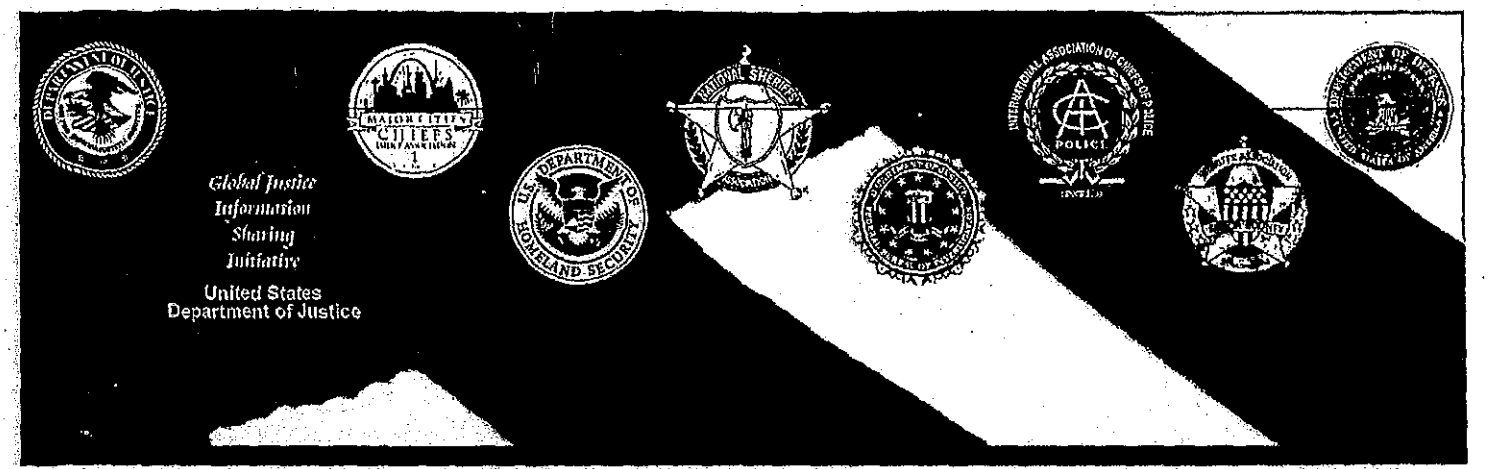


FINAL REPORT: INFORMATION SHARING ENVIRONMENT (ISE)-SUSPICIOUS ACTIVITY REPORT (SAR)

EVALUATION ENVIRONMENT

EGuardian-325

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

EGuardian-327

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. The ISE-SAR EE was designed to leverage existing operational processes, technology, policies, and systems to create a dynamic approach to information sharing.

INFORMATION SHARING: A NATIONAL PRIORITY

The recognized need to advance the sharing of terrorism-related law enforcement information was clearly articulated in the release of 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 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

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

EGuardian-328

process. It was developed for the analysis of SARs and includes the business rules for collecting, documenting, processing, and sharing terrorism-related suspicious activity information.[2] 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), is one of the methods by which information may be entered or discovered in the ISE-SAR Shared Spaces. 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.

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 technological configuration that allows data sharing through a distributed model which emphasizes the importance of maintaining the originating agency's ownership of the data. Additionally, this technological 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 technological 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

[2] A diagram of this process can be found in the Nationwide SAR Cycle chart located in Appendix ___.

on local agency-controlled servers from one central location—the National Criminal Intelligence Resource Center. The ISE-SAR Shared Spaces integrate the National Information Exchange Model standard and the ISE-SAR Functional Standard into a standardized process to efficiently and effectively share information.

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, 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. Further, in order to participate in the ISE-SAR EE and share information, all agencies had to develop a privacy policy 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. There must be 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 requires the ultimate determination as to the level of sharing of that information.

EGuardian-330

MULTILAYERED TRAINING

The design and implementation of a cohesive national ISE-SAR training program was a vital part 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 the 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.

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 proven 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

EGuardian-331

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, IACP, the FBI, the Criminal Intelligence Coordinating Council (CICC), and Global[3] have endorsed this project.

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. The ISE-SAR EE has proven 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
- Participating Agency Assessments
- Appendices:
  - Appendix One: Project Participants
  - Appendix Two: Project Timeline
  - Appendix Three: Acronyms and Abbreviations
- Contacts for Questions

[3] 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.

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. 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. 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. These 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. Consistent with the IRTPA, the ISE sought an information sharing solution that would allow

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

EGuardian-333

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.

> 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.'

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 the federal, state, and local communities. The information to be shared in this national network includes information based on an activity that most law enforcement agencies already do as part of their everyday activities: 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 sectors, the collection 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).

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

EGuardian-334

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). 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 behavior codes, business processes, and implementation procedures. 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, the Privacy and Civil Liberties Policy Development Guide and Implementation Templates, and the Privacy and Civil Liberties Implementation Manual for the Information Sharing Environment. 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 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 collecting, documenting, processing, and sharing terrorism-

EGuardian-335

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 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 success of the technology design and provided a viable tool for further applications. It is recommended that this project be revisited for potential deployment as soon as is feasible.

> 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 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, [5] 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 2007, a short-term study was conducted with some of the participants to determine the value of including personally indentifiable 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

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

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.

In early 2008, development began on the Findings and Recommendations of the Suspicious Activity Reporting (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 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 policy, 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 need for each participating agency to have a privacy policy. The group also advocated for continued project transparency through the inclusion of privacy and civil liberties advocates where feasible. Recommendations from the

> 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.'

EGuardian-337

training committee focused on the development of the three levels of training for the line officer, analyst, and executive.

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. Based on the finding at local law enforment agencies, 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 systems as they formalize the SAR process into the agency, allowing the agency to leverage existing operational processes, technology, policies, and protocols as the new SAR process is implemented.

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 the 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[6] have endorsed this project.

On December 23, 2008, the Nationwide SAR Initiative Concept of Operations[7] (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:

[6] 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 Major Cities Chiefs Association. This report was unanimously approved by the CICC in September 2008 and by the GAC in October 2008.

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

- 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 this 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.

Figure 1 describes the NSI process:

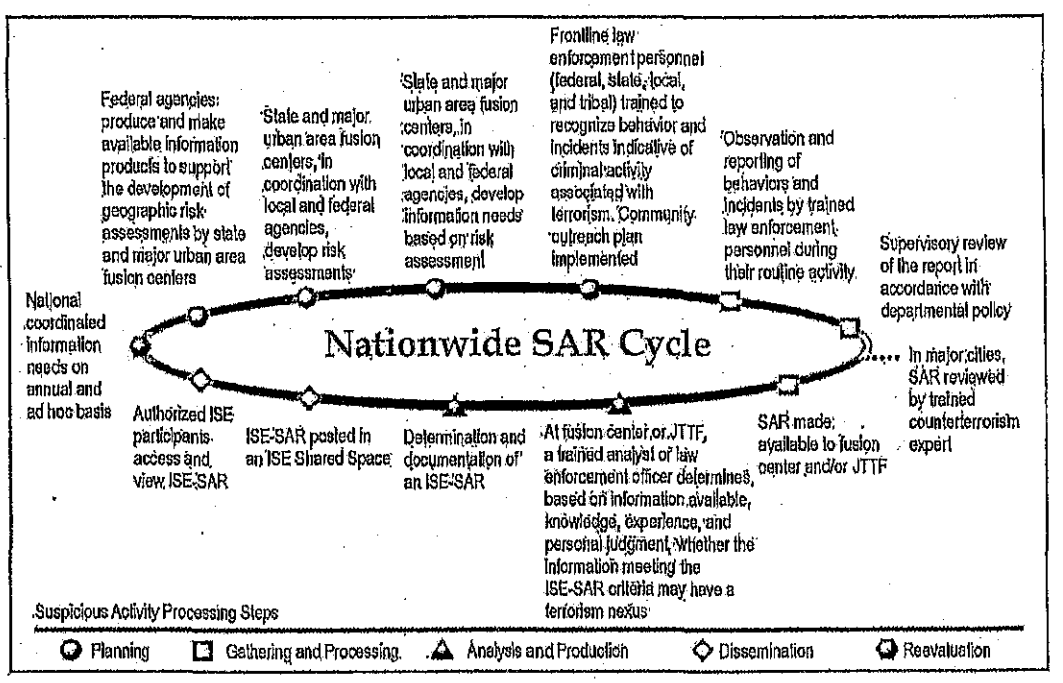


FIGURE 1.

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. This partial implementation was accompanied by training for the

first-line officers, executive leadership, and analysts within the fusion center. 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 into the final development stages of 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.

On January 9, 2009, the Information Sharing Environment (ISE)-Suspicious Activity Reporting (SAR) Evaluation Environment Implementation Guide (Implementation Guide), was issued after a collaborative effort with 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,[8] 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.

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

EGuardian-340

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.

ISE-SAR EE IMPLEMENTATION

The ISE-SAR EE, made up of 12 state and major urban area fusion centers, provides a relatively controlled environment to test the documented ISE-SAR policies, business process, capabilities, architecture, and standards. Additionally, the ISE-SAR EE allows for the assessment and refinement of processes and capabilities prior to full-scale operation. The objectives of the ISE-SAR EE include, but are not limited to, the following:[9]

- 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[10] 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 these pilot sites and potential future pilot site cities met in St. Louis, Missouri, to discuss the ISE-SAR EE. 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 policy development,

[9] 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).
[10] For additional information regarding the ISE Enterprise Architecture Framework, see http://www.ise.gov/pages/eaf.aspx.

EGuardian-341

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, training, and technology. Ultimately, building on the successes of the first Shared Spaces connections, the second phase expanded the project to other major law enforcement agencies and regional fusion centers, including Boston, Massachusetts (UASI); Chicago, Illinois (UASI); Houston, Texas (UASI); Las Vegas, Nevada (UASI); Los Angeles, California/JRIC (UASI/State); 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.[11]

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, with the goal of examining 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 section personnel report some kind of 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.

The ISE-SAR process, as outlined in the ISE-SAR Functional Standard, sets forth a four-part "integration/consolidation' process for identifying and collecting 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 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

[11] 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.

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.

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" for a report documenting such activity to be considered an ISE-SAR under this standard.

> 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.'

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.

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.[12] 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.

> 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.'

Data contained in reports designated as ISE-SARs derive from information gathered by source or reporting law enforcement organizations. Before the suspicious incident or behavior is documented in the first instance, entities 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.

The authors[13] of the Information Sharing Environment" Suspicious Activity Reporting Functional Standard and Evaluation Environment: Initial Privacy and Civil Liberties Analysis

[12] 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.

[13] 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.

(Version 1" September 2008)[14] recommend 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, printing, download, and exporting of SAR data is not allowed. 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.

PROTECTION OF PRIVACY RIGHTS AND CIVIL LIBERTIES

Throughout the ISE-SAR EE, safeguards were developed to ensure, to the greatest degree possible, that only information regarding individuals suspected to be involved in criminal activities associated with terrorism will be documented and shared. Aimed at protecting privacy rights and civil liberties, these safeguards are intended to avoid the gathering, documenting, processing, and sharing of information regarding race, ethnicity, national origin, or religious preference that has no reasonable relation to the criminal activity. In

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

accordance with this goal, subject-matter experts coordinated the review of 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.

> 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...'

During September 2008, the Information Sharing Environment" Suspicious Activity Reporting Functional Standard and Evaluation Environment: Initial Privacy and Civil Liberties Analysis was developed by 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, DHS, the FBI, and the Legal Issues Working Group of the ISE Privacy Guidelines Committee. Following this analysis, in January 2009, the ISE-SAR Evaluation Environment Privacy, Civil Rights, and Civil Liberties Protection Policy Template was developed in collaboration with the project partners and ISE privacy/ civil liberties officials. Based on the work of the Global's privacy document, ISE-SAR Evaluation Environment Privacy, Civil Rights, and Civil Liberties Protection Policy Template, the template is designed to cover all ISE-SAR EE activities conducted by participating pilot sites, including source, submitting, and use agencies. The template was designed to enable participating agencies to make any necessary modifications to include the requirements of their state constitution, executive orders, court decisions, statutes, rules and regulations, and local codes/ ordinances. To assist with the implementation of the template, a "Privacy Policy Template Sample Participation Agreement-Source Agencies' was developed. This sample participation agreement assists pilot ISE-SAR EE sites in developing agreements or memoranda documents for agencies that want to provide source documents to the sites for possible inclusion in the Shared Spaces.'

TRAINING

Training is a critical element of this project, and it is a vital component to 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.[15]

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.[16]

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 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 agencies within the ISE-SAR EE, training was also provided to representatives of 11 of the DHS components. Understanding the vital role the analysts/ investigators play in the SAR process, the Florida Department of Law Enforcement sponsored additional SAR analyst/ investigator training to 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. This online course will continued to be refined and rolled out to additional participants. 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.

To continue the theme of transparency and openness, the American Civil Liberties Union and other privacy advocates were invited to review the training as it was developed. The

[15]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.

[16]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. EGuardian-347

input from these advocates provided significant enhancements and improvements of the overall SAR training programs.

TECHNOLOGY

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 utilizes a distributed data model to operate its Shared Spaces and make terrorism-related information available through Common Terrorism Information Sharing Standards, applications, and Web Services. 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. During the deployment of each Shared Spaces environment, fusion center information technology and security staff reviewed several installation options and selected an option that was consistent with local network security guidelines and technology preferences. 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, 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. Each participating agency is linked to create an encrypted tunnel using the VPN technology delivering the information between sites in a secure manner.

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

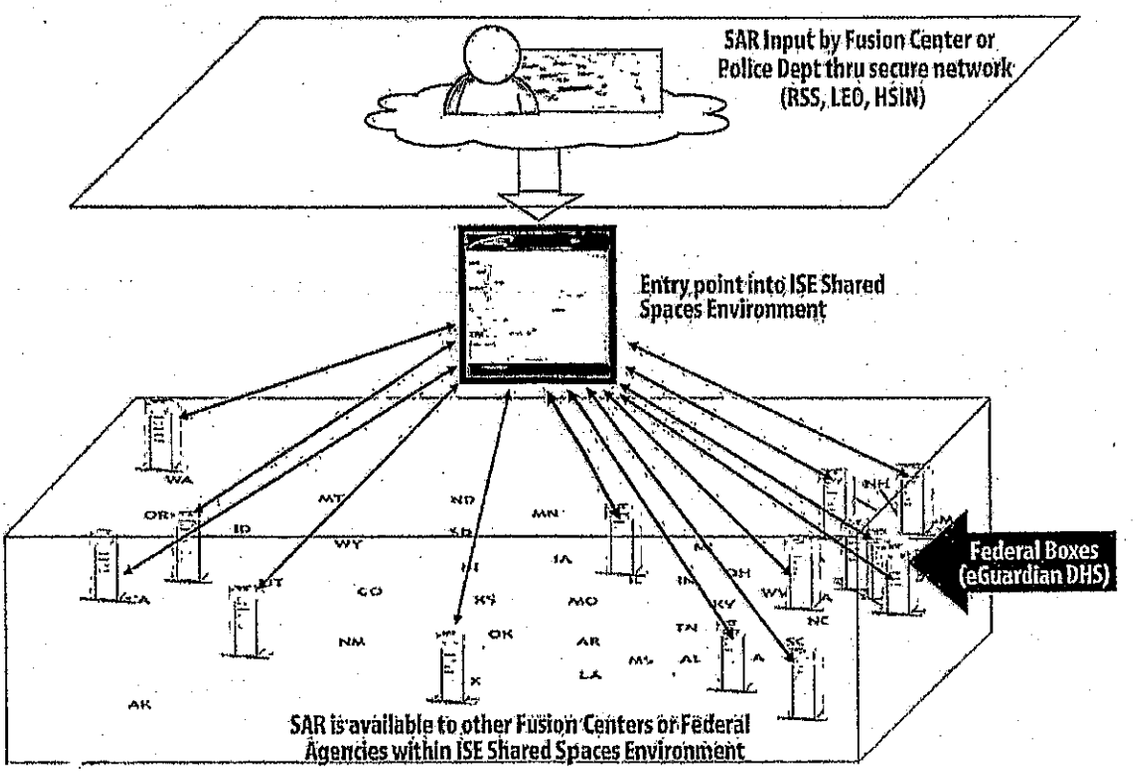


FIGURE 2

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. This sgment achitecture 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.[17]

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

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

EGuardian-349

- 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.

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 DOJ-supported Regional Information Sharing Systems® Secure Intranet (RISSNET™), the FBI-supported Law Enforcement Online, and DHS-supported Homeland Security Information Network, 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.

EGuardian-350

- 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.
- Forcing 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.

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 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 assess 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 was 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, there were numerous partner meetings and conference calls held to ensure partner collaboration and project awareness.

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

EGuardian-352

The federal project sponsors were tantamount 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

Blending the 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.

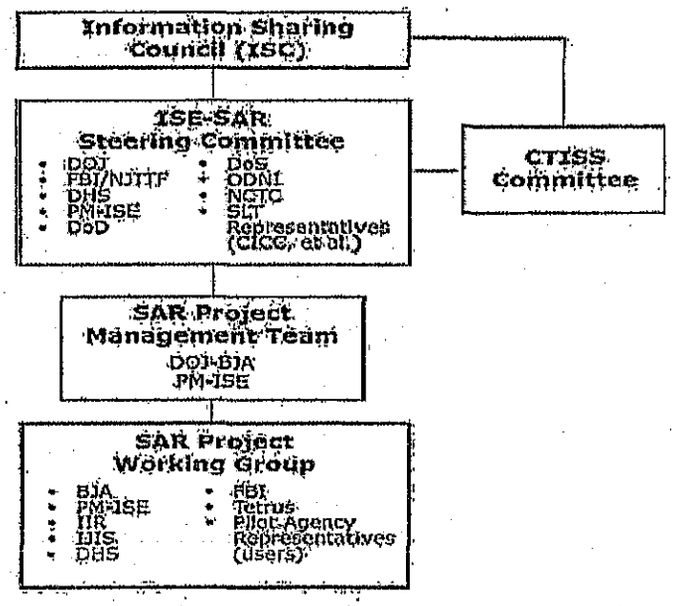
The support mechanism in place for the ISE-SAR EE included a Steering Committee, which provided strategic direction for the project. The committee synchronized interagency activities, resolves major issues, and addresses resource needs. It is charged with developing ISE-SAR policies and practices, addressing 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.

EGuardian-353

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, the ISE SAR Steering Committee.

The following graphic depicts the SAR Governance Structure:



PERFORMANCE MEASURES

The supporting data for the following observations came from several sources. Sites were asked to share statistics on internal SAR processes, including the number of SARs collected, vetted, and posted to the Shared Spaces. Another set of data came from the Shared Space server recording transactional information such as the number of users and search activity. Finally, interviews were conducted with each site at the beginning and end of the evaluation to provide a complete operational picture.

PROCESSES FOR REPORTING, PROCESSING, ANALYZING, AND SHARING SAR INFORMATION

A foundational process step is the ability to apply criteria in a manner that discriminates between SARs and those with a terrorism nexus, known as ISE-SARs. The sites were asked to track the number of total SARs collected prior to and during the evaluation as well as the

EGuardian-354

number of ISE-SARs that were produced from the whole. This is a key performance indicator that confirms that the appropriate training and operational steps have occurred previously to establish the means to identify and report suspicious behavior to the authorities and for the reports to be codified and made available to the fusion center.

Two examples illustrate this capability by vetting their previously collected SAR records together with those SARs received during the evaluation.

- Florida Department of Law Enforcement (FDLE): Over the course of the evaluation, FDLE vetted 5,727 SARs (most predating the evaluation) and identified 12 ISE-SARs.
- Virginia Fusion Center (VFC): Over the course of the evaluation, VFC vetted 347 SARs and identified 7 ISE-SARs.

Both FDLE and VFC were able to apply the ISE-SAR vetting criteria, while meeting privacy and civil liberties protections requirements, and select analytically useful ISE-SARs with a potential nexus to terrorism. These ISE-SARs were then placed and accessible in the Shared Spaces.

Once the ISE-SARs were posted to the Shared Spaces, the site team examined how the searches were being conducted. Two points of interest emerged: most searches were equally against all servers in the Shared Spaces and the number of queries increased steadily from August.

Looking at the number of queries directed to each site's server, nearly all searches tended to be directed equally to all Shared Spaces sites, though each query could be directed to one or more sites. Figure 3, below, illustrates each operational SAR server receiving similar numbers of queries. Conversely, if sites chose to drill into a single site's data (their own or others), the query counts would show greater variability and not line up as they had.

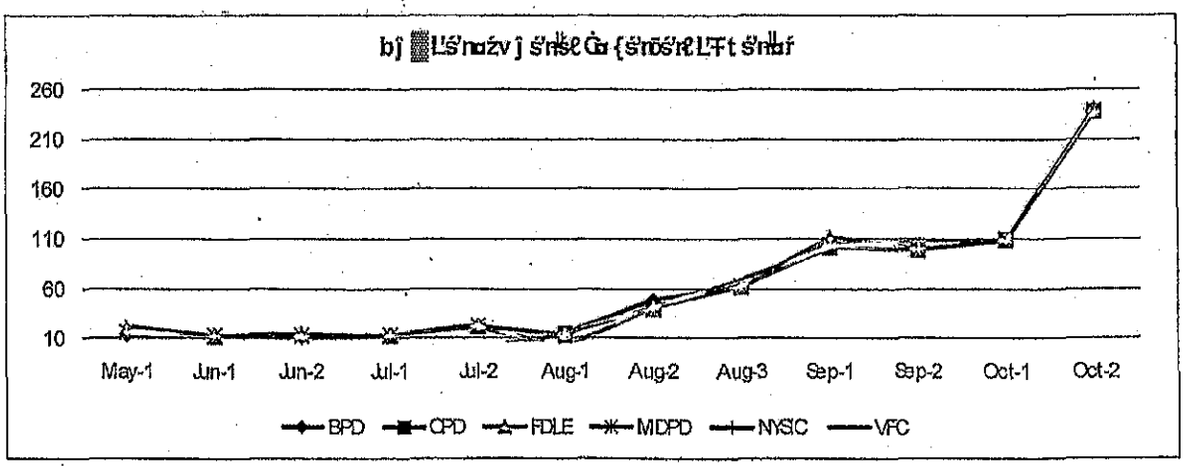


FIGURE 3

EGuardian-355

There was a steady increase in search activity beginning in August that remained fairly constant into October. It turned out that most of this growth may be attributed to the increase in number of users receiving search access to the Shared Spaces. The data indicates that Boston, FDLE, New York, and Virginia had the most significant increase in users. When compared to the number of searches produced by these four sites, all showed an increase, but FDLE showed a significant and sustained increase from the end of August.

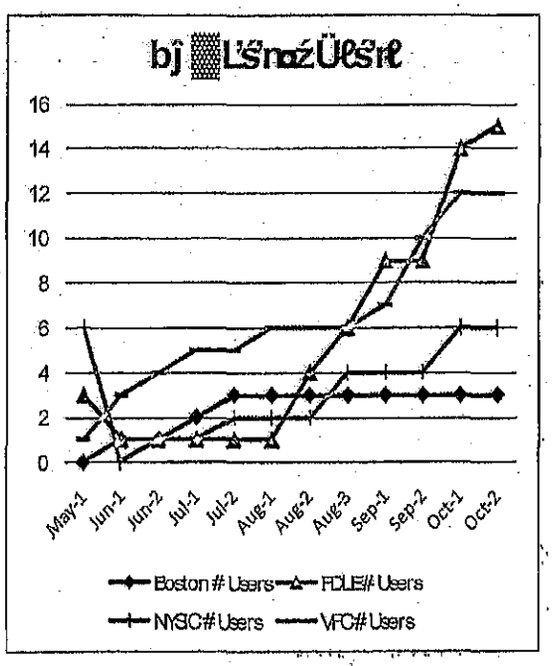


FIGURE 4

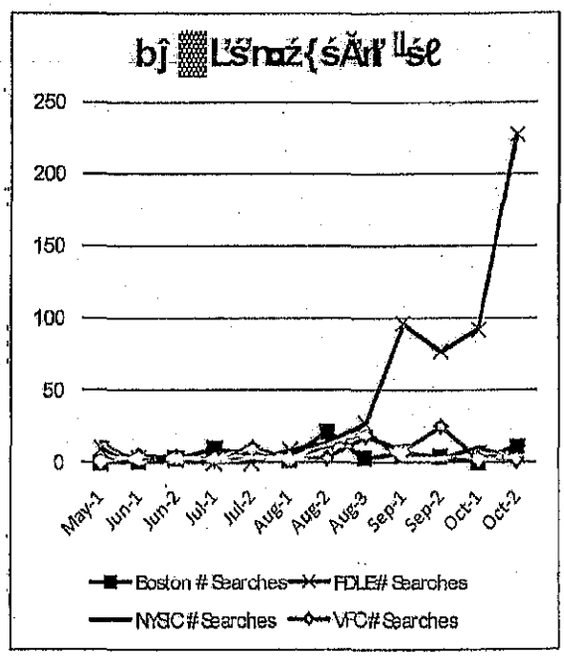


FIGURE 5

The increase in queries, above, is consistent with the increase in users. Sites at Boston, FDLE, New York, and Virginia showed increases in users granted access to the SAR Shared Spaces, as depicted in Figure 4. When reviewing the search activity of these users, Boston and New York remained fairly constant, while Virginia and especially FDLE showed increases in search activity (Figure 5).

It was learned through an interview that FDLE's significant difference may be attributed to the fact that it has updated its Standard Operating Procedures to include the Shared Spaces as one of FDLE's required systems to search as a routine part of analysts' indices checks. This provides an example of how the implementing policy can lead to sustained levels of activity.

RESULTS OBSERVED

At the beginning of the evaluation, a number of metrics were selected that were indicative of the SAR process working effectively. These include investigations, arrests, preparedness

activities, and analytical products and were collected through two surveys administered to the evaluation sites. Five sites were able to report some results statistics.

The following are the observations:

- Four of the five were able to report the number of federal investigations initiated as a result of ISE-SARs.
- Three sites were able to report on the number of local investigations initiated as a result of ISE- SARs.
- Two sites were able to report on the number of local or federal investigations that led to arrests or convictions in cases involving ISE-SARs.
- Two 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 results data are all major urban area fusion centers. By function, these fusion centers work closely with the officers and detectives investigating SARs in their jurisdiction and may have more ready access to such information. For instance, in Washington DC, detectives investigating four SARs received at the fusion center led to the arrest of an individual for producing 25 bomb threats. Several other sites produce analytic products, though only Los Angeles and Washington, DC, provided statistics on the number produced.

It became apparent during the evaluation that collecting information through surveys was challenging. In many cases, sites did not have the automated ability to report on SAR activity in the steps prior to posting in the Shared Spaces or after in analytical and law enforcement activities. Use of the Shared Spaces, however, provided us with an automated feed of the transactional activity of each site. Future measurement activity should focus on improving the means to collect automated reporting information.

EGuardian-357

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 the 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 implications to 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.[18]

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

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

EGuardian-359

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 Committee (PGC)[19] 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.

[19] 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.

EGuardian-361

Recommendation 1: 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.

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 establish 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 policy 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.

EGuardian-362

Recommendation 2: Agencies should ensure transparency and openness in their privacy policy 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 that 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.

EGuardian-363

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: Due to 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.

EGuardian-364

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 collecting, 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.

EGuardian-365

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: 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.

EGuardian-366

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 the agencies to enter their SAR data (either manually or by automated interfaces to existing legacy systems) into the tool and use the SVT 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 Mangager 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. Futher 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 tools would be beneficial; however, due to 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

EGuardian-368

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

EGuardian-369

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;[20] the Los Angeles Police

[20] 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.

EGuardian-370

Department's iWATCH program;[21] 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 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 FLOs 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 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 a TLO program 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

[21] More information about the iWatch program can be found at www.iwatchla.org.

EGuardian-371

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.

EGuardian-372

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,[22] 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 Specification (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 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.

[22] Including the 12 sites, eGuardian, and DHS.

EGuardian-373

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 record 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).

EGuardian-375

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: Efforts should be made to 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.

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.

EGuardian-376

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 where 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 with not only 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.

EGuardian-378

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 Spaces 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.

EGuardian-379

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.

EGuardian-380

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.

EGuardian-381

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

EGuardian-382

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 a 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).

EGuardian-384

- 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. 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. Additionally, the model was built from the foundational elements of the Global Justice XML Data Model, its companion documents, training, and technical support mechanisms.

EGuardian-385

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 policy 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

EGuardian-386

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 SAR TRAINING PROGRAM

Training was recognized as critical to the successful implementation of the Nationwide SAR Initiative. The ISE-SAR Functional Standard outlined a new set of protocols and standards that would need to be utilized by law enforcement before SAR information could 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 a terrorism indicator training program for private sector personnel, including oil industry officials, and will be delivering the training to all private sector infrastructure owners.

EGuardian-387

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.

EGuardian-388

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

EGuardian-389

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.
>
> EGuardian-390

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 extensive outreach program with the public and has conducted community meetings, trained members on the Crime Stoppers program, and coordinated with the Houston-area FBI's tip hotline, which 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.

EGuardian-391

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

EGuardian-392

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 National Conference
  - Major City 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

EGuardian-393

- 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 to successfully implementing an agency-wide process to ensure that all agency members understand their role in collecting 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 Intelligence Bureau, 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. Per this order, all terrorism-related information is routed to the fusion center. The fusion center has a process

EGuardian-394

in place to review all SAR data consistent with the agency's privacy policy. 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

EGuardian-395

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 where 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.

EGuardian-396

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 collecting 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

EGuardian-397

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.

EGuardian-398

Arizona Counter Terrorism Information Center

SAR PROCESS REPORT" POSTIMPLEMENTATION 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.[23] 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 TIP entry is made, it is electronically sent to an investigative supervisor who reviews the

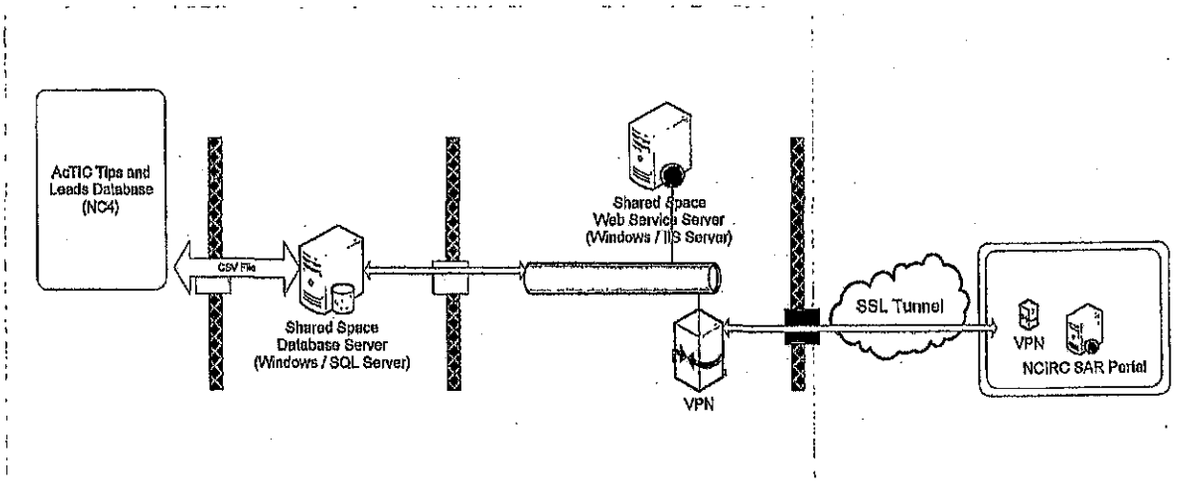
[23] The Fusion Center Privacy Policy Development Technical Assistance course is offered through the DHS/DOJ Fusion Process Technical Assistance Program and Services. EGuardian-400

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.



EGuardian-401

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

EGuardian-402

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.
- It is recommended that a national users group 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.
- It is recommended that a national legal office for this initiative be established to protect the data being collected and to address concerns raised by the American Civil Liberties Union and other privacy advocates.
- It is recommended that agencies receive training, technical support, and funding for the servers during this initiative.

EGuardian-403

Boston, Massachusetts, Police Department

SAR Process Report" Postimplementation 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 eight 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

EGuardian-404

occurred between BRIC and the Massachusetts Commonwealth Fusion Center[24] 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

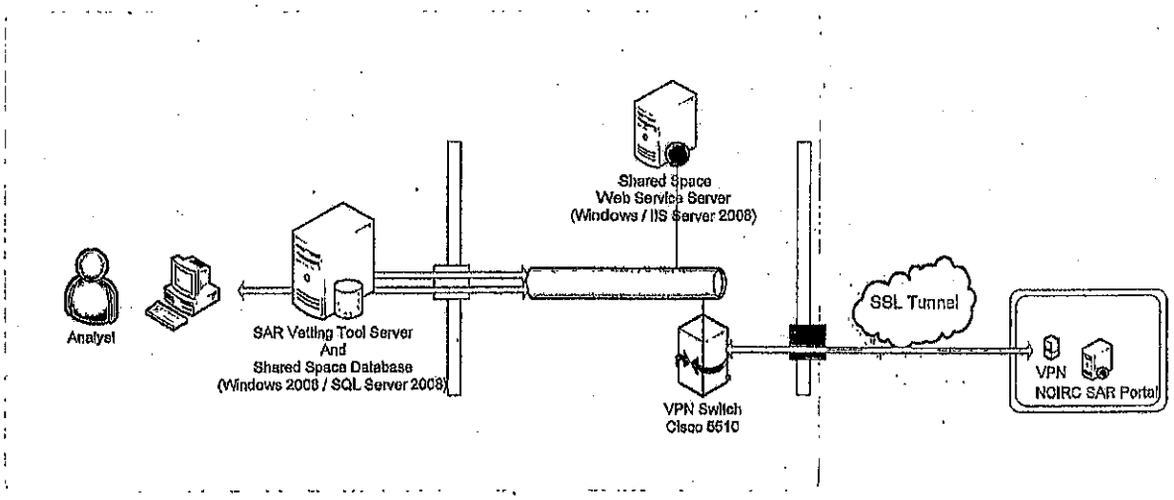
Prior to the ISE-SAR EE, BRIC's technical process included an in-house-designed data warehouse solution with an interface to the Environmental Systems Research Institute, Inc. (ESRI), geographic information system software application. Each night, all incident data, including potential SARs, is loaded 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.

[24] The state-designated fusion center, as determined by the Federal Bureau of Investigation (FBI) and the U.S. Department of Homeland Security (DHS).

EGuardian-405

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 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 EGuardian-407

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.
  - It is recommended that the national program office be located within DHS's State and Local Program Office, not within the FBI.
- It is recommended that there 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.
- It is recommended that a national legal office not be created. Multiple legal resources already exist for law enforcement agencies at all levels of the government.
- It is recommended that a "daily digest" 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.
- It is recommended that the appropriate threshold 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.

EGuardian-408

Chicago, Illinois, Police Department

SAR Process Report" Postimplementation 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 EGuardian-409

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.

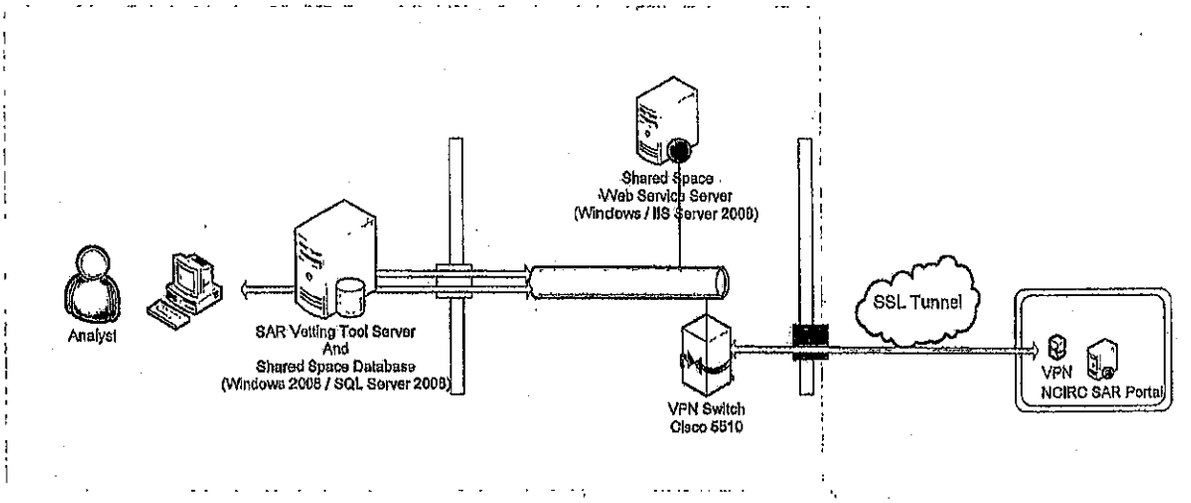
During the ISE-SAR EE, CPD continued to use the same SAR mechanisms that were used prior to the ISE-SAR EE. However, CPD created a multilayer review process for reviewing and vetting SARs and moving them to the ISE-SAR Shared Spaces. The department requested use of the SAR Vetting Tool (SVT) to input 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:

EGuardian-410



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).

EGuardian-411

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.

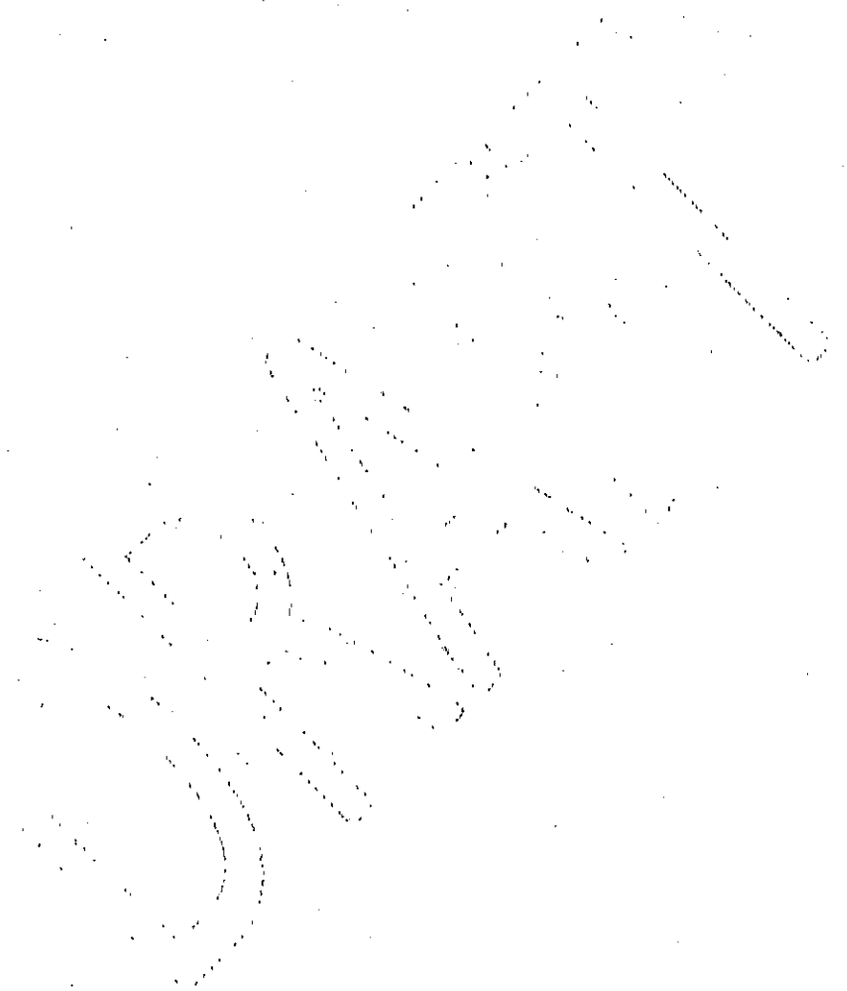
Project Recommendations From the Chicago Police Department

There needs to be some federal level coordination; however, there does not need to be a national program office. 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.

EGuardian-412

- 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.



EGuardian-413

Florida Department of Law Enforcement

SAR Process Report" Postimplementation 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[25]). Before this initiative, tips/SARs were initially reviewed by analysts within the Counter-Terrorism Intelligence Center (CTIC)[26]

[25] InSite is the statewide intelligence system.
[26] CTIC is a component of the FFC.

EGuardian-414

to determine their disposition, forwarded to appropriate agencies, and used to produce intelligence products, as necessary.

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

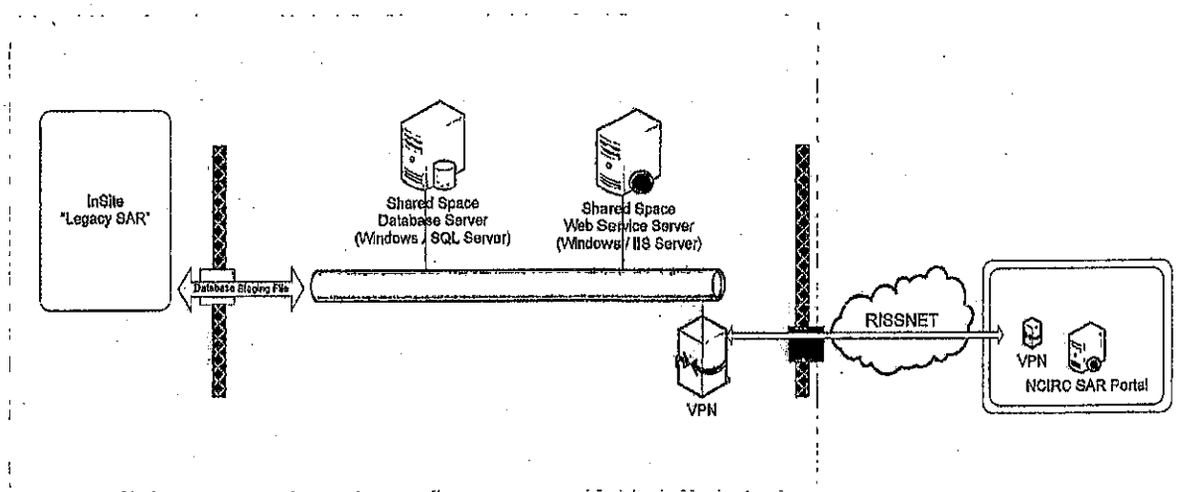
FDLE uses an intelligence system called InSite that is provided by ACISS Systems, Inc. InSite has multiple modules, including a case management application that is used to track SARs.

EGuardian-415

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.[27]

[27] Individuals who have access to InSite are required to receive training on the system.

EGuardian-416

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.[28] 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.

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 into 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.

[28] 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.

EGuardian-417

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.

EGuardian-418

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.

EGuardian-419

Houston, Texas, Police Department

SAR Process Report" Postimplementation 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.[29] 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

[29] A copy of the General Order is available upon request. EGuardian-420

analyze SAR data within the department. Prior to the ISE-SAR EE, the HRISC did not use the 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.

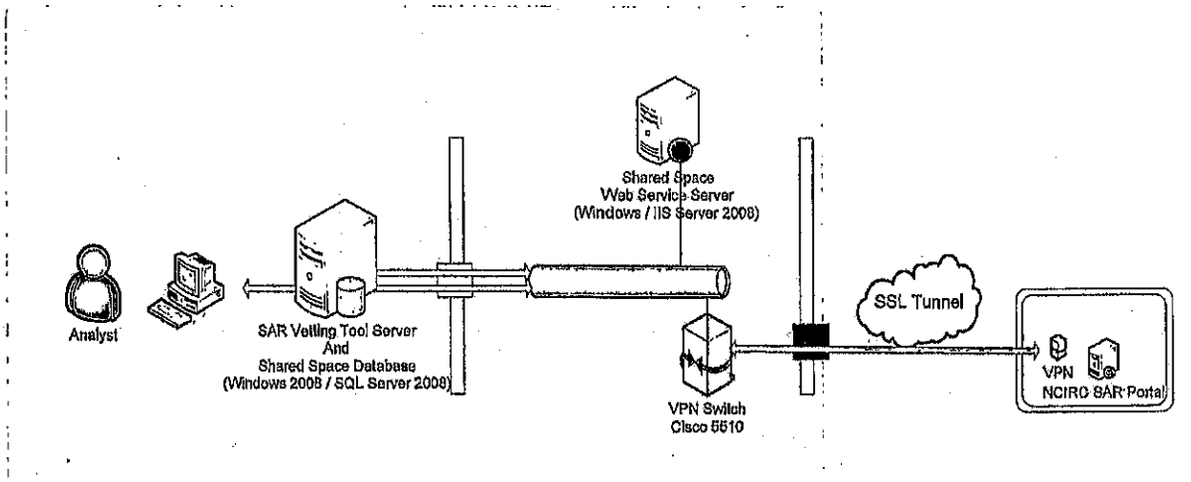
During the ISE-SAR EE, HPD adopted the behavior-specific codes specified in the ISE-SAR Functional Standard. The command staff decided that they would continue to use their previous "Investigative CID' report because of its comprehensiveness and familiarity to the officers. The department has created 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 a 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.

EGuardian-421



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.[30] The SAR analyst/investigator course was delivered in March 2009, and 32 individuals received the training from eight 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

[30] The CEOB was previously discussed in the Executive Leadership section.

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.

Outreach to the Public

Prior to the ISE-SAR EE, HRISC had an extensive 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 the state legislature, 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. In addition, the assistant chief has briefed other members of the HPD command staff and appropriate outside entities on the ISE-SAR EE. 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.

EGuardian-423

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 being 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 are trying to share information.

Additional Comments

The privacy policy template for the project was longer than the HPD attorneys felt was needed. In addition, the template was particularly troublesome in that if it is read literally, every person who enters the center" regardless of role or responsibility" must have a full background check and be briefed on privacy issues.

EGuardian-424

Las Vegas, Nevada, Metropolitan Police Department

SAR Process Report" Postimplementation 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.

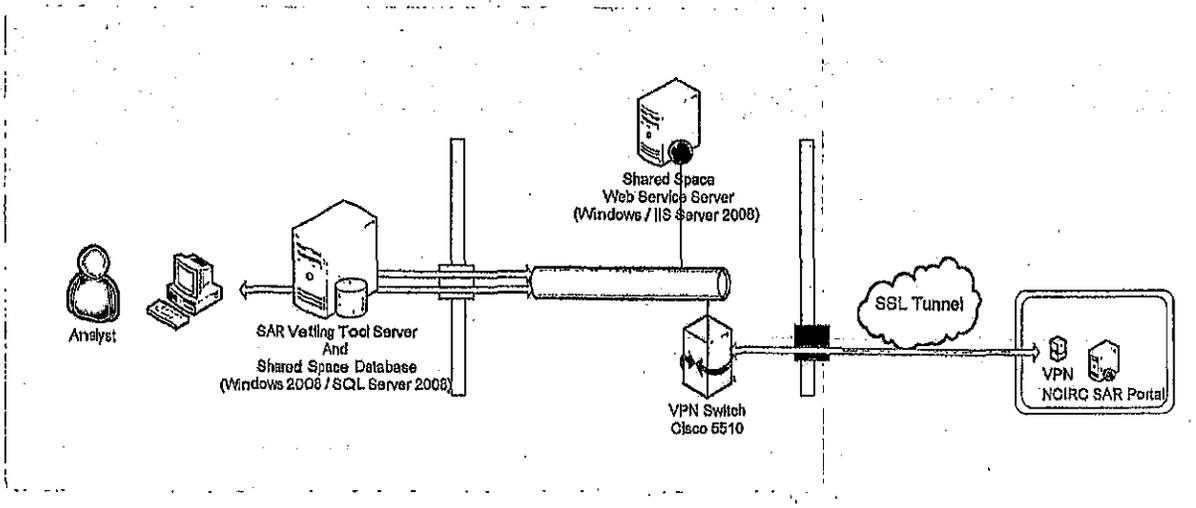
During the ISE-SAR, the LVMPD received the MCCA's Chief Executive Officer Briefing in March 2009, and 24 command staff personnel from approximately eight law enforcement agencies participated.

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

EGuardian-425



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.

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 enble 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.

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.[31] 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[32] 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.

[31] The LVPD press release is available at http://www.lvmpd.com/news/pdfs/2008/011808release.pdf.
[32] The SAR form is available at http://www.lvmpd.com/pdf/SAR_form.pdf.

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 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.

EGuardian-429

- 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" Postimplementation 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

EGuardian-431

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.[33]

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

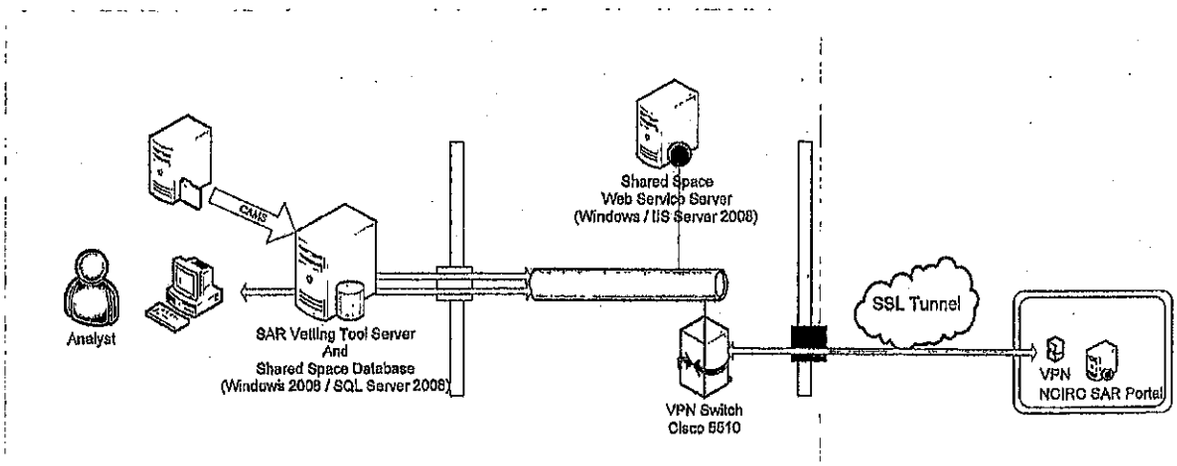
[33] This is a regionally based FBI counterterrorism squad located in a command center in Norwalk, California, and is responsible for protecting seven counties and 18 million people. The CT-6 Unit was created in May 2004 after a series of reported threats diverted too much manpower from other counterterrorism investigators. EGuardian-432

entered into the SAR Vetting Tool (SVT) by trained analysts in the SAR Unit and moved to the 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.



EGuardian-433

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[34] 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.[35] 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

EGuardian-435

[34] See www.iwatchla.org.

[35] The Web site may be applied nationally for other agencies to utilize in their SAR processes.

has built a regional awareness of SARs and provides training to local law enforcement 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.[36]

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; DHS Federal Air Marshal Service; the California State Board of Equalization;[37] 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.

[36] All of the regional fusion centers in California are connected to the state fusion center.
[37] 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.

EGuardian-436

- There should be a national training program for the SAR process.
- 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 as a crime report to ensure that it gets the attention and proper emphasis needed.

Miami-Dade, Florida, Police Department

SAR Process Report" Postimplementation 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, Florida, Police Department (MDPD) Homeland Security Bureau's (HSB) 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." 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 directive was 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 HSB.

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 HSB, which served as the collection point for all SARs within the department. Officers were also encouraged to call HSB to inform the center of the suspicious activity notated in their reports. HSB utilized an online form located on the South Florida Virtual Fusion Center[38] 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 Virtual Fusion Center, and if there is a terrorism nexus, the Joint Terrorism Task Force (JTTF)

[38] The South Florida Virtual Fusion Center is a collaboration site that allows government agencies from the South Florida area to post and share information. EGuardian-438

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 HSB, and it has adopted the behavior-specific codes specified in the ISE-SAR Functional Standard. HSB is utilizing the SAR Vetting Tool (SVT) provided by the NSI to retrieve and analyze SARs.

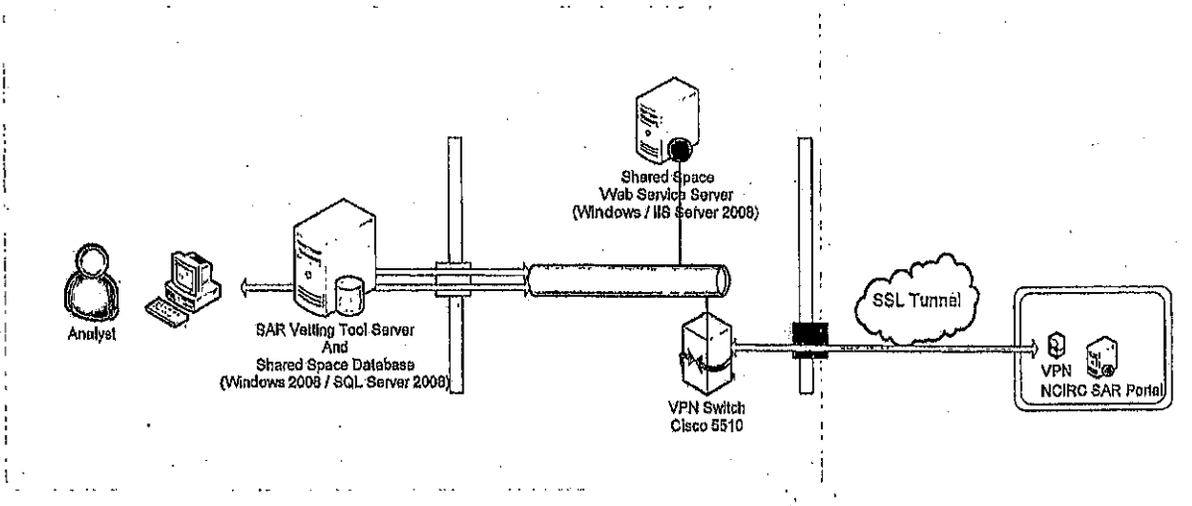
During the ISE-SAR EE, the center developed a multilayer review and vetting process to identify SARs. Once the initial report is submitted, a field supervisor reviews the report to ensure accuracy and appropriateness of the report. Once it is sent to HSB, it is immediately reviewed by an analyst and 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 HSB 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. HSB maintains the same process prior to the ISE-SAR EE for forwarding SARs to local, state, and federal agencies.

During the ISE-SAR EE, HSB 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 HSB'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.

EGuardian-439



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, HSB provided SAR roll call training to more than 1,100 officers within the department. In addition, HSB 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.[39]

INSTITUTIONALIZATION OF THE SAR PROCESS

Prior to the ISE-SAR EE, MDPD had several institutionalization efforts of the SAR process within the department. 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. HSB 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. HSB released alerts, warnings, and notifications as necessary.

[39] For example, training was developed for airport maintenance personnel to look for suspicious activity based upon the analysis of SAR information received.

EGuardian-440

During the ISE-SAR EE, MDPD continued its aforementioned efforts to institutionalize the SAR process throughout the department.

Outreach to the Public

Prior to the ISE-SAR EE, MDPS developed Seven Signs of Terrorism DVDs and CDs and distributed them to surrounding agencies and private sector entities.[40] 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, HSB was a U.S. Department of Homeland Security (DHS)-recognized fusion center and has a representative and an analyst from DHS assigned to the center. Additional center personnel include a JTTF representative and three full-time public safety personnel. HSB also partners with surrounding government agencies via the South Florida Virtual Fusion Center.

HSB can access the Regional Information Sharing Systems Secure Intranet (RISSNET), the Federal Bureau of Investigation's (FBI) Law Enforcement Online, and the Homeland Security Information Network but does not utilize these systems. HSB can also access the state's criminal justice network and intelligence database but does not post intelligence to them. HSB 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 program. In addition, MDPD has a working relationship with all the major private security operations in South Florida.

[40] The video is also available on the MDFC Web site at http://www.miamidade.gov/mdpd/BureausDivisions/bureau_Hls.asp.

EGuardian-441

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. HSB 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.
  - The national program office should not be located within the FBI but with an uninvolved third-party agency.
- 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.

EGuardian-442

New York State Police

SAR Process Report" Postimplementation 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, located in the NYSP Manual under "Article 30D: NYSP Law Enforcement Field Interview Card,' there is a section 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 collecting 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.

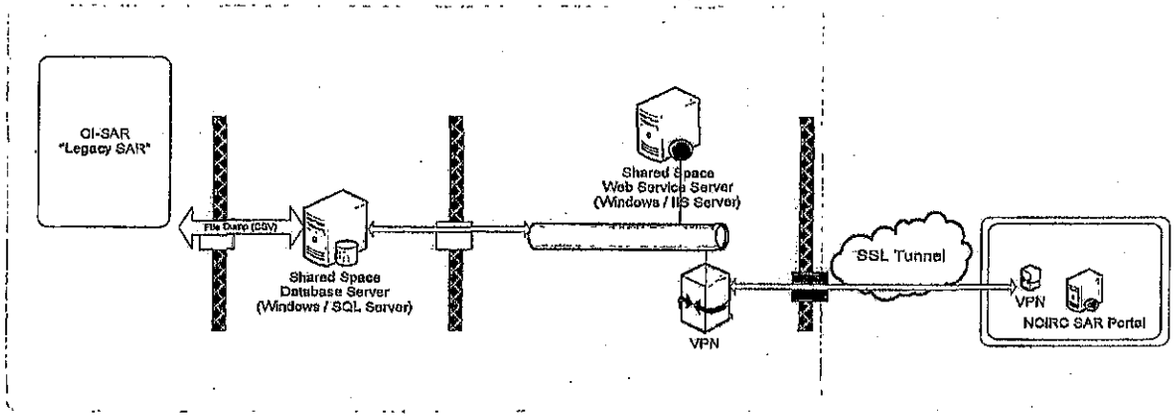
During the ISE-SAR EE, NYSIC adopted the behavior-specific codes located in the ISE-SAR Functional Standard and developed and implemented a privacy policy regarding the reporting of suspicious activity that meets the applicable requirements of the ISE Privacy Guidelines. In order to protect the information 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 described earlier.

EGuardian-444



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.[41] 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.

[41] The New York OHS Web site address is http://www.security.state.ny.us.

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.

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.

EGuardian-447

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" Postimplementation 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 collecting 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,

EGuardian-449

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.

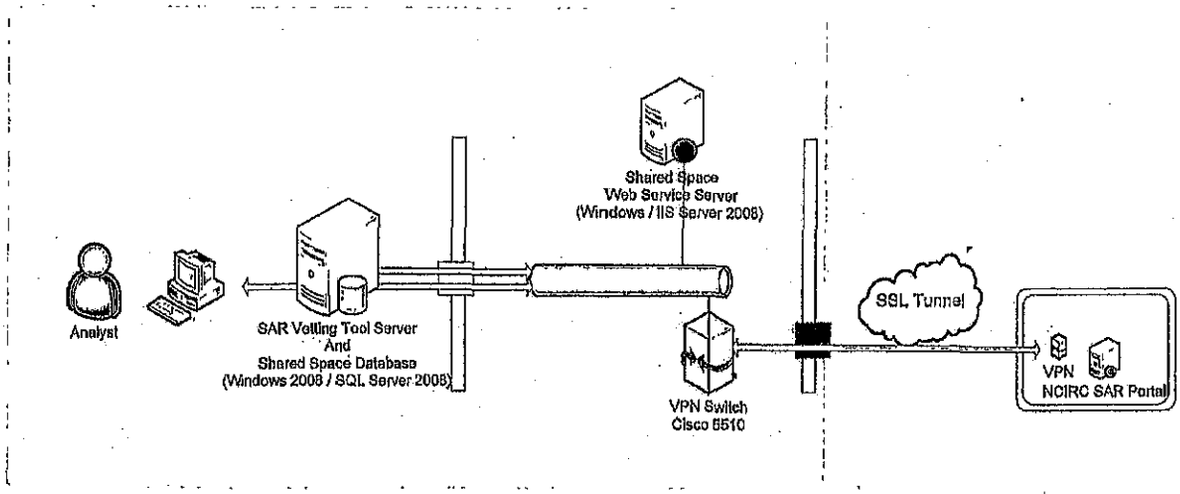
During the ISE-SAR EE, a multilayer review process was established to identify ISE-SARs within 24 hours. SARs that are submitted to Seattle PD are reviewed by CIB and then sent to WSFC for review and analysis. Once the fusion center determines that the information has a nexus to terrorism, the ISE-SAR 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.

EGuardian-450



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,[42] and Seattle PD supports those efforts. Seattle PD also supports the Northwest Warning, Alert and Response Network (NWWARN), 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.

[42] The link to the Seattle Emergency Management public Web site is http://www.seattle.gov/emergency/hazards/terrorism.htm.

EGuardian-452

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 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" Postimplementation 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[43] 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.[44] 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 Northern Virginia Urban Areas Security Initiative fusion center

[43] Intelligence reports are sent to VFC either electronically or in hard copy.
[44] The Web site is located at http://www.vsp.state.va.us/ FusionCenter/ Index.shtm.

EGuardian-454

as well as the Joint Terrorism Task Force. VFC works closely with all local jurisdictions to share SAR information throughout Virginia and the National Capital Region Intelligence Center located in Fairfax, Virginia, as well as jurisdictions in Washington, DC, and the Maryland area.

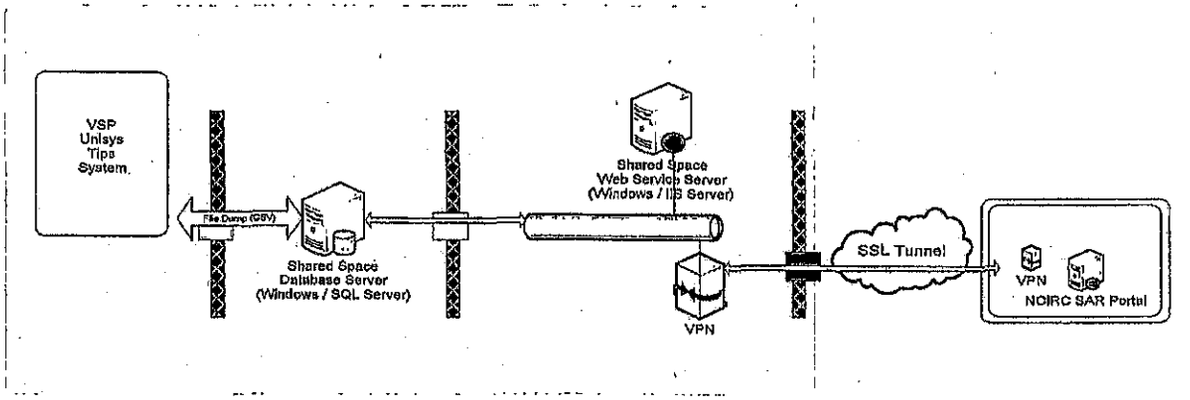
Because of its robust SAR process prior to the ISE-SAR EE, VSP had only minor enhancements to its SAR process as it implemented this project. The center adopted and modified its current report to comply with the behavior-specific codes located in the ISE-SAR Functional Standard; however, not all codes 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.

EGuardian-455



TRAINING

VFC conducts numerous terrorism awareness training events throughout the state of Virginia; however, no specific training on the reporting of suspicious activity existed 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.[45] 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.

[45] The line officer training is under development, and VFC worked with the IACP during the pilot phase of the training.

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 FBI 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.

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.[46] 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 hosted five analysts from the public safety/emergency management sector 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 more than 200 military points of contact. Additionally, two U.S. Army National Guard representatives are 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

[46] The Sevens Signs of Terrorism is available at http://www.vsp.state.va.us/FusionCenter/7-Signs.shtm.

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 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, the Federal Emergency Management Agency, 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.

EGuardian-458

- 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" Postimplementation 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

EGuardian-460

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[47] 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.

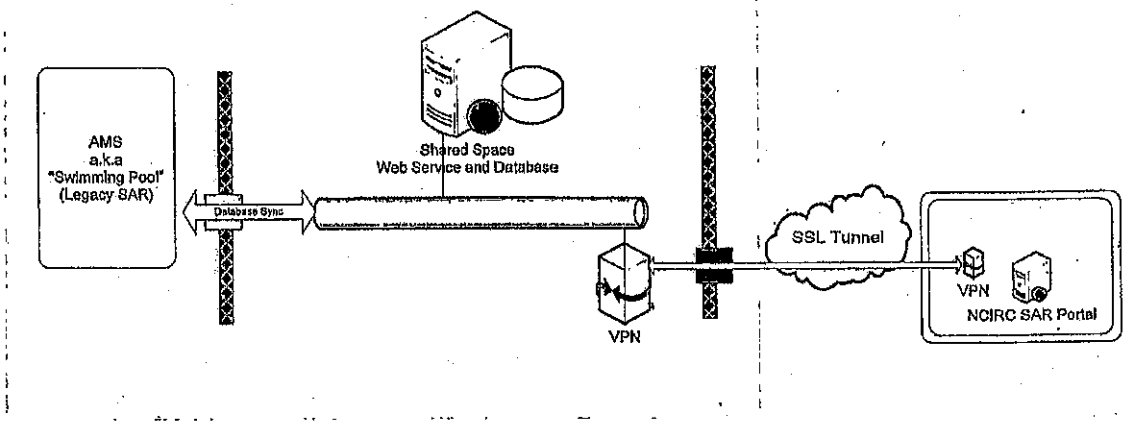
During the ISE-SAR EE, MPD indicated that it had developed a privacy and civil liberties policy regarding the SAR process; however, the policy is in the MPD legal office and has not been made available for review to determine whether the policy meets the applicable requirements of the ISE Privacy Guidelines. Once the privacy policy meets the applicable requirements, SARs will be entered into the ISE-SAR Shared Spaces for sharing with other urban area, regional, and statewide fusion centers and the Joint Terrorism Task Force (JTTF). 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.

[47] The MPD central repository is also referred to as the "swimming pool.'

EGuardian-461

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 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,[48] the SAR analyst/investigator course, and the line officer training. The SAR analyst/investigator course was delivered in

[48] The CEOB was previously discussed in the Executive Leadership section.

December 2008, and 15 individuals received the training from six agencies 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 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 are in the process of securing a domain name for this program.

EGuardian-463

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.

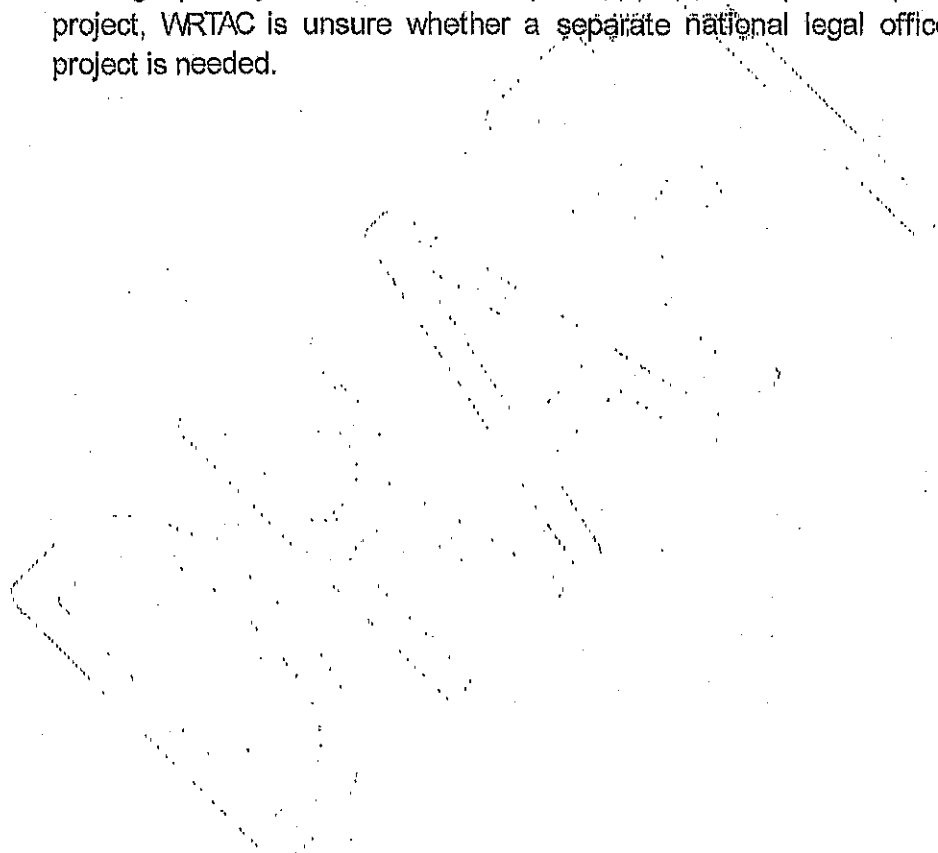
Partnering to Develop Geographic Risk Assessments

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.

EGuardian-464

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.



EGuardian-465

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
- Seattle Police Department/ Washington State Fusion Center
- 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

EGuardian-467

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

EGuardian-468

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

EGuardian-469

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
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

EGuardian-470

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 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

EGuardian-472

Line Officer Training	TBD
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

EGuardian-473

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
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 delivered to Virginia State Police	April 2, 2009
Line Officer Training delivered to Virginia State Police (pilot)	June 9, 2009
Chief Executive Officer Briefing delivered to Virginia State Police	October 29, 2009
Washington, DC, Metropolitan Police Department	
Line Officer Training delivered to Washington, DC, Metropolitan Police Department	December 2008
SAR Analyst/ Investigator Training delivered to Washington, DC, Metropolitan Police Department	December 12, 2008
Chief Executive Officer Briefing delivered to Washington, DC, Metropolitan Police Department	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

EGuardian-475

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 the 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

EGuardian-476

ISE-SAR EE Shared Space and SVT Install Completed at Houston Police Department	April 24, 2009
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 Space	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 Space	November 30, 2009 (estimated)
Los Angeles Police Department went "live" and was able to utilize the ISE-SAR EE Shared Space	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)

EGuardian-477

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

EGuardian-478

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

QUESTIONS

FOR QUESTIONS REGARDING THE ISE-SAR EVALUATION ENVIRONMENT PROJECT, CONTACT:

Mr. [redacted]
Senior Policy Advisor
Bureau of Justice Assistance
Office of Justice Programs
U.S. Department of Justice
[redacted]

b6 per FBI
b7C

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

Ms. [redacted]
Information Sharing Environment
Office of the Director of National Intelligence
[redacted]