SAR Shared Spaces Server as an economical approach to share hardware and MS-SQL resources. The common architecture is described below.



Training

Prior to the ISE-SAR EE, Seattle PD trained all of its officers on suspicious activity relating to terrorism and terrorism awareness. Once the agency's privacy policy is in place, tenets of the policy will be included in officer in-service training.

During the ISE-SAR EE, Seattle PD participated in the Chief Executive Officer Briefing and the analyst/investigator course. During the SAR analyst/investigator course in the Seattle area in May 2009, 23 personnel were trained from 12 law enforcement agencies. In addition, officers have been sent bulletins explaining the SAR program and the need for information to be sent to CIB. The Seattle PD plans to utilize the line officer training once it is made available nationwide.

Institutionalization of the SAR Process

Prior to the ISE-SAR EE, Seattle PD institutionalized a well-developed program to receive, review, and analyze SAR data. Representatives from the FBI and DHS are colocated with the state fusion center, giving Seattle PD and WSFC the ability to conduct additional follow-up investigation and analysis. All officers in the city of Seattle have been trained in terrorism awareness and are aware of the process for feeding information to WSFC.

Prior to the ISE-SAR EE, Seattle PD did not have a Terrorism Liaison Officer (TLO) program, although they work closely with law enforcement agencies in the area to share information and intelligence. Seattle PD is also working on the development of a private sector SAR process utilizing the FBI's InfraGard system. Seattle PD produces alerts, warnings, and notifications that are sent to the department's officers and command staff, as well as area law enforcement agencies. The department also coordinates with WSFC in the production of Intelligence and Information Bulletins to distribute statewide. It was noted that all intelligence functions of Seattle PD are the subject of an annual audit by the Office of the Chief of Police. In addition, provisions are in place for regular outside audits of all intelligence and information systems within Seattle PD.

During the ISE-SAR EE, Seattle PD continued the previously mentioned institutionalization efforts throughout the department. Currently, the department is working to develop a TLO program within government agencies in the Seattle area. In addition, Seattle PD incorporated the SAR data into the development of alerts, warnings, and notifications.

Outreach to the Public

Prior to and during the ISE-SAR EE, Seattle PD developed several informational materials for the public. The city of Seattle's Office of Emergency Management has the responsibility of providing the public with information concerning terrorism,[53] and Seattle PD supports those efforts. Seattle PD also supports the Northwest Warning, Alert and Response Network (NW WARN), which is an e-mail alert system developed to inform the public. NW WARN is a collaborative effort between government and private sector partners within different regions of the state. The goal of NW WARN is to maximize real-time sharing of situational information without delay and provide immediate distribution of intelligence to those in the field who need to act on it. NW WARN uses readily available communication methods to rapidly disseminate actionable information between members. Additionally, Seattle PD is planning on participating in the Communities of Trust Program.

Partnering With Other Agencies and Connecting to Information Sharing

Prior to the ISE-SAR EE, personnel from Seattle PD were involved in the U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative's (Global) Intelligence Working Group and Global's Criminal Intelligence Coordinating Council. In addition to participating in WSFC, Seattle PD participates in other regional information and intelligence organizations. Seattle PD has developed an outreach program to the fire services and has utilized the DHS/DOJ Fusion Process Technical Assistance Program and Services to develop its outreach program.

Prior to and during the ISE-SAR EE, Seattle PD accessed the Regional Information Sharing Systems Secure Intranet (RISSNET), Law Enforcement Online, and the Homeland Security Information Network and can send and receive secure e-mail via these secure networks. The department has actively engaged with NSI partners in the development of its SAR program and works closely with the state's Emergency Management Division and the city's Office of Emergency Management to develop partnerships with other government agencies and the private sector.

Partnering to Develop Geographic Risk Assessments

Prior to the ISE-SAR EE, Seattle PD was working with WSFC and the colocated FBI office to develop its information needs based on the results of risk assessments. WAJAC and the FBI

[53] The link to the Seattle Emergency Management public Web site is http://www.seattle.gov/emergency/hazards/terrorism.htm.

jointly develop risk assessments according to local needs and are working on assessments for the Olympics and developing an Olympic Intelligence Coordination Center in Bellingham, Washington.

During the ISE-SAR EE, Seattle PD continued the previously mentioned efforts in the development of geographic risk assessments.

Project Recommendations From the Seattle Police Department

- There is a need for a national program office—not necessarily a federal office—with joint operation by local, state, and federal agencies. The office needs to look at the all-crimes approach to SARs and recommend that the deputy directors of a national program office be state and local officials.
- There is a need for a national training program to maintain consistency with the initiative.
- The analyst training should include scenarios so that everyone is doing the same type of analysis. A checklist for analysts would be very helpful when they are reviewing any potential terrorism-related SARs.
- There is a need for a national user group for the initiative; however, the group should have a well-defined function within the NSI.
- There is a need for continued initial implementation, research, development, and technical assistance as it relates to technology throughout the NSI.
- There is no need for a national legal officer, but perhaps access to legal advice. The legal needs are at the local level.
- There is a need for this project to be more than just terrorism-related SARs and should expand to all crimes.

VIRGINIA STATE POLICE

SAR PROCESS REPORT—POST-IMPLEMENTATION PHASE

Following the conclusion of the Information Sharing Environment-Suspicious Activity Reporting Evaluation Environment (ISE-SAR EE), a discussion was held with the Virginia State Police's (VSP) state-designated Virginia Fusion Center (VFC) to document the implementation efforts conducted during the ISE-SAR EE. The results of the discussion are detailed below.

EXECUTIVE LEADERSHIP

Prior to the ISE-SAR EE, VSP had no specific General/Special Order relating to SAR; however, during the ISE-SAR EE, VSP developed Information Bulletin—2009—No. 35 that explained suspicious activity reporting procedures. No specific command staff training on the SAR process existed before the project.

During the ISE-SAR EE, the command staff was given details on the projects, and the Fusion Center Advisory Board was briefed on the ISE-SAR EE. The superintendent released the aforementioned information bulletin regarding suspicious activity reporting procedures. In addition, VSP utilized the Major Cities Chiefs Association's Chief Executive Officer Briefing to train command staff personnel throughout the state. As part of the SAR process planning development, a VSP lieutenant and first sergeant were assigned to the project; the primary responsibility of the lieutenant and first sergeant is to implement a SAR process throughout VSP, including VFC.

SAR BUSINESS PROCESS

Prior to the ISE-SAR EE, VFC had a process for the reporting of suspicious activity. VFC was designated as the intake point for the collection and receipt of all SARs within VSP. SARs are processed internally within VSP by submitting[54] an intelligence report to the center; externally, the public or other law enforcement agencies can file a Suspicious Incident Report via the VFC Web site.[55] An intelligence report filed with VFC receives an initial vetting within 24 hours. When a report is submitted, the watch center within VFC documents what has occurred with the SAR and provides additional analytical value at the time of initial vetting. The report is then sent back to the original submitter as well as other agencies that may have a need for the information. Field Intelligence Officers in the regions have the responsibility of updating the disposition of the intelligence reports. All SARs with a Northern Virginia nexus are sent to the National Capitol Region Intelligence Center as well as the Joint Terrorism Task Force. VFC works closely with all local jurisdictions to share SAR information

[54] Intelligence reports are sent to VFC via Email, telephone and the VSP website.
[55] The Web site is located at http://www.vsp.state.va.us/FusionCenter/index.shtm.

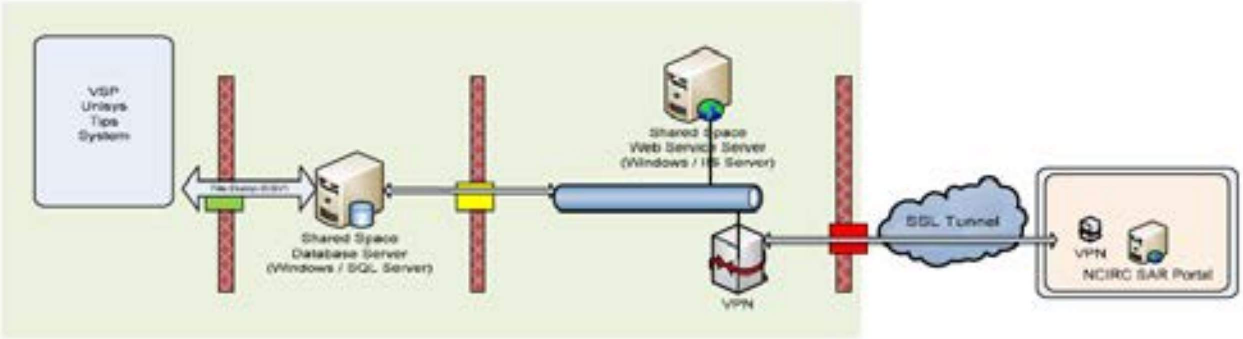
throughout Virginia and the National Capital Region Intelligence Center located in Fairfax, Virginia, as well as jurisdictions in Washington, DC, and the Maryland area.

Because of its robust SAR process prior to the ISE-SAR EE, VSP had only minor enhancements to its SAR process as it implemented this project. The center adopted and modified its current report to comply with the behavior-specific codes located in the ISE-SAR Functional Standard; however, not all codes are being utilized in the current system because of records management system (RMS) limitations. In addition, the center modified its RMS to add check boxes to indicate the data is a SAR; this function allows the RMS to be searched for SAR information. Lastly, VFC developed a multilayer review for vetting SARs. Information that comes into the watch center is analyzed within 24 hours, and if it meets the criteria for an ISE-SAR, it is then sent to a supervisor for review. Once approved by the supervisor, the SAR is then entered into the ISE-SAR Shared Spaces. All SARs that meet these requirements are also sent to the Federal Bureau of Investigation (FBI), DHS, affected VSP personnel, and affected local jurisdictions.

During the ISE-SAR EE, VFC developed and implemented a privacy policy regarding the reporting of suspicious activity that met the applicable requirements of the ISE Privacy Guidelines. In order to protect the information within the ISE-SAR Shared Spaces, it was determined that only trained fusion center personnel would be allowed access to the ISE-SAR Shared Spaces. By policy, all queries on the information within the ISE-SAR Shared Spaces is for law enforcement purposes only and must have a criminal nexus. During the vetting process, if an error in the information is identified, the reporting agency is notified and the error is corrected.

SAR Technical Process

VFC relies upon an aging mainframe to process SARs received and/or generated by VSP, partner organizations, and/or VFC analysts. The VFC information technology staff modified the system to identify SARs for submission to the ISE-SAR Shared Spaces. Periodically, a file download routine on the mainframe would pull designated SARs for processing by an extraction, transformation, and load process on the ISE-SAR Shared Spaces Server and update the ISE-SAR Shared Spaces database. The installation in Virginia is depicted below.



TRAINING

VFC conducts numerous terrorism awareness training events throughout the state of Virginia and provided SAR specific training on the reporting of suspicious activity before the ISE-SAR EE.

During the ISE-SAR EE, VFC participated in several SAR training events, including the Chief Executive Officer Briefing, the SAR analyst/investigator course, and the line officer training.[56] The analyst/investigator training was conducted in April 2009 and had 49 analysts participate. The superintendent's Information Bulletin regarding the reporting of suspicious activity was distributed to all employees within VSP, and once available, VSP plans to follow up the release of the bulletin with the online version of the line officer training to train all sworn personnel on the SAR process. VFC indicated that there is no formal review process for modifying or enhancing the existing SAR training program based on emerging trends and patterns; however, the center is considering implementing this type of enhancement.

INSTITUTIONALIZATION OF THE SAR PROCESS

Prior to the ISE-SAR EE, VFC had taken steps to begin institutionalizing the SAR process agency-wide. VFC continues to build relationships with its fusion center partners. To further enhance the process of gathering suspicious activity, a Fusion Liaison Officer (FLO) program has been developed within VSP. The first phase of this program is to concentrate on training one officer in each of the state's seven regions to serve as the FLO. Once this phase is complete, the center will expand the program and train other fusion partners, such as first responders, health agencies, and government agencies.

VFC created information requirements based on priority information needs for emerging trends and behaviors, and the center will modify the SAR process based on these needs. The SAR process is incorporated into the current alerts, warnings, and notification process, and information is distributed via e-mail or through the Homeland Security Information Network (HSIN) to VSP and other fusion center partners. Also, VFC works with the DHS to satisfy the center's information needs requirements and is developing collection plans that address these needs.

During the ISE-SAR EE, VFC continued with the implementation of its FLO program. VFC indicated that it is in the process of developing quantitative and qualitative measures to gauge the effectiveness of the SAR process, as well as an audit process. The center has decided to utilize the behavior-specific codes described in the ISE-SAR Functional Standard as the basis for collection of information.

[56] The line officer training is under development, and VFC worked with the IACP during the pilot phase of the training.

Outreach to the Public

Prior to the ISE-SAR EE, VSP and VFC had instituted numerous outreach initiatives that include the need for the public to submit suspicious activity to the center. Personnel from the agency continuously attend and present at public forums regarding how the public can report suspicious activity. VFC developed the *Seven Signs of Terrorism* video, which is available to view on the VSP Web site.[57] In addition to the video, VFC has a toll-free Terrorism Hotline, available at (877) 4VA-TIPS, that citizens can call to report suspicious activity.

During the ISE-SAR EE, VFC utilized and distributed the *Safeguarding America—It All Starts With You* DVD to assist the public in identifying the types of suspicious activity. In addition, VFC continued to promote its Web site, where citizens may review information concerning terrorism as well as report suspicious activity to the fusion center.

Partnering With Other Agencies and Connecting to Information Sharing

Prior to the ISE-SAR EE, VFC worked closely with the U.S. Department of Homeland Security (DHS), the FBI, and local jurisdictions to share information throughout the state. The center has developed partnerships with public safety personnel and has five analysts from the public safety/emergency management sector and one fire programs analyst in the center, as well as a U.S. Postal Inspector. VFC has a strong relationship with the U.S. Department of Defense and has established many military points of contact. Additionally, one U.S. Army National Guard representative is assigned to the center. VSP is also a member of a number of professional working groups throughout Virginia and the Southeast, including the Virginia Information Sharing Working Group (VISWG), which includes information sharing partners from agriculture, health, power, and electric. VISWG conducts periodic meetings, where it shares information that is "for official use only." In addition to VISWG, VSP is also a member of Southern Shield, an information sharing group that has members throughout the southeastern United States.

VFC can access the Regional Information Sharing Systems Secure Intranet (RISSNET), Law Enforcement Online, HSIN, and the Homeland Security State and Local Intelligence Community of Interest and has the ability to send and receive secure e-mail through all of these sites. VSP maintains the Virginia Criminal Information Network and has access to the Virginia Law Enforcement Information Exchange and the FBI's Law Enforcement National Data Exchange. Although the current VSP information technology systems are not National Information Exchange Model (NIEM)-compatible, the systems being developed will be able to share data with fusion partners in the NIEM format.

Because of its robust partnerships prior to the ISE-SAR EE, during the project, the center had only a few additional SAR-related efforts with fusion center partners. The center conducted

[57] The *Sevens Signs of Terrorism* is available at http://www.vsp.state.va.us/FusionCenter/7-Signs.shtm.

SAR presentations with local agencies and has provided SAR training materials to its public safety and private partners. Letters were also sent to all chiefs and sheriffs in the commonwealth of Virginia expressing the importance of and providing information on privacy issues and concerns. In addition, VSP prepares an annual report to the Governor's Office, and the next report will include information about the SAR process.

Partnering to Develop Geographic Risk Assessments

VFC has worked with DHS and the FBI in the development of geographic risk assessments. VFC also worked with numerous local, state, and other federal agencies, as well as state and urban fusion centers, to develop risk assessments. An example is the recent work with the Washington, DC, Metropolitan Police Department to develop risk assessments for the 2008 election year and the 2009 Presidential Inauguration. During that time, VFC identified intelligence gaps and provided this information to DHS and the FBI as well as to its fusion partners. In addition, VFC releases an Annual Threat Assessment to convey potential terrorism threats affecting the commonwealth of Virginia.

Although VSP and VFC have a process for developing geographic risk assessments with numerous local, state, and federal agencies prior to the ISE-SAR EE, during the ISE-SAR EE there has been no additional emphasis placed on this effort.

Project Recommendations From the Virginia State Police

- There is a need to coordinate with federal partners for consistency nationwide; however, the initiative focuses on state and local agency issues, so there is no need for a national program office.
- There is a need for a train-the-trainer program for the states to help integrate the SAR process into local agencies.
- Elements of the Chief Executive Officer Briefing and the line officer training should be combined to ensure that a consistent message is being delivered to both audiences.
- There is a need for a SAR national users group similar to the DHS Office of Intelligence and Analysis/Homeland Security State and Local Intelligence Community of Interest because of changing behaviors, indicators, and techniques.
- There is a need for ongoing technical assistance because agencies are constantly changing and updating systems.
- Legal issues are more associated at the state and local levels, so there does not need to be a national legal office; however, there needs to be "one voice" from the federal government regarding legal matters.

- All training should be provided within a one-week period, followed by a project meeting with all of the individuals trained. The close proximity of the training would allow for the SAR processes to be implemented in a more timely manner and will assist with providing a consistent method throughout the agency.

Washington, DC, Metropolitan Police Department

SAR Process Report—Post-Implementation Phase

Following the conclusion of the Information Sharing Environment-Suspicious Activity Reporting Evaluation Environment (ISE-SAR EE), a discussion was held with the Washington, DC, Metropolitan Police Department's (MPD) Washington Regional Threat and Analysis Center (WRTAC) to document the implementation efforts conducted during the ISE-SAR EE. The results of the discussion are detailed below.

Executive Leadership

Prior to the ISE-SAR EE, MPD had no General/Special Order relating to suspicious activity reporting; however, Chief of Police Cathy Lanier expressed her full support of the development and implementation of a SAR process. A General Order was in the planning stages, and once complete, Chief Lanier planned to brief her agency and surrounding agencies on MPD's involvement in the ISE-SAR EE.

During the ISE-SAR EE, the department received the initial Major Cities Chiefs Association's Chief Executive Officer Briefing (CEOB) held in December 2008, which included 51 participants from 29 law enforcement agencies. Chief Lanier released the General Order, GO-HSC-802.06, titled "Suspicious Activity Reporting Program," on January 16, 2009. The order was promulgated agency-wide, and personnel were required to review and sign off on the policy. Chief Lanier briefed MPD command staff and members of the White House staff on MPD's development of a SAR process and its involvement in the ISE-SAR EE. As part of the agency's SAR process development, the Assistant Chief of Homeland Security was assigned the overall responsibility of implementing a SAR process within MPD.

SAR Business Process

Prior to the ISE-SAR EE, WRTAC staff indicated that they had been working with the Los Angeles, California, Police Department (LAPD) to develop a SAR process within WRTAC and MPD. To simplify the suspicious activity reporting process, MPD created a Web-based Terrorist Incident Prevention Program (TIPP) form that gave the public a method of reporting suspicious activity. The TIPP form can also be accessed by line officers, Fusion Liaison Officers (FLOs), and investigators. SARs can also be initiated whenever crime or incident reports in the field are tagged as involving suspicious activity; this cataloging occurs when a box on the report labeled "Suspicious Activity" is checked. As TIPP forms and crime/incident reports are reported to MPD and identified as suspicious, they are immediately forwarded to the Intelligence Fusion Division (IFD) for review and analysis by a trained analyst. This process allows for a centralized location for the collection and receipt of SARs within the agency. Once information is submitted into the TIPP system, an e-mail is generated back to the original submitter acknowledging its receipt.

It was indicated that once SARs are reported, they are maintained in MPD's records management system. SAR data is also entered into a central repository[58] and reviewed by a trained SAR analyst at WRTAC within 24 hours of receipt. Once a SAR is contained in the central repository and deemed terrorism-related, an analyst assigns a code to the SAR prior to its entry into the ISE-SAR Shared Spaces. If a SAR needs further analysis, it is then forwarded to the Investigations Division. To determine the disposition of SARs, IFD provides MPD with a tracking sheet for the TIPP database to track the disposition. There is no retention time for SARs, but if a piece of information rises to the level of reasonable suspicion, it is then moved to an intelligence database.

MPD was also in the process of automating its PD-76 form to provide non-MPD officers with an additional means to report suspicious activity to the department. Automating the form will provide other law enforcement agencies with a simple and efficient mechanism for reporting suspicious activity to WRTAC.

During the ISE-SAR EE, MPD adopted the behavior-specific codes identified in the ISE-SAR Functional Standard and developed a multilayer review process for reviewing SARs and moving them to the ISE-SAR Shared Spaces. When SARs are submitted to WRTAC, they receive an initial review from the "SAR Czar," who is experienced and trained in identifying terrorism indicators. WRTAC controls SAR data but is not an investigative unit, and the "SAR Czar" has the responsibility of determining the disposition and follow-up of the SARs coming into the center. The MPD has an all-crimes approach to SARs coming into the center. SARs are reviewed to determine the appropriate crime category, and then information is sent to the appropriate entity for follow-up. If at any time an error is detected during the review process, the source agency or individual is contacted and the information is corrected.

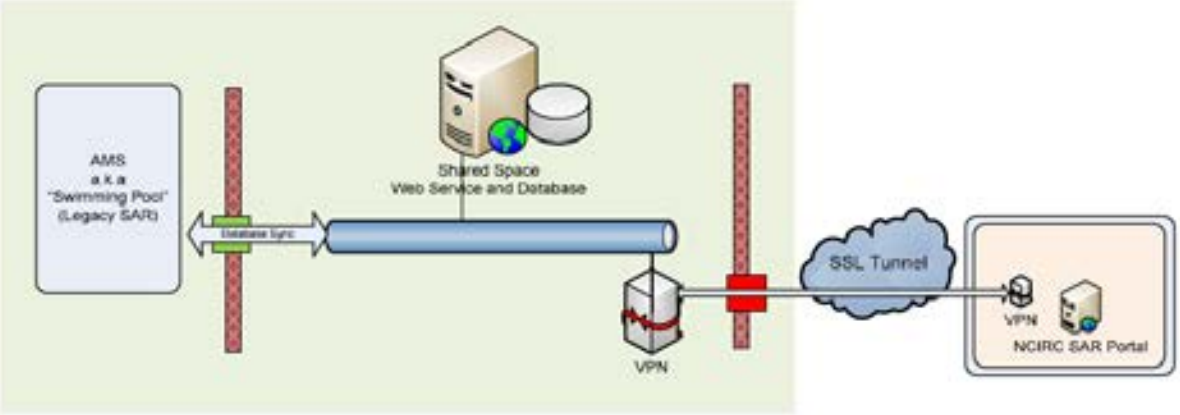
During the ISE-SAR EE, MPD developed a privacy and civil liberties policy regarding the SAR process. WRTAC command staff determined that there will be limited access to the ISE-SAR Shared Spaces to ensure accountability, and by policy, all querying of SAR information must have a criminal nexus and be for legitimate law enforcement purposes.

SAR Technical Process

MPD had embarked upon development of an Alert Management System (AMS) to provide overall records management capabilities at WRTAC. In 2008, with the pending Presidential Inauguration, a decision was made to create a separate module on the AMS to support the collection and vetting of SARs. Similar to the Florida Department of Law Enforcement, the AMS pushed candidate SARs to a staging area on the ISE-SAR Shared Spaces Server, where

[58] The MPD central repository is also referred to as the "swimming pool."

they can be processed via extracting, transforming, and loading routines and stored in the ISE-SAR Shared Spaces repository. The deployment at MPD differs from the other sites in colocating the Web and database servers on the same machine. This is depicted in the following illustration.



Training

Prior to the ISE-SAR EE, MPD and WRTAC were participating in a number of training efforts throughout the agency. MPD was working on lesson plans for the implementation of the TIPP system within the department and would modify the training curriculum based on the analysis of SAR data, if needed. It was indicated that once the SAR process is fully implemented within the agency, MPD will enhance its training based on emerging trends, lessons learned, and identified gaps.

During the ISE-SAR EE, MPD participated in the CEOB,[59] the SAR analyst/investigator course, and the line officer training. The SAR analyst/investigator course was delivered in December 2008, and 15 individuals from 6 agencies received the training in the Washington, DC, area. The line officer training was conducted during roll call in December 2008. An estimated 3,840 officers received training on the SAR process and the behaviors associated with terrorist activity.

Institutionalization of the SAR Process

Prior to the ISE-SAR EE, MPD was in the beginning stage of developing a formalized SAR process and institutionalization efforts were starting to emerge. During the ISE-SAR EE, IFD developed a plan to conduct annual audits to ensure the validity of the SAR process to determine whether improvements will need to be made. Further, MPD worked with the U.S. Department of Homeland Security (DHS) to establish a FLO program with public safety, public health, and private sector entities within its jurisdiction. The goal of the FLO program will be to ensure that multiple disciplines participate in the SAR process and can serve as

[59] The CEOB was previously discussed in the Executive Leadership section.

the conduit through which homeland security-related information can flow from outside agencies to the fusion center for assessment and analysis.

During the ISE-SAR EE, WRTAC planned to evaluate and potentially modify its SAR process based on priority information needs. IFD had recently identified the information needs of different departments within the agency and established collection requirements based on these needs. An IFD member was assigned to monitor collection requirements for each of the department's districts. IFD also utilized "Temperature Boards" in the district offices to display emerging trends and behaviors for the line officers within those district offices.

Outreach to the Public

MPD and WRTAC understand the importance of educating the community on the SAR process to ensure transparency and to obtain the community's support and input. Chief Lanier planned to make a formal announcement regarding MPD's involvement in the SAR process, and IFD will work with the agency's public information office to develop additional outreach efforts.

During the ISE-SAR EE, MPD conducted robust outreach efforts to ensure that the community was aware of the SAR process. MPD has worked with several hotels to help them understand how to report suspicious activity. It has utilized billboards on buses to explain how to report suspicious activity and continues to send out SAR tip information to critical infrastructure and key resources facilities so they understand how to recognize and report suspicious activity. In addition, MPD conducted a Homeland Security Emergency Management seminar, which was a public and private sector event that attracted approximately 100 people. During the seminar, representatives discussed how to recognize and report suspicious activity. Currently, MPD is taking steps to develop an iWATCH program similar to the Los Angeles, California, Police Department and is in the process of securing a domain name for this program.

Partnering With Other Agencies and Connecting to Information Sharing

Prior to the ISE-SAR EE, it was noted that WRTAC had a strong relationship with DHS and the JTTF; a DHS representative and five JTTF representatives were located in IFD. IFD staff members were in the process of obtaining Law Enforcement Online (LEO) and Homeland Security Information Network-Intel (HSIN) accounts. WRTAC could also access the state of Virginia's criminal justice network and had the ability to share information with Virginia and the surrounding region. IFD had a secure site from which it could send and receive information and had two Homeland Secure Data Network terminals to send secure e-mails. MPD was also working with the IJIS Institute to develop the necessary technology to become NIEM-compliant. In continuing efforts to collaborate and share SAR data with nationwide partners such as fusion centers, homeland security officials, and the JTTF, MPD plans to utilize the ISE-SAR Shared Spaces.

During the ISE-SAR EE, MPD continued its previous partnership efforts and worked to establish additional partnerships. WRTAC reported that 96 agency heads in the National Capitol Region as well as the city administrator were briefed on MPD's SAR process and involvement in the ISE-SAR EE. WRTAC has fire and health officials located inside the center and indicated that they are responsible for conducting their own outreach to their respective sectors. Since the inception of the ISE-SAR EE, WRTAC has established accounts with the secure law enforcement networks LEO and HSIN.

Partnering to Develop Geographic Risk Assessments

During the final site assessment, it was indicated that MPD is currently finalizing a department threat assessment. This assessment will focus on the 18 sectors that are handled by WRTAC (transportation, criminal, nuclear, etc.). For major events in the DC Metro area, WRTAC works with a special events working group made up of local, state, and federal agencies to develop assessments. The department works with DHS and the Federal Bureau of Investigation to develop information needs based on the results of the risk assessments it receives or participates in.

Project Recommendations From the Metropolitan Police Department

- There is a coordination element to this effort that needs to exist; however, WRTAC is unsure whether a national program office is needed.
- There is a need for consistent training nationwide that focuses on the behaviors and indicators which terrorists exhibit.
- There is a need for a national users group that is made up of fusion center representatives at the state and local levels.
- There is a need for ongoing technical support for this project.
- Although privacy and civil liberties protections are important parts of this project, WRTAC is unsure whether a separate national legal office for this project is needed.

QUESTIONS

FOR QUESTIONS REGARDING THE ISE-SAR EVALUATION ENVIRONMENT PROJECT, CONTACT:

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

Mr. David Lewis
Senior Policy Advisor
Information Technology Office, Policy Division
Bureau of Justice Assistance
U.S. Department of Justice
03 [redacted]
03 [redacted]

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

Note: This is a non-exhaustive list for Background Purposes

Review of Advocate Websites for Concerns and Issues on ISE-related Activities

1. Review of websites of proposed P/CL and open government advocate groups to identify concerns and positions on ISE-related activities for discussion during engagement meetings.

   a. American Civil Liberties Union (ACLU) – Mike German

   - **ACLU Lawsuit Seeks Information from FBI on Nationwide System for Collecting "Suspicious System May be Used to Track and Store Information about Innocent Americans with No Evidence of Wrongdoing (**"The American Civil Liberties Union [in August 2011] filed a Freedom of Information Act (FOIA) lawsuit challenging the government's failure to release documents about the FBI's nationwide system of collecting and sharing so-called "Suspicious Activity Reports" from local, state and federal law enforcement agencies….The public needs to know if the government is collecting information for eGuardian through the illegal profiling of innocent Americans on the basis of their race, religion or constitutionally protected beliefs and activities.") http://www.aclu.org/free-speech-technology-and-liberty/aclu-v-united-states-department-justice-complaint-injunctive

   - We encourage greater oversight and transparency in the ISE SAR program to ensure these [ISE-SAR FS version 1.5]are being met and maintained. http://www.aclu.org/spy-files/more-about-suspicious-activity-reporting

   - Rather than tightening SAR collection standards, however, many federal, state and local law enforcement agencies are expanding them by encouraging not just police but the general public to report suspicious activity…. And none of these new SAR programs have the same limiting language that was added to the ISE functional standard, making it far more likely that both the police and the public will continue over-reporting the commonplace behavior of their neighbors. http://www.aclu.org/spy-files/more-about-suspicious-activity-reporting

   - Photographers appear to be the most frequent targets of SAR and SAR-like information collection efforts. Whether lawfully photographing scenic railroad stations, government-commissioned art displays outside federal buildings or national landmarks, citizens, artists and journalists have been systematically harassed or detained by federal, state, and local law enforcement. In some instances, the ensuing confrontation with police escalates to the point where the photographer is arrested and their photos erased or cameras confiscated with no reasonable indication that criminal activity is involved. A Los Angeles Sheriff's Deputy even threatened to put a subway photographer on the Terrorist Watchlist. http://www.aclu.org/spy-files/more-about-suspicious-activity-reporting .... There is also evidence that some law enforcement officers are using SAR or SAR-like criteria to abuse their power. Many SAR programs describe photography of security personnel or facilities as a precursor to terrorism and a growing number of cases, such as those in Maryland, Washington, Tennessee, New Jersey, Boston, and Miami, involve police harassment, demands for identification, and even arrests of photographers for taking pictures or video documenting law enforcement officers in the performance of their duties. None of these incidents involved any reasonable links to terrorism or other threats to security. SAR criteria have also been used as a pretext for local law enforcement to check immigration status, and played a precipitating role the arrest of a political activist in Connecticut. http://www.aclu.org/spy-files/more-about-suspicious-activity-reporting; see also http://www.aclu.org/free-speech/you-have-every-right-photograph-cop

- The Federal Bureau of Investigation is collecting racial and ethnic information and "mapping" American communities around the country based on crude stereotypes about which groups commit different types of crimes. Nationwide, the FBI is gathering reports on innocent Americans' so-called "suspicious activity" and sharing it with unknown numbers of federal, state and local government agencies. http://www.aclu.org/mapping-fbi-uncovering-abusive-surveillance-and-racial-profiling

b. <u>Center for Democracy and Technology (CDT) – James Dempsey et al.</u>

- The government should not be **investigating groups based on political beliefs without some evidence that illegality is afoot**. Fishing expeditions are not just intrusive and contrary to the values of a pluralistic democracy, they divert law enforcement resources from analyzing real threats. Yet, as the Under Secretary noted in the released document, "intelligence organizations prepare intelligence assessments and analytic pieces on a vast array of issues where there are no 'specific tasking.'" ….The fiascos revealed a tendency among government agencies at all levels to investigate, or encourage investigation of, groups based on political beliefs, despite lacking evidence that these groups advocate or engage in violence or other illegal activity. That is precisely what occurred with DHS' investigation of the Nation of Islam. Was the "strong and rigorous system of **safeguards and oversight**" implemented since last spring and does it apply to the entire domestic intelligence apparatus? Or is the information sharing oversight system that failed in 2007 and 2009 still failing behind the scenes today? https://www.cdt.org/blogs/harleygeiger/newly-released-documents-show-flaws-domestic-intelligence-collection-and-oversight

c. Freedom & Justice Foundation - Mohamed Elibiary

- The Freedom and Justice Foundation (F&J) was founded in 2002 to politically empower the Texas Muslim community not simply through a special interest electoral strategy but through a sophisticated public policy reform strategy that would allow Muslims to coalition build while working for the greater benefit of society at large. F&J works on policy areas, including:
    - **Civil-Religious Liberties:** While sometimes working through national coalitions to protect civil liberties at the federal levels, F&J has mostly worked with state and federal government agencies tasked by law with a mandate to protect these freedoms in order to address civil or religious discrimination issues impacting Texas Muslims.
    - **National and Homeland Security Policy:** Coordination between intelligence agencies and law enforcement in the domestic arena, comprehensive immigration reform, DHS and FBI community partnership efforts, effective domestic counter-terrorism strategies that protect the homeland yet also safeguard our freedoms, effective counter-radicalization policies, etc.
- Note: The F&J website (http://www.freeandjust.org/) has limited information.

d. Electronic Privacy Information Center (EPIC) – Lillie Coney

- EPIC has a longstanding interest in the privacy implications of domestic surveillance and fusion centers. SAR presents privacy, civil liberties, and civil rights concerns. In particular SAR could be the basis for detaining and arresting people who pose no threat to public safety and who have engaged in no criminal activity. Additionally, SAR does not adhere to well-established legal parameters of probable cause and reasonable suspicion. Moreover, uncorroborated, adverse judgments about individuals are added to federal record systems without the clear protections of the Privacy Act. To the extent that this becomes a widely adopted policing techniques, there are significant implications for Constitutional and statutory rights. http://epic.org/privacy/suspicious-activity-reporting/default.html and citing http://americaswarwithin.org/articles/2011/09/07/mall-america-visitors-unknowingly-end-counterterrorism-reports about suspicious activity reporting by the Mall of America

Note: This is a non-exhaustive list for Background Purposes

2. Other groups/organizations concerned about transparency and use of technology for surveillance (e.g., Jones v. US), etc. Most groups are focused on issues beyond the ISE, e.g., detainees
    a. The Constitution Project - TCP Senior Counsel Sharon Bradford Franklin
    b. Think tanks (Brookings, Cato) - TDB
    c. Other Community groups – NAACP, National Council on La Raza (NCLR)

3. Other Sources of Commentary on SARs:
    a. Dana Priest of the Washington Post:
        - According to an investigation by the Washington Post, the NSI program, "by far the largest and most technologically sophisticated in the nation's history, collects, stores and analyzes information about thousands of U.S. citizens and residents, many of whom have not been accused of any wrongdoing."

        - Reports of suspicious behavior noticed by local law enforcement, or even by private citizens, are forwarded to the program, and profiles are constructed of persons who are merely under suspicion, without adjudicated evidence or reasonable suspicion that a crime is being committed.

        - See http://www.cbsnews.com/8301-503544_162-20010990-503544.html?tag=mncol;lst;1 for news story.

    b. Center for Strategic and International Studies (CSIS)
        - The numerous programs tied to the Nationwide SAR Initiative and the broader Information Sharing Environment signal an important step toward alleviating what the 9/11 Commission recognized as a major flaw in the country's national security apparatus. And with the recent uptick in "homegrown" extremism, programs like the NSI, which explicitly reaches out to state and local law enforcement officials, will prove especially important. How these initiatives are implemented—and how they evolve —will ultimately determine their success.
        - Another low-profile aspect of the NSI is its applicability to an "all-crimes environment," as described in the February status update. According the report, the NSI cycle, while focused on terrorism, can be applied just as readily to other criminal activity. This feature is likely to appeal most especially to local law enforcement officials, for whom terrorism is one of many concerns. The February status report suggested that changes to the NSI's concept of operations may be necessary to ensure that the program functions according to an "all-crimes" paradigm. The PM-ISE's lengthy July report to Congress made no mention of such potential alterations. Going forward, it will be interesting to see whether the

Note: This is a non-exhaustive list for Background Purposes

NSI's Program Management Office, in consultation with the PM-ISE, decides to reshape the concept of operations to better address non-terrorist threats. Such a move would likely prove useful for state and local law enforcement agencies forced to deal with crime tied to drugs, gangs, and other non-terrorist activities.

The numerous programs tied to the Nationwide SAR Initiative and the broader Information Sharing Environment signal an important step toward alleviating what the 9/11 Commission recognized as a major flaw in the country's national security apparatus. And with the recent uptick in "homegrown" extremism, programs like the NSI, which explicitly reaches out to state and local law enforcement officials, will prove especially important. How these initiatives are implemented—and how they evolve —will ultimately determine their success.

- See at http://csis.org/files/publication/100831_nelson_sar.pdf for more information.

c. Congressional Research Service (CRS):

   i. "Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress" (June 10, 2011) at http://fpc.state.gov/documents/organization/166837.pdf

   ii. Terrorism Information Sharing and the Nationwide Suspicious **Activity Report Initiative: Background and Issues for Congress"** (December 28, 2011) at http://www.fas.org/sgp/crs/intel/R40901.pdf raises the question of whether a national system may become overwhelmed by the sheer number of inputs.

The CRS report, in fact, identifies four primary issues that Congress, as the final overseer of the NSI, will face in plotting a course for DHS' suspicious activity reporting (SAR) programs:

- ***Too Many Dots.*** The NSI is designed to increase the amount of information flowing from state and local law enforcement agencies to the federal government, but the goal of "connecting the dots" will become more difficult as the number of dots increase. An avalanche of irrelevant or redundant data will divert law enforcement personnel and other resources from meaningful work. During a 40-month period prior to a 2007 SAR pilot program, for example, the FBI documented about 108,000 potential terror threats, suspicious incidents, and terrorist watchlist hits. The report

Note: This is a non-exhaustive list for Background Purposes

points to a need for Congress to consider which agency or agencies should handle quality control of SARs to prevent system overload.

- ***Data Privacy and Access.*** To achieve the objectives of the program, the report states, agency partners must establish protocols for protecting the privacy and civil liberties of individual citizens. An authorized use standard, including identification/authentication and privilege management, should be developed for users of a system that contains sensitive information, and Congress should examine NSI policies governing data privacy and access.

- ***Information Technology (IT) Infrastructure*.** The success of the NSI will depend on the infrastructure that supports it, and funding may fall short at fusion centers in some jurisdictions. As the minder of the nation's purse strings, Congress will need to consider ways to provide funding to fusion centers for this purpose.

- ***Metrics*.** Critics of SAR programs, who claim that a focus on suspicious activity will lead to racial and ethnic profiling and an avalanche of spurious tips, are – much like the DHS in formulating the program – relying on anecdotal or even hypothetical information. The only way to validate the program's effectiveness is through concrete measurements – of how many of the SARs collected by the program are meaningful intelligence "dots," or whether the right "dots" are being connected as a result of the program, for example. The report recommends that Congress request the DHS' Program Management Office for the NSI to develop these metrics.

  Metrics are an important first step in determining the NSI's value – but once those metrics are established, of course, DHS will be faced with the task of achieving these new standards of success. History has shown that SAR reporting has stopped several terrorist attacks. But will a nationwide SAR program increase the likelihood that additional attacks will be stopped? The Department of Homeland Security thinks so – it just can't prove it yet.

d. Berkeley City Council backs police reforms with civil liberties in mind. The council decided Tuesday night to approve recommendations that would make it more difficult for police to report suspected terrorists and criminals to regional and federal authorities; stop holding some people in its jails the federal government wants for immigration violations; and restrict police from gathering intelligence on people engaged in nonviolent, non-felonious civil disobedience.

http://www.mercurynews.com/breaking-news/ci_20901524/berkeley-passes-tentative-police-reforms-civil-liberties-mind

e. Center for Investigative Reporting – GW Schultz (in partnership with NPR) -- Civil liberties and privacy advocates, including members of Congress, have criticized some homeland security initiatives as intrusive and prone to abusive profiling. Advocates say such reporting can fuel anxiety and create a chilling atmosphere in which people who seem different are targeted for extra attention. Suspicious activity reports, they add, are part of a broader trend of surveillance of the innocent and suspect alike since 9/11. http://americaswarwithin.org/articles/2011/09/07/finding-meaning-suspicious-activity-reports-more-art-science

f. Geoffrey Stone, a constitutional law professor at the University of Chicago, said that government officials should consider how a program affects the exercise of political and religious beliefs, regardless of whether they insist the information is being used appropriately.
    i. Publications include: *Speaking Out! Reflections on Law, Liberty and Justice* (2010); *Top Secret: When Our Government Keeps Us in the Dark* (2007) and *War and Liberty: An American Dilemma* (2007); and *Perilous Times: Free Speech in Wartime from the Sedition Act of 1798 to the War on Terrorism* (2004)

g. Juliette Kayyem, a former homeland security assistant secretary in the Obama administration and a onetime adviser to Massachusetts Gov. Deval Patrick, said that "You have just a tremendous amount of information going into the intelligence-sharing apparatus in the hopes that it will either come up with terrorism or suspicious activity or criminal activity," "That's a lot of input … to ensure that you're going to connect the dots better, right? One clear way is to make sure the dots are better. There (are) too many dots right now."

MORGAN, LEWIS & BOCKIUS LLP
Stephen Sotch-Marmo (admitted *pro hac vice*)
stephen.scotch-marmo@morganlewis.com
Michael James Ableson (admitted *pro hac vice*)
michael.ableson@morganlewis.com
101 Park Avenue
New York, NY 10178
(212) 309.6000; Facsimile: (212) 309.6001

AMERICAN CIVIL LIBERTIES UNION FOUNDATION
OF NORTHERN CALIFORNIA
Linda Lye (#215584) llye@aclunc.org
Julia Harumi Mass (#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 (#238917) nasrinab@advancingjustice-alc.org
Yaman Salahi (#288752) yamans@advancingjustice-alc.org
55 Columbus Avenue
San Francisco, CA 94111
Telephone: 415-848-7711
Facsimile: 415-896-1702

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

Additional counsel listed on signature page

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

WILEY GILL; JAMES PRIGOFF;TARIQ RAZAK; KHALED IBRAHIM; and AARON CONKLIN, Plaintiffs, v. DEPARTMENT OF JUSTICE; LORETTA E. LYNCH,[1] in her official capacity as the Attorney General of the United States; PROGRAM MANAGER - INFORMATION SHARING ENVIRONMENT; KSHEMENDRA PAUL, in his official capacity as the Program Manager of the Information Sharing Environment, Defendants.	Case No. 3:14-cv-03120 (RS) **FIRST SUPPLEMENTAL COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF** Administrative Procedure Act Case

[1] In light of Ms. Lynch's swearing in as Attorney General on April 27, 2015, she is automatically substituted as a Defendant in this action in place of Eric Holder. *See* Fed. R. Civ. P. 25(d).

INTRODUCTION

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

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

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

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

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

PARTIES

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

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

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

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

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

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

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

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

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

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

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

15. Defendant Loretta Lynch is the Attorney General of the United States and as the head of DOJ is responsible for the regulations, guidelines, and standards adopted by DOJ. She is sued in her official capacity.

16. Defendant PM-ISE is a federal agency within the meaning of the APA, 5 U.S.C. § 551(1) (2012). Pursuant to the Intelligence Reform and Terrorism Prevention Act of 2004 ("IRTPA"), PM-ISE is charged with issuing uniform standards for sharing terrorism and homeland security information across federal, state, and local governments. 6 U.S.C. § 485 (2012). PM-ISE has issued a standard governing SAR reporting and conducts trainings on that standard. PM-ISE's standard for SAR reporting is set forth its "Information Sharing Environment (ISE) - Functional Standard (FS) - Suspicious Activity Reporting (SAR)" ("Functional Standard"). PM-ISE issued Version 1.5 of the Functional Standard " in May 2009. Functional Standard 1.5 is attached as Appendix D to this Complaint. PM-ISE issued Version 1.5.5 of the Functional Standard in February 2015. Functional Standard 1.5.5 is attached as Appendix K to this Complaint.

17. Defendant Kshemendra Paul occupies the office of the PM-ISE, is the head of PM-ISE, and is responsible for the regulations, guidelines, and standards adopted by PM-ISE. He is sued in his official capacity.

<u>JURISDICTION AND VENUE</u>

18. This is an action under the APA, to set aside agency actions because they are arbitrary and capricious, an abuse of discretion, and not in accordance with law, and because they are without observance of procedure required by law. *See* 5 U.S.C. § 706 (2)(A), (D) (2012). This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 and § 1349 (2012).

19. The Court has authority to grant declaratory relief pursuant to the Declaratory Judgment Act, 28 U.S.C. § 2201 and § 2202 (2012).

20. Venue is proper in this district pursuant to 28 U.S.C. § 1391(e) (2012) because Defendants are agencies of the United States and officers of the United States sued in their official capacities, a substantial part of the events or omissions giving rise to this action occurred

in this district, including Alameda and Contra Costa Counties, and one or more plaintiffs reside in this district.

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

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

(a) At the initial response and investigation stage, and even before a SAR is submitted to a fusion center or the FBI, Defendant PM-ISE instructs the federal, state, local, or tribal law enforcement agency with jurisdiction to respond to the reported observation by "gather[ing] additional facts through personal observations, interviews, and other investigative activities. This may, at the discretion of the [responding] official, require further observation or engaging the suspect in conversation." Functional Standard 1.5 at 32; accord Functional Standard 1.5.5 at 53.

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

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

(d) FBI agents have admitted that they are required to follow-up on SARs, even when they know the individual does not pose a threat. For example, a professional freelance photographer in Los Angeles, California who specializes in industrial photography, has twice been interviewed by the FBI after photographing industrial sites. After security guards instructed him not to photograph certain industrial sites in the area of the Port of Long Beach in April 2008, FBI agents visited him at his home to question him about the incident. The FBI contacted him again, after Los Angeles Sheriff's Department personnel interfered with his efforts to photograph another industrial site in approximately December 2009. The FBI agent told the photographer that he knew the photographer did not pose a threat but that because a report had been opened, he was required to follow-up on it.

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

28. This surveillance program has not proven effective in the fight against terrorism. The United States Government Accountability Office ("GAO") has faulted the program for failing to demonstrate *any* results-oriented outcomes, such as arrests, convictions, or thwarted threats, even though tens of thousands of SARs had been deemed sufficiently significant to be uploaded to national SAR databases as of October 2012. *See* GAO SAR Report at 33, 36-38. In 2012, a Senate Subcommittee reviewed a year of similar intelligence reporting from state and local authorities, and identified "dozens of problematic or useless" reports "potentially violating civil liberties protections." United States Senate, Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, "Federal Support for and

Involvement in State and Local Fusion Centers," October 3, 2012 at 27. Another report, co-authored by Los Angeles Police Department Deputy Chief Michael Downing, found that SARs have "flooded fusion centers, law enforcement, and other security entities with white noise." The George Washington University Homeland Security Policy Institute, "Counterterrorism Intelligence: Fusion Center Perspectives," June 26, 2012 at 31.

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

- "Suspicious ME [Middle Eastern] Males Buy Several Large Pallets of Water"
- A sergeant from the Elk Grove Police Department reported "on a suspicious individual in his neighborhood"; the sergeant had "long been concerned about a residence in his neighborhood occupied by a Middle Eastern male adult physician who is very unfriendly"
- "Female Subject taking photos of Folsom Post Office"
- "an identified subject was reported to be taking photographs of a bridge crossing the American River Bike trail"
- "I was called out to the above address regarding a male who was taking photographs of the [name of facility blacked out] [in Commerce, California]. The male stated, he is an artist and enjoys photographing building[s] in industrial areas … [and] stated he is a professor at San Diego State private college, and takes the photos for his art class."
- "I observed a male nonchalantly taking numerous pictures inside a purple line train [in Los Angeles County] … The male said he was taking pictures because they were going to film the television show '24' on the train next week."

- "two middle eastern looking males taking photographs of Folsom Dam. One of the ME males appeared to be in his 50's"
- "Suspicious photography of the Federal Courthouse in Sacramento": an "AUSA [Assistant United States Attorney] reported to the Court Security Officer (CSO) a suspicious vehicle occupied by what [name blacked out] described as two Middle Eastern males, the passenger being between 40-50 years of age."
- "Suspicious photography of Folsom Dam by Chinese Nationals": "a Sac County Sheriff's Deputy contacted 3 adult Asian males who were taking photos of Folsom Dam. They were evasive when the deputy asked them for identification and said their passports were in their vehicle."

B. Conflicting Federal Rules for Collection of Intelligence Information

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

1. 28 C.F.R. Part 23

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

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

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

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

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

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

37. DOJ amended the rule again in 1993 to include a definition of "reasonable suspicion":

> Reasonable Suspicion . . . is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, 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.

See 28 C.F.R. § 23.20.

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

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

> the potential for national dissemination of information in intelligence information 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 is enhanced by the reasonable suspicion requirement. Scarce resources are not wasted by agencies in coordinating information on subjects for whom information is vague, incomplete and conjectural.

Id.

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

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

<u>2. PM-ISE Standard for Suspicious Activity Reporting</u>

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

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

44. In or about May 2009, PM-ISE released Information Sharing Environment (ISE) - Functional Standard (FS) - Suspicious Activity Reporting (SAR) Version 1.5 ("Functional Standard 1.5"). In or about February 2015, PM-ISE released Information Sharing Environment (ISE) – Functional Standard (FS) – Suspicious Activity Reporting (SAR) Version 1.5.5 ("Functional Standard 1.5.5"). Both Functional Standard 1.5 and Functional Standard 1.5.5 adopt a "reasonably indicative" standard for suspicious activity reporting. *See* Functional Standard 1.5 at 2 (defining suspicious activity as "[o]bserved behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity"); Functional Standard 1.5.5 at 4 (defining suspicious activity as "[o]bserved behavior reasonably indicative of pre-operational planning associated with terrorism or other criminal activity"). PM-ISE is considering a further update to the Functional Standard (to be designated Version 2.0) that may broaden the standard for suspicious activity reporting.

45. The agency has expressly acknowledged that the Functional Standard's "reasonably indicative" standard requires "less than the 'reasonable suspicion' standard." PM-ISE, <u>Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations–Nationwide Suspicious Activity Reporting Initiative</u> at 12 (draft May 2010).

46. The Functional Standard also identifies sixteen categories of activity that fall under the standard and provide a guide to law enforcement in determining what amounts to a suspicious activity. These categories include photography, observation/surveillance, and acquisition of materials or expertise. Functional Standard 1.5 at 29-30; Functional Standard 1.5.5 at 42-51.

47. The Functional Standard applies to, *inter alia,* "all departments or agencies that possess or use terrorism or homeland security information." Functional Standard 1.5 at 1; Functional Standard 1.5.5 at 1. The Functional Standard applies to state, local, and tribal law

enforcement agencies and fusion centers that participate in the NSI. Agencies participating in the NSI follow the Functional Standard in reporting suspicious activity.

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

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

50. In promulgating the Functional Standard, PM-ISE expressly cited its legislative authority under, *inter alia*, the IRTPA over governmentwide standards for information sharing. Functional Standard 1.5 at 1; Functional Standard 1.5.5 at 1.

51. The Functional Standard constitutes final agency action and a legislative rule within the meaning of the APA.

52. PM-ISE issued the Functional Standard without observing the process set forth in the APA for public notice and comment. Functional Standard 1.5.5 went into immediate effect upon its publication on February 23, 2015 and remains currently in effect.

<u>3. DOJ Standard for Suspicious Activity Reporting</u>

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

54. DOJ, through its component the FBI, has set forth the following standard for suspicious activity reporting: "observed behavior that *may be indicative* of intelligence gathering or pre-operational planning related to terrorism, criminal or other illicit intention." FBI, Privacy Impact Assessment for the eGuardian Threat Tracking System at § 1.1 (emphasis added). This standard is set forth in the FBI's 2008 eGuardian Privacy Impact Assessment ("2008 eGuardian PIA"), which is attached as Appendix E to this Complaint. "[T]he FBI uses the criteria in the

eGuardian Privacy Impact Assessment (dated November 25, 2008) … to determine if SARs have a potential nexus to terrorism." GAO SAR Report at 6 n.10.

55. DOJ's "may be indicative" SAR Standard is even broader than PM-ISE's "reasonably indicative" Functional Standard. *See* GAO SAR Report at 15-16. But like the Functional Standard, DOJ's SAR Standard encourages reporting even in the absence of reasonable suspicion of criminal activity.

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

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

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

(2) "Interest in using Internet cafes, despite hotel Internet availability…." *Id.*

(3) "Requests for specific rooms, floors, or other locations in the hotel…." *Id.*

(4) "Multiple visitors or deliveries to one individual or room." *Id.*

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

(c) "Possess student visa but not English Proficient." *Id.*

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

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

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

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

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

(a) "[P]eople acting suspiciously." *Id.*

58. DOJ through its components has also issued "Potential Indicators of Terrorist Activities Related to Electronic Stores" (attached as Appendix I to this Complaint) and "Potential Indicators of Terrorist Activities Related to Mass Transportation" (attached as Appendix J to this Complaint). Activities identified as suspicious in connection with mass transportation include "[a]cting nervous or suspicious," and "[u]nusual or prolonged interest in … entry points and access controls."

59. DOJ through its components trains participants in the NSI about DOJ's SAR Standard. For example, as of 2013, the PMO had provided training for 290,000 line officers (law enforcement officers whose routine duties put them in a position to observe "suspicious" activity), 2,000 analytical personnel, and executives from 77 fusion centers. *See* GAO SAR Report at 29. DOJ components teach participants in the NSI, including frontline officers and fusion center analysts to submit to the FBI "all potentially terrorism-related information and not just ISE-SARs that met the [PM-ISE's] Functional Standard." GAO SAR Report at 16.

60. DOJ's SAR Standard applies to state, local, and tribal law enforcement agencies and fusion centers that participate in the NSI. Agencies participating in the NSI follow DOJ's SAR Standard in reporting suspicious activity.

61. DOJ's SAR Standard purports to define the scope of suspicious activity that should be reported for agencies participating in the NSI. The purpose of DOJ's SAR Standard is to standardize SAR reporting at the federal, state, and local levels.

62. Because DOJ's SAR Standard is broader than PM-ISE's Functional Standard and DOJ's behavioral categories include the catch-all "people acting suspiciously," any activity that falls under PM-ISE's Functional Standard also falls under DOJ's SAR Standard.

63. Fusion centers that follow DOJ's SAR Standard instead of PM-ISE's Functional Standard send many SARs to the FBI for review. For example, of the SARs uploaded by one state's fusion center to a national SAR database from June 2011 to October 2012, only 10% met PM-ISE's Functional Standard. *See* GAO SAR Report at 16.

64. DOJ establishes an even broader standard than the already overbroad Functional Standard, and the DOJ reinforces its broader standard through the trainings it provides to NSI participants and through other mechanisms. For example, when fusion center personnel are uncertain whether to share a SAR, DOJ encourages them to err on the side of overreporting. *See* GAO SAR Report at 16. In addition, the only feedback mechanism participants in the NSI currently receive on whether they are reporting SARs appropriately is provided by the FBI through its eGuardian system. *See* GAO SAR Report at 13-14. The feedback the FBI provides reinforces the DOJ SAR Standard to NSI participants.

65. DOJ's 2008 eGuardian PIA, which sets forth the agency's standard for reporting suspicious activity, was signed by four "Responsible Officials," two "Reviewing Officials," and one "Approving Official." It reflects the consummation of the agency's decision making process.

66. DOJ's 2008 eGuardian PIA contains a set of mandatory, non-discretionary rules and obligations. It lays out clear instructions for the use of the eGuardian system to collect and share SARs and the standard for defining "suspicious activity." For example, the 2008 eGuardian PIA states that the eGuardian system will "ensure consistency of process and of handling protocols" and mandates that all users "will be required to complete robust system training that will incorporate eGuardian policies and procedures." 2008 eGuardian PIA at 4. In

addition, the eGuardian User Agreement, attached to the 2008 eGuardian PIA, states that "[i]ncidents not meeting the criteria of suspicious activity or with a potential nexus to terrorism and that, further, do not comply with the above-stated rules, will be immediately deleted from eGuardian." 2008 eGuardian PIA at 25.

67. DOJ has consistently reinforced its standard for SAR reporting, set forth in the 2008 eGuardian PIA, through training materials and other publications that identify categories of behavior that the agency contends are suspicious and should be reported.

68. In promulgating DOJ's SAR Standard, DOJ expressly invoked its statutory "mandate" under IRTPA and "other statutes … to share terrorism information with other federal, and state, local and tribal (SLT) law enforcement partners." 2008 eGuardian PIA at 2.

69. DOJ's SAR Standard constitutes final agency action and a legislative rule within the meaning of the APA.

70. Defendant DOJ issued the DOJ SAR Standard without observing the process set forth in the APA for public notice and comment. It is the DOJ Standard for SAR reporting currently in effect.

<u>**4. PM-ISE's Functional Standard and DOJ's SAR Standard Conflict with 28 CFR Part 23**</u>

71. As a report of "[o]bserved behavior reasonably indicative of pre-operational planning" related to or associated with "terrorism or other criminal activity" (Functional Standard) or a report of "observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal or other illicit intention" (DOJ's SAR Standard), a SAR contains data relevant to the identification of an individual who is suspected in some fashion of being involved in criminal, in particular, terrorist activity.

72. A SAR constitutes "criminal intelligence" within the meaning of 28 CFR Part 23.

73. State, local, and tribal law enforcement agencies and fusion centers that participate in the NSI and observe PM-ISE's Functional Standard and/or DOJ's SAR Standard collect, review, analyze, and disseminate SARs. These entities operate arrangements, equipment, facilities, and procedures, used for the receipt, storage, interagency exchange or

dissemination, and analysis of SARs. Upon information and belief, these entities and the systems they operate for receiving, storing, exchanging, disseminating, and analyzing SARs operate through support from Defendant DOJ's component OJP.

74. State, local, and tribal law enforcement agencies and fusion centers that participate in the NSI and observe PM-ISE's Functional Standard and/or DOJ's SAR Standard are "projects" within the meaning of 28 CFR Part 23. The systems or databases on which SARs are maintained and through which they are collected and disseminated are "criminal intelligence systems" within the meaning of 28 CFR Part 23.

75. PM-ISE's Functional Standard and DOJ's SAR Standard set forth operating principles for the collection, maintenance, and dissemination of data relevant to the identification of an individual who is suspected in some fashion of being involved in criminal, in particular, terrorist activity. Both standards, however, encourage or purport to authorize collection, maintenance, and dissemination of such data even in the absence of reasonable suspicion of criminal activity. Both standards encourage or purport to authorize collection, maintenance, and dissemination of much more data than that permitted under 28 CFR Part 23. Both standards therefore conflict with 28 CFR Part 23.

76. Through PM-ISE's promulgation of its Functional Standard and DOJ's promulgation of its SAR Standard, and through each agency's training of entities participating in the NSI in their respective standards for reporting suspicious activity, Defendants PM-ISE, Paul, DOJ, and Holder have undermined and thereby violated 28 CFR Part 23.

77. Neither DOJ nor PM-ISE has offered any reasoned basis for departing from the reasonable suspicion standard set forth in 28 CFR Part 23 for the collection, maintenance, and dissemination of SARs.

78. DOJ could rescind its SAR reporting standard. If DOJ rescinded its SAR reporting standard, participants in the NSI would cease collecting, maintaining, reviewing, analyzing and disseminating SARs based on DOJ's SAR Standard, and it would be clear that the governing standard for suspicious activity reporting is 28 CFR Part 23. As a result, individuals who are currently the subject of SARs but whose conduct did not give rise to a reasonable

suspicion of criminal activity would no longer have their information collected, maintained, and disseminated in SAR databases. DOJ could cease collecting, maintaining, reviewing, analyzing, and disseminating SARs about individuals whose conduct did not give rise to a reasonable suspicion of criminal activity.

79. PM-ISE could rescind the Functional Standard. If PM-ISE rescinded the Functional Standard, participants in the NSI would cease collecting, maintaining, reviewing, analyzing and disseminating SARs based on the Functional Standard, and it would be clear that the governing standard for suspicious activity reporting is 28 CFR Part 23. As a result, individuals who are currently the subject of SARs but whose conduct did not give rise to a reasonable suspicion of criminal activity would no longer have their information collected, maintained, and disseminated in SAR databases.

C. Plaintiff's Allegations

1. Wiley Gill

80. Wiley Gill is a United States citizen living in Chico, California. He works as a custodian at Chico State, which he attended as an undergraduate. Mr. Gill converted to Islam in 2009, after learning about the religion in a course he took while a student at Chico State.

81. Mr. Gill is the subject of a SAR that identifies him as a "Suspicious Male Subject in Possession of Flight Simulator Game." This SAR falls into one or more of the behavioral categories identified in the Functional Standard, in particular, "[a]cquisition of [e]xpertise" and potentially "[a]viation [a]ctivity." Functional Standard 1.5 at 29-30; Functional Standard 1.5.5 at 45, 50. It also falls under one or more behavioral categories identified by Defendant DOJ, such as the catch-all behavioral category of "acting suspiciously."

82. Mr. Gill's SAR was collected, maintained, and disseminated through a fusion center SAR database, and uploaded to eGuardian and/or another national SAR database. As a result, the FBI has scrutinized Mr. Gill, conducted extensive background checks on him, and created a file about him.

83. The SAR was created on or about May 23, 2012, and purports to document an encounter between Mr. Gill and the Chico Police Department ("CPD") on or about May 20,

2012. The SAR states that a CPD officer was investigating a domestic violence incident and believed the suspect may have fled into Mr. Gill's residence. The SAR states that this was later discovered to be unfounded. It acknowledges that the CPD officer searched Mr. Gill's home. The SAR asserts that Mr. Gill's computer displayed a screen titled something to the effect of "Games that fly under the radar," which appeared to be a "flight simulator type of game." The SAR concludes by describing Mr. Gill's "full conversion to Islam as a young WMA [white, male adult]," "pious demeanor," and "potential access to flight simulators via the internet" as "worthy of note."

84. CPD's search of Mr. Gill's residence on or about May 20, 2012 did in fact occur. But the SAR contains numerous misstatements and omits several crucial facts, including that two CPD officers banged on Mr. Gill's door and after when he went to open it, they came around the corner of the house with their guns drawn and pointed at Mr. Gill. Mr. Gill was thrown off guard. The officers eventually lowered their guns, and then asked to search Mr. Gill's home, based on the alleged domestic violence incident involving two individuals that they claimed to have received. Mr. Gill informed the officers that he was home alone. Despite that, the officers continued to ask to search his home. Mr. Gill was reluctant to grant permission, but felt that he had no choice under the circumstances. One officer remained with Mr. Gill outside, while the other searched his home. Mr. Gill did not feel free to leave. Mr. Gill cooperated with the officers' request for identification. Mr. Gill believes that he was likely viewing a website about video games at the time of the May 20, 2012, incident.

85. On information and belief, the officers' contention that they were investigating a domestic violence call was a pretext for searching Mr. Gill's home because CPD had already decided to investigate Mr. Gill because of his religion.

86. The SAR also describes two earlier encounters between CPD and Mr. Gill, one at the Mosque that Mr. Gill attends and another while Mr. Gill was walking through downtown Chico "with elders." The SAR describes Mr. Gill in these instances as "avoid[ing] eye contact" and "hesitant to answer questions."

87. Mr. Gill recalls CPD officers visiting the Mosque he attends, paying what they described as a courtesy visit in an attempt to build good relations with the Muslim community. Mr. Gill listened to the presentation. When it was over, CPD officers asked Mr. Gill his name, whether he went to school, and if he was employed. Mr. Gill answered all of their questions. His understanding is that the officers did not question anyone else in this manner.

88. Mr. Gill also recalls encountering CPD officers while he was walking through downtown Chico with two older Muslim men who are friends from the Mosque. A CPD officer called out Mr. Gill's name and asked Mr. Gill if he had found a job yet. Mr. Gill answered the question, but was caught off guard by the encounter because he did not recognize the officer and was surprised that the officer knew his name and employment status.

89. At no point during any of the encounters with CPD recounted in the SAR did Mr. Gill engage in conduct that gave rise to a reasonable suspicion of criminal activity.

90. The CPD also targeted Mr. Gill in two other encounters that are not described in the SAR, and that do not involve any conduct by Mr. Gill that gave rise to a reasonable suspicion of criminal activity, but instead reflect CPD's suspicion of Mr. Gill because of his religion. One of the incidents occurred before CPD filed the SAR about Mr. Gill on or about May 23, 2012; the other occurred after. This religious harassment is attributable to the training of local law enforcement on the SARs standards and process.

91. In approximately September 2010, after Mr. Gill had converted to Islam, two CPD officers visited him at his apartment and requested to speak to him about supposedly "anti-American statements" that he had made. One of the officers referred to having a file on Mr. Gill, refused to explain what "anti-American statements" Mr. Gill had purportedly made or the source of the information, and stated that he wished to ensure Mr. Gill would not turn into another Mohammed Atta, one of the individuals identified as a September 11 hijacker. Mr. Gill still does not know how he came to the attention of the CPD.

92. Around or after July 2012, Mr. Gill also received a telephone call from a CPD officer. Over the phone, the CPD officer said Mr. Gill should shut down his Facebook page because of the video games Mr. Gill played. At the time, Mr. Gill had a picture of the Shahada,

the Muslim statement of faith, on his Facebook page. Mr. Gill told the CPD officer he would not take down his Facebook page and Mr. Gill also told the CPD officer that he believed the CPD wanted Mr. Gill to take down his Facebook page because of its references to Islam. The CPD officer refused to comment on Mr. Gill's observation, but stated that he had a report on Mr. Gill and indicated that Mr. Gill was on some kind of watch list.

93. By describing Mr. Gill's conversion to Islam and "pious demeanor" in the SAR as "worthy of note," CPD implicitly acknowledges that it found him "suspicious" because he is a devout Muslim.

94. Defendants' issuance of overly broad definitions of "suspicious activity" and the categories of behavior they have identified as "suspicious" include, among other things, "[a]cquisition of expertise" (PM-ISE) and "[n]o obvious signs of employment" (DOJ). On information and belief, CPD officers are trained in Defendants' standards for SAR reporting.

95. Defendants' overly broad standards for reporting suspicious activity opens the door to and encourages religious profiling. These standards opened the door to and encouraged the religious profiling of Mr. Gill by CPD, CPD's repeated questioning and ongoing scrutiny of Mr. Gill, and CPD's identification of Mr. Gill in a SAR as someone engaged in activity with a potential nexus to terrorism.

96. In addition, the Functional Standard instructs law enforcement agencies at the "[i]nitial [r]esponse and [i]nvestigation stage" to respond to the observation reported in a SAR, and "gather[] additional facts," by, *inter alia*, "engaging the suspect in conversation" and "other investigative activities." Functional Standard 1.5 at 32; Functional Standard 1.5.5 at 53. The CPD was implementing the protocols set forth in the Functional Standard when it harassed Mr. Gill on or about May 2012, before, and after.

97. Because Mr. Gill is the subject of a SAR that falls under Defendants' standards for suspicious activity reporting, Mr. Gill has been automatically subjected to law enforcement scrutiny. That scrutiny has included, among other things, CPD's telephone call to him around or after July 2012 and the FBI's creation of a file about and investigation of Mr. Gill.

98. Given the repeated harassment Mr. Gill has already suffered by CPD, he fears further action may be taken against him by CPD and other investigative agencies as the result of this SAR. He also fears further investigative harassment at the hands of the CPD and other agencies caused by the existence of the SAR.

99. Mr. Gill also has experienced frustration and stress resulting from the creation of the SAR based on innocent conduct. He is also deeply troubled by what may result from the collection, maintenance, and dissemination in a national database of a report describing him as engaging in suspicious activity with a potential nexus to terrorism.

100. The SAR about Mr. Gill is maintained and will continue to be maintained in one or more national SAR databases, where it can be accessed by law enforcement agencies across the country.

2. James Prigoff

101. James Prigoff is a United States citizen who resides in Sacramento, California. He is an internationally renowned photographer. The focus of his work is public art, such as murals and graffiti art. He has amassed over 80,000 photographic slides and published several books containing his photography. Mr. Prigoff is also a former business executive, having served as a Senior Vice President of the Sara Lee Corporation and a President of a division of Levi Strauss.

102. In or around the spring of 2004, Mr. Prigoff was in Boston, Massachusetts. While there, he sought to photograph a famous piece of public art known as the “Rainbow Swash,” located in the Dorchester neighborhood of Boston. The artwork is painted on a natural gas storage tank, which is surrounded by a chain link fence. It is highly visible to commuters from the local expressway.

103. Mr. Prigoff drove a rental car to a public area outside the fence surrounding the Rainbow Swash, and set up to take photographs. He chose the location in part because of favorable lighting conditions. From this location, the sun was behind him and casting its light on the Rainbow Swash. Before Mr. Prigoff could take any photographs, two private security guards came out from inside the fenced area and told him that he was not allowed to photograph,

claiming the area was private property. Mr. Prigoff pointed out to the security guards that he was not, in fact, on private property. The guards still insisted that Mr. Prigoff could not photograph.

104. To avoid a confrontation with the guards, Mr. Prigoff departed. He left without giving the security guards any identifying information.

105. He drove further down the road to another public location outside the fenced perimeter and attempted to take photographs from this second location. But the guards began to follow him.

106. To avoid further harassment by the guards, he drove to a third location on the other side of the Rainbow Swash. The guards did not follow him to this third location, and he was finally able to take photographs of the Rainbow Swash unmolested. But the lighting conditions were significantly inferior to those at the first two locations; from this third location, he had to photograph into the sunlight.

107. At no point while he was attempting to photograph the Rainbow Swash did Mr. Prigoff engage in conduct that gave rise to a reasonable suspicion of criminal activity.

108. Mr. Prigoff subsequently discovered photographs online, including on the Rainbow Swash's Wikipedia webpage. These widely available photographs were taken from vantage points closer than the three locations from which Mr. Prigoff attempted to and actually took photographs.

109. Mr. Prigoff returned to his home in Sacramento, California after his trip to Boston. A few months later, on or about August 19, 2004, he came home one day to find a business card affixed to his door from Agent A. Ayaz of the Joint Terrorism Task Force, which, as noted above, is a partnership between the FBI and other law enforcement agencies. On the back was a handwritten note stating, "Mr. Prigoff, please call me. Thanks." Mr. Prigoff later learned from a neighbor across the street that two agents had knocked on her door and asked for information about Mr. Prigoff.

110. Mr. Prigoff called Mr. Ayaz, who asked if Mr. Prigoff had been to Boston. Realizing that Mr. Ayaz was referring to his efforts to photograph a piece of public art, Mr.

Prigoff explained what had occurred. On information and belief, security guards at the site of the Rainbow Swash had submitted a SAR or SAR precursor report regarding Mr. Prigoff that included his rental car information, after which authorities traced him from Boston, Massachusetts, to his home in Sacramento, California.

111. Mr. Prigoff is very upset that he was tracked cross-country from Boston to Sacramento, and contacted by law enforcement agents at his home over his effort to engage in photography from a public location. Mr. Prigoff is also very upset that law enforcement agents questioned at least one of his neighbors about him, as such questioning casts the negative and strong implication that Mr. Prigoff had somehow engaged in misconduct.

112. Taking photographs of infrastructure falls under one or more of the behavioral categories identified by Defendant PM-ISE under the Functional Standard as “suspicious,” and also falls under one or more behavioral categories identified by Defendant DOJ, such as the catch-all behavioral category of “acting suspiciously.” After attempting to photograph a piece of public art painted on a natural gas storage tank in Boston, Mr. Prigoff was tracked to his home in Sacramento and questioned about his trip to Boston, even though he never provided the security guards with identifying information. On information and belief, Mr. Prigoff is the subject of a SAR or SAR precursor report, which was filed by security guards at the Rainbow Swash. On information and belief, the report about him was collected, maintained, and disseminated through a fusion center database, and uploaded to eGuardian and/or another national SAR or similar counterrorism database. On information and belief, the report about him was collected, maintained, and disseminated under standards that authorized collection, maintenance and dissemination of information even in the absence of reasonable suspicion of criminal activity; Defendants’ standards for SAR reporting ratify that conduct.

113. On information and belief, security guards at the Rainbow Swash were trained in standards that encourage reporting of activity deemed connected to terrorism, even in the absence of reasonable suspicion of criminal activity; Defendants’ standards for SAR reporting ratify that conduct. Because of that training, they interfered with Mr. Prigoff’s lawful efforts to take photographs of the Rainbow Swash.

114. Because Mr. Prigoff is the subject of a report that falls under Defendants' standards for suspicious activity reporting, Mr. Prigoff has been automatically subjected to law enforcement scrutiny. That scrutiny has included but may not be limited to a follow-up visit by an agent of the Joint Terrorism Task Force to his home, a telephone call with that agent, and inquiries by that agent of at least one of his neighbors about him.

115. Upon information and belief, the report about Mr. Prigoff is maintained and will continue to be maintained in one or more national SAR or similar counterterrorism databases, where it can be accessed by law enforcement agencies across the country.

116. Mr. Prigoff continues to be an active photographer and often takes pictures of architectural structures and post offices, among other sites that could be described as "infrastructure." Because taking photographs of infrastructure falls under one or more of the behavioral categories identified by Defendant PM-ISE under the Functional Standard as "suspicious," and also falls under one or more behavioral categories identified by Defendant DOJ, such as the catch-all behavioral category of "acting suspiciously," he is likely to be the subject of another SAR in the future. He fears that his efforts to take photographs of such areas will be hindered again in the future.

117. Mr. Prigoff is also deeply troubled by what may result from the collection, maintenance, and dissemination in a national database of a report describing him as engaging in suspicious activity with a potential nexus to terrorism.

3. Khaled Ibrahim

118. Khaled Ibrahim is a United States citizen of Egyptian descent living in San Jose, California. He works in accounting for Nordix Computer Corporation, a computer network consulting and service company. He formerly worked as a purchasing agent for Nordix. As part of his job as purchasing agent, Mr. Ibrahim bought computers in bulk from retail stores, where the stores allowed such transactions.

119. On several occasions in 2011, Mr. Ibrahim went to the Best Buy in Dublin, California in order to attempt to purchase computers in bulk for Nordix. On one such occasion, he was told that management did not allow such bulk purchases and, with that, Mr. Ibrahim left.

120. At no point while he was attempting to purchase computers from Best Buy did Mr. Ibrahim engage in conduct that gave rise to a reasonable suspicion of criminal activity.

121. Mr. Ibrahim is the subject of a SAR, created on November 14, 2011, regarding Mr. Ibrahim's attempts to purchase "a large amount of computers." The SAR about him was collected, maintained, and disseminated through a fusion center SAR database, and uploaded to the FBI's eGuardian database. Upon information and belief, the personnel at the fusion center who uploaded Mr. Ibrahim's SAR to eGuardian were trained in Defendants' standards for SAR reporting.

122. The SAR pertaining to Mr. Ibrahim falls into one or more of the behavioral categories identified in the Functional Standard, in particular, "[a]cquisition … of unusual quantities of materials." Functional Standard 1.5 at 30; Functional Standard 1.5.5 at 50. It also falls under one or more behavioral categories identified by Defendant DOJ, such as the catch-all behavioral category of "acting suspiciously" and DOJ's "Potential Indicators of Terrorist Activities Related to Electronic Stores."

123. Because Mr. Ibrahim is the subject of a SAR that falls under Defendants' standards for suspicious activity reporting, Mr. Ibrahim has been automatically subjected to law enforcement scrutiny. That scrutiny may include but is not limited to scrutiny or interviews by any of the law enforcement agencies across the country that have access to the FBI's eGuardian system, to which his SAR was uploaded.

124. Mr. Ibrahim is particularly disturbed that trained law enforcement personnel at a fusion center uploaded the SAR about him to eGuardian, thereby flagging him as an individual with a potential nexus to terrorism. He is also troubled by what may result from the collection, maintenance, and dissemination in a national database of a report describing him as engaging in suspicious activity with a potential nexus to terrorism. Mr. Ibrahim is upset that a SAR was entered about him potentially because of his Middle Eastern descent, and believes that this system of racial profiling diminishes the rights of Middle Eastern communities.

125. The SAR about Mr. Ibrahim is maintained and will continue to be maintained in one or more national SAR databases, where it can be accessed by law enforcement agencies across the country.

<u>4. Tariq Razak</u>

126. Tariq Razak is a United States citizen of Pakistani descent. He resides in Placentia, California. A graduate of the University of California at Irvine, he works in the bio-tech industry.

127. Mr. Razak is the subject of a SAR pertaining to a "Male of Middle Eastern decent [sic] observed surveying entry/exit points" at the Santa Ana Train Depot.

128. On May 16, 2011, Santa Ana Police Officer J. Gallardo filed a SAR regarding Mr. Razak. According to the SAR, Officer Gallardo responded to a call at the Santa Ana Train Depot from Security Officer Karina De La Rosa. Ms. De La Rosa explained that her "suspicion became aroused because the male appeared to be observant of his surroundings and was constantly surveying all areas of the facility. The male's appearance was neat and clean with a closely cropped beard, short hair wearing blue jeans and a blue plaid shirt." The SAR goes on to describe how Mr. Razak, after studying entry/exit points moved to a part of the train station where the restrooms are located and eventually departed the train station with "a female wearing a white burka head dress" who had emerged from the restrooms. Office Gallardo concludes the SAR by requesting that it be forwarded to the fusion center in Orange County "for review and possible follow-up."

129. According to the SAR, Security Officer De La Rosa stated that "she received 'suspicious activity as related to terrorism training'" and that "the behavior depicted by the male was similar to examples shown in her training raising her suspicion and making the decision to notify the police." Mr. Razak is the subject of the SAR because of Defendants' trainings on their SAR reporting standards to state and local law enforcement and the private sector.

130. Mr. Razak was, indeed, at the Santa Ana Train Depot on May 16, 2011. The woman he was with was his mother. He had an appointment at the county employment resource center, which is located in the station building. He had not been to the station before and spent

some time locating the office before meeting up with his mother by the restrooms and leaving. His mother was wearing a hijab (head scarf), and not a burka.

131. Mr. Razak did not talk to any security officers at the Santa Ana Train Depot that day. The SAR notes the make and model of Mr. Razak's vehicle, and his license plate number. On information and belief, Security Officer De La Rosa followed Mr. Razak to his vehicle and wrote down his license plate number to identify him.

132. At no point while he was waiting in the Train Depot did Mr. Razak engage in conduct that gave rise to a reasonable suspicion of criminal activity.

133. This SAR falls into one or more of the behavioral categories identified in the Functional Standard, in particular, "Observation/Surveillance." Functional Standard 1.5 at 30; Functional Standard 1.5.5 at 49. It also falls under DOJ's "Potential Indicators of Terrorist Activities Related to Mass Transportation," which includes, among other things, "[u]nusual or prolonged interest in … [e]ntry points and access controls." It also falls under one or more behavioral categories identified by Defendant DOJ, such as the catch-all behavioral category of "acting suspiciously." The SAR about Mr. Razak was collected, maintained, and disseminated through a fusion center SAR database, and on information and belief has been uploaded to eGuardian and/or another national SAR database.

134. Because Mr. Razak is the subject of a SAR that falls under Defendants' standards for suspicious activity reporting, Mr. Razak has been automatically subjected to law enforcement scrutiny. That scrutiny may include but is not limited to scrutiny or interviews by any of the law enforcement agencies across the country that have access to the SAR about him.

135. Mr. Razak is deeply troubled by what may result from the collection, maintenance, and dissemination in a national database of a report describing him as engaging in suspicious activity with a potential nexus to terrorism.

136. Upon information and belief, the SAR about Mr. Razak is maintained and will continue to be maintained in one or more national SAR databases, where it can be accessed by law enforcement agencies across the country.

<u>5.</u> **<u>Aaron Conklin</u>**

137. Aaron Conklin resides in Vallejo, California. Mr. Conklin is a student at Diablo Valley College, studying graphic design. He is also an amateur photographer who posts his work online. Mr. Conklin has a strong aesthetic interest in photographing industrial architecture, including refineries.

138. In either 2011 or 2012, Mr. Conklin was photographing the Valero Refinery located in Benicia, California at around 10:00 p.m. He chose to photograph at night for aesthetic reasons, to capture the refinery illuminated against the dark night sky. Mr. Conklin set up in an empty lot where a food truck parks during the day, near a publicly accessible sidewalk and a bus stop. Mr. Conklin was positioned outside the refinery's fenced perimeter.

139. Despite Mr. Conklin's location outside the refinery's perimeter in a publicly accessible location, a private security guard from the refinery came out to tell Mr. Conklin that he could not photograph the refinery and issued stern warnings. Mr. Conklin felt threatened and feared that the situation would escalate if he remained, so he left. Because he fears further harassment, he has not returned to photograph the refinery, despite his desire to develop his portfolio with photographs of industrial sites.

140. Mr. Conklin later discovered that images of the refinery, taken from a similar location, were viewable on the internet through Google Maps, using the site's "street view" feature.

141. In or about November 2013, Mr. Conklin was attempting to photograph the Shell Refinery located in Martinez, California at approximately 9:30 or 10:00 pm. He wished to photograph the refinery at night for artistic reasons.

142. Mr. Conklin set up in the parking lot of a strip mall containing a smog testing center and a dance studio, across the street from the Shell Refinery's fenced perimeter.

143. As Mr. Conklin was preparing to photograph, a private security guard came out from the refinery and stopped him. At least one other guard from the refinery soon joined the first security guard. The security guards told Mr. Conklin that he was prohibited from photographing the refinery and that photographing the refinery was illegal and somehow connected to terrorism.

144. Despite Mr. Conklin's complete cooperation with the security guards, they called the Contra Costa County Sheriff's department, and at least two deputies arrived on the scene. The deputies searched through the pictures on Mr. Conklin's camera and searched his car. They also took pictures of Mr. Conklin, his camera equipment, and his vehicle. Mr. Conklin was afraid and felt as though he did not have the option to object to the searches without making matters worse for himself.

145. The deputies concluded by telling Mr. Conklin that he would have to be placed on an "NSA watch list." Only then was Mr. Conklin allowed to leave. The entire encounter lasted between forty-five minutes and an hour.

146. At no point while he was attempting to photograph the Valero or Shell refineries did Mr. Conklin engage in conduct that gave rise to a reasonable suspicion of criminal activity.

147. Taking photographs of infrastructure falls under one or more of the behavioral categories identified by Defendant PM-ISE as "suspicious," and also falls under one or more behavioral categories identified by Defendant DOJ, such as the catch-all behavioral category of "acting suspiciously." A Contra Costa deputy sheriff expressly told Mr. Conklin that he had to be put on an "NSA watchlist." On information and belief, Mr. Conklin is the subject of a SAR, which was collected, maintained, and disseminated through a fusion center SAR database, and uploaded to eGuardian and/or another national SAR database.

148. On information and belief, security guards at oil refineries are trained in Defendants' standards for SAR reporting. As a result, security guards at the Valero and Shell oil refineries prevented Mr. Conklin from taking photographs of sites of aesthetic interest to him. On information and belief, the Contra Costa deputy sheriffs are trained in Defendants' standards for SAR reporting. As a result, they detained and searched Mr. Conklin for doing nothing more than attempting to photograph a site of aesthetic interest from a public location, told Mr. Conklin that he had to be placed on a watchlist, and reported Mr. Conklin in a SAR.

149. Because Mr. Conklin is the subject of a SAR that falls under Defendants' standards for suspicious activity reporting, Mr. Conklin has been automatically subjected to law

enforcement scrutiny. That scrutiny may include but is not limited to scrutiny or interviews by any of the law enforcement agencies across the country that have access to the SAR about him.

150. Mr. Conklin was very upset by the encounter with private security and Contra Costa deputy sheriffs at the Shell refinery. He wants to continue taking photographs of industrial architecture in the future. But because of this event and the earlier incident at the Valero refinery, he is afraid to continue photographing industrial sites for fear of being stopped and questioned or, worse, arrested. Mr. Conklin has been chilled and has refrained from engaging in certain forms of photography, despite his desire to develop his photography portfolio. His inability to develop his photography portfolio limits his ability to apply successfully for jobs in his chosen field.

151. Mr. Conklin is also deeply troubled by what may result from the collection, maintenance, and dissemination in a national database of a report describing him as engaging in suspicious activity with a potential nexus to terrorism.

152. Mr. Conklin currently worries about being on a watchlist because he fears it will adversely impact him in the future. For example, he is concerned about his employment prospects if employers conduct background checks and he is flagged as someone with a potential connection to terrorism. Mr. Conklin also currently worries about being on a watchlist because he fears it will adversely impact his family. His father has worked and is seeking employment in the aviation industry and as a result must undergo rigorous background checks; Mr. Conklin is afraid about jeopardizing his father's career based on his own innocent efforts to take photographs of aesthetically interesting sites.

FIRST CLAIM FOR RELIEF

Violation of APA by Defendants DOJ and Loretta Lynch for Agency Action that is Arbitrary and Capricious and Not in Accordance with Law 5 U.S.C. §§ 702, 706(2)(A)

153. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

154. DOJ's promulgation of DOJ's SAR Standard constitutes final agency action.

155. DOJ and Loretta Lynch have issued a SAR Standard that sets forth operating principles for the collection, maintenance, and dissemination of "criminal intelligence information" within the meaning of 28 CFR Part 23. It applies to entities that operate arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination and analysis of criminal intelligence information. These entities and the systems they operate receive support from OJP and constitute "projects" and "criminal intelligence systems" within the meaning of 28 CFR Part 23.

156. Because DOJ's SAR standard is broader than 28 CFR Part 23 and authorizes the collection, maintenance, and dissemination of information even in the absence of reasonable suspicion of criminal activity, it conflicts with 28 CFR Part 23. DOJ has also undermined 28 CFR Part 23 by training participants in the NSI on DOJ's SAR Standard.

157. Defendants DOJ and Loretta Lynch have not provided a reasoned basis for adopting a conflicting standard.

158. Defendants' actions described herein were and are arbitrary, capricious, an abuse of discretion, and otherwise not in accordance with law, and should be set aside as unlawful pursuant to 5 U.S.C. § 706 (2012).

SECOND CLAIM FOR RELIEF

Violation of APA by Defendants PM-ISE and Kshemendra Paul for Agency Action that is Arbitrary and Capricious and Not in Accordance with Law 5 U.S.C. §§ 702, 706(2)(A)

159. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

160. PM-ISE's promulgation of the Functional Standard constitutes final agency action.

161. PM-ISE and Kshemendra Paul have issued a SAR Standard that sets forth operating principles for the collection, maintenance, and dissemination of "criminal intelligence information" within the meaning of 28 CFR Part 23. It applies to entities that operate arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination and analysis of criminal intelligence information. These entities and

the systems they operate receive support from OJP and constitute "projects" and "criminal intelligence systems" within the meaning of 28 CFR Part 23.

162. Because the Functional Standard is broader than 28 CFR Part 23 and authorizes the collection, maintenance, and dissemination of information even in the absence of reasonable suspicion of criminal activity, it conflicts with 28 CFR Part 23. PM-ISE has also undermined 28 CFR Part 23 by training participants in the NSI on the Functional Standard.

163. Defendants PM-ISE and Kshemendra Paul have not provided a reasoned basis for adopting a conflicting standard.

164. Defendants' actions described herein were and are arbitrary, capricious, an abuse of discretion, otherwise not in accordance with law and should be set aside as unlawful pursuant to 5 U.S.C. § 706 (2012).

THIRD CLAIM FOR RELIEF

Violation of APA by Defendants DOJ and Loretta Lynch
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 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 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, and any successor standard for SAR reporting that adopts a standard lower than "reasonable suspicion," is invalid and issue a permanent injunction requiring Defendants DOJ and LORETTA LYNCH to rescind DOJ's SAR Standard and cease and desist from training participants in the NSI in DOJ's SAR Standard.

2. Enter a declaratory judgment that PM-ISE's Functional Standard, and any successor standard for SAR reporting that adopts a standard lower than "reasonable suspicion," is invalid and issue a permanent injunction requiring Defendants PM-ISE and KSHEMENDRA PAUL to rescind the Functional Standard and cease and desist from training participants in the NSI in the Functional Standard.

3. Enter a declaratory judgment that 28 CFR Part 23 sets forth the standard for SAR reporting.

4. Enter a permanent injunction requiring Defendants to use 28 CFR Part 23 as the standard for SAR reporting.

5. Award Plaintiffs their costs and expenses, including reasonable attorneys' fees and expert witness fees; and

6. Award such further and additional relief as is just and proper.

DATED: August 25, 2015

Respectfully submitted,

By:___________*/s/ Linda Lye*______________

Linda Lye

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

MORGAN, LEWIS & BROCKIUS LLP
Stephen Scotch-Marmo (admitted *pro hac vice*)
stephen.scotch-marmo@morganlewis.com
Michael Abelson (admitted *pro hac vice*)
michael.abelson@morganlewis.com
101 Park Avenue,
New York, NY 10178
Tel: 212.309.6000
Fax: 212.309.6001
399 Park Avenue
New York, NY 10022

MORGAN, LEWIS & BROCKIUS LLP
Jeffrey Raskin (#169096)
jraskin@morganlewis.com
Nicole R. Sadler (#275333)
nsadler@morganlewis.com
Phillip Wiese (#291842)
pwiese@morganlewis.com
One Market Street, Spear Street Tower
San Francisco, CA 94105
Tel: 415.442.1000
Fax: 415.442.1001

AMERICAN CIVIL LIBERTIES UNION

FOUNDATION
Hina Shamsi (admitted *pro hac vice*)
hshamsi@aclu.org
Hugh Handeyside (admitted *pro hac vice*)
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

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