Fact Sheet
Nationwide Suspicious Activities Reporting Initiative

BACKGROUND

- On October 31, 2007, the President issued the first *National Strategy for Information Sharing* (*Strategy*) to prioritize and unify our Nation's efforts to advance the sharing of terrorism-related information among Federal, State, local, and tribal Governments, the private sector, and foreign partners.
- The *Strategy* calls for the Federal Government to support the development of a nationwide capacity for gathering, documenting, processing, analyzing and sharing terrorism-related suspicious activity reports (SARs) generated at the local, regional, state or federal levels, in a manner that rigorously protects the privacy and civil liberties of Americans.
    - While suspicious activities have been documented by individual entities for years, this effort seeks to standardize the SAR process.

NATIONWIDE SAR INITIATIVE

- The Nationwide SAR Initiative (NSI) is an outgrowth of a number of separate but related activities over the last several years that respond directly to the *Strategy's* mandate, with the long term goal of having most Federal, State, local, and tribal law enforcement organizations participating in a standardized, integrated approach to gathering, documenting, processing, analyzing, and sharing information about suspicious activity that is potentially terrorism-related.
    - In addition to government agencies, private sector organizations responsible for Critical Infrastructure/Key Resources (CI/KR) and foreign partners are also potential sources for terrorism-related SARs.
- The NSI process is a cycle of 12 interrelated operational activities required to address the requirements outlined in the NSIS.
- The NSI is not a single monolithic program, but is rather a coordinated effort that leverages and integrates all SAR-related activities into a nationwide unified process.
- The initiative will ensure that NSI participants at all levels of government adopt consistent policies and procedures that foster broader sharing of terrorism-related SARs, also known as ISE-SARs, while ensuring that privacy and civil liberties are adequately protected in accordance with Federal, State, and local laws and regulations.

NATIONWIDE SAR INITIATIVE CONCEPT OF OPERATIONS

- On December 23, 2008, the Office of the Program Manager for the Information Sharing Environment (PM-ISE) released the NSI Concept of Operations (CONOPS), which presents a top-level operational view of the NSI.
- The NSI CONOPS provides a common understanding of the NSI cycle so that implementation activities can be planned, executed, and measured by:
    - Defining requirements that drive the NSI process and associated implementation activities;
    - Describing the overall process and multiple ISE-SAR-related activities in sufficient detail to ensure that these activities adhere to standard approaches and that all embody adequate protections for privacy and civil liberties;

- Clarifying the role of the ISE-SAR Evaluation Environment (described below) as a microcosm of the broader NSI—a smaller-scale implementation test-bed;
- Describing the roles, missions, and responsibilities of NSI participating agencies and the top-level NSI governance structure; and
- Serving as the foundation for other NSI baseline documents, such as the ISE-SAR Segment Architecture, that provide additional details on specific aspects of the NSI.

ISE-SARs - A UNIFIED PROCESS FOR TERRORISM-RELATED SARs

- In support of the *Strategy* and the Nationwide SAR Initiative, and as a part of efforts to establish the Information Sharing Environment (ISE), the PM-ISE is establishing a unified process for terrorism-related SARs also known as ISE-SARs.
- To date the ISE-SAR efforts include:
  - Developing, issuing, and evaluating the ISE-SAR Functional Standard and included Information Exchange Package Documentation (IEPD) component that defines both the data standards and business processes that will enable the sharing of terrorism-related SARs across the ISE—including between State and major urban area fusion centers and federal entities at the headquarters level. The ISE-SAR Functional Standard V.1 was issued in January 2008.
  - Identifying a limited number of current practices at the local, regional and field office level related to training front line personnel to recognize terrorism-related suspicious activities that may represent pre-incident indicators of a terrorism threat, and documenting those activities once observed. Some of the current practices are documented in the recently released report by the Department of Justice (DOJ), the Department of Homeland Security (DHS) and the Major Cities Police Chiefs Association entitled, *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project*.
  - Establishing an ISE-SAR Evaluation Environment to test and evaluate the steps in the NSI cycle in a real world setting.
  - Conducting an initial analysis of the privacy and civil liberties ramifications of the ISE-SAR Functional Standard and Evaluation Environment and providing recommendations regarding the policies and safeguards that should be implemented (see below for further information.)
  - Developing and issuing the ISE-SAR Evaluation Environment Segment Architecture, (see below for further information.)

ISE-SAR EVALUATION ENVIRONMENT

- The ISE-SAR Evaluation Environment represents a low risk approach for testing and evaluating ISE policies, business processes, capabilities, architectures, and standards by sponsoring efforts that implement and evaluate solutions to operational needs in a relatively controlled environment.
  - It is not merely a proof-of-concept or technology demonstration, but rather serves as a preliminary phase of a longer term effort that assesses and refines processes and capabilities prior to full-scale operation.
- Specific objectives include:
  - Improving operational processes at local law enforcement agencies and fusion centers by providing capabilities to document, store, and share terrorism-related SARs;
  - Testing and validating fundamental ISE Enterprise Architecture Framework concepts and core services;

  - Incorporating "Lessons-Learned" and "Best Practices" into an implementation guide and template for establishment of a nationwide ISE-SAR process;
  - Informing ISE Investment Planning; and
  - Issuing an updated version of the ISE-SAR Functional Standard.
- The project currently envisions twelve ISE-SAR Evaluation Environment sites, located at State and major urban area fusion centers and their source agency law enforcement partners, which will be implemented and activated incrementally as each site is provided the necessary technology, technical assistance, and training, and adopts an appropriate privacy protection policy for ISE-SAR information. [The twelve sites will be announced in the near future.]

ISE-SAR EVALUATION ENVIRONMENT SEGMENT ARCHITECTURE

- On December 23, 2008, the PM-ISE released the Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Evaluation Environment Segment Architecture, Version 1.0, which will assist program managers, chief architects, and systems designers and implementers as they determine the programmatic and solution strategies to support the business case for the ISE-SAR Evaluation Environment project.
- This new ISE Architecture program document is the next level of technical detail following the Nationwide Suspicious Activity Reporting Initiative (NSI): Concept of Operations.
- This ISE-SAR Evaluation Environment Segment Architecture provides a logical arrangement of business and functional drivers, information exchange requirements, outcomes and constraints for building the operational ISE-SAR Evaluation Environment, and is consistent with the Federal Government's new Federal Segment Architecture Methodology (FSAM).
- Derived from ISE Architecture program documentation, this segment architecture identifies enabling services required for operational implementation and use in the ISE-SAR Evaluation Environment, and also provides technical guidance to other departments and agencies as they implement information technology capability supporting terrorism-related suspicious activity reporting.

FURTHER BACKGROUND ON ISE-SAR EVALUATION ENVIRONMENT

- To satisfy privacy and civil liberties concerns, each fusion center and local entity participating in the ISE-SAR Evaluation Environment initiative will develop or follow established business rules for multi-level review and vetting of suspicious activity reporting by personnel trained in the ISE-SAR process.
  - The review and vetting process begins when a front-line law enforcement officer responds to a call for service, self-initiates law enforcement action based on a reported incident or observation, or observes suspicious behavior.
  - To preclude reporting on individuals involved in innocent activities, front line personnel must be able to recognize indicators (incidents, behaviors, and modus operandi of individuals and organizations) of criminal activity associated with domestic and international terrorism and must understand the scope of their legal authority to obtain information.
  - As a part of this effort, DOJ, DHS, the Major Cities Police Chiefs Association and the International Association of Chiefs of Police will work with local participants to develop and provide appropriate training of front line personnel; senior officers, investigators, and analysts who will provide multiple levels of report review; and other agency personnel on the criteria of the ISE-SAR Functional Standard, legal collection thresholds, and other privacy protections.

- Once reported or observed, the behaviors and incidents indicative of criminal activity will be documented and evaluated in a two-step process by trained personnel to determine if they meet terrorism-related SAR criteria and have a potential terrorism nexus. If a potential nexus is established, the ISE-SAR may be made available through the ISE to appropriate agencies and entities.
- Technical resources will be provided to enable the "posting" of terrorism-related SARs to a server (i.e., Shared Space) in a manner consistent with technical standards contained within the ISE-SAR Functional Standard and included IEPD component. This will allow ISE-SARs to be accessed by other fusion centers, authorized Federal, State, local, and tribal law enforcement agencies, DHS Headquarters, and the FBI's Joint Terrorism Task Forces (JTTFs) and Field Intelligence Groups (FIGs) to support regional and national analysis.
    - Access to the Shared Spaces will be via Law Enforcement Online (LEO), the Regional Information Sharing Systems Network (RISSNET) and the Homeland Security Information Network (HSIN).
    - The FBI will use an unclassified version of its GUARDIAN system, known as eGuardian, as the primary mechanism for JTTFs to receive terrorism-related investigative leads. The FBI plans for eGuardian to also serve as an ISE-SAR Shared Space and is making its use available to Federal, State, local and tribal law enforcement entities. EGuardian is accessible via LEO.
- Protecting the legal rights of Americans and other "protected persons," including information privacy, civil rights, and civil liberties guaranteed by the Constitution and the laws of the United States, is critical to the success of the ISE-SAR initiative.
    - To that end, an initial analysis of the privacy and civil liberties ramifications of the ISE-SAR Functional Standard and Evaluation Environment was conducted and recommendations were made regarding the policies and safeguards that should be implemented.
    - The *Initial Privacy and Civil Liberties Analysis of the Information Sharing Environment – Suspicious Activities Reporting (ISE-SAR) Functional Standard and Evaluation Environment (September 2008, Version 1)*, was prepared by the PM-ISE, in consultation with the Civil Liberties and Privacy Office of the Office of the Director of National Intelligence, the DOJ's Office of Privacy and Civil Liberties, and the Legal Issues Working Group of the ISE Privacy Guidelines Committee. [This report is available at www.ise.gov.]
    - This is an *interim* privacy and civil liberties analysis that will be updated as more information is obtained during the ISE-SAR Evaluation Environment initiative, including lessons learned from participants and feedback received from privacy and civil liberties advocates and other interested parties. [For more information, see *Initial Privacy and Civil Liberties Analysis* Fact Sheet.]
- The results of the ISE-SAR Evaluation Environment will be documented to support the development and publication of an implementation guide and template for use by other Federal, State, local and tribal jurisdictions and to update the ISE-SAR Functional Standard and the IEPD component.
- Funding for the ISE-SAR Evaluation Environment project is being provided by both the PM-ISE and the DOJ and will be administered by the DOJ's Bureau of Justice Assistance (BJA).
    - A number of State and local officials and associations were involved in planning and will be involved in implementation, including the International Association of Chiefs of Police, the Major Cities Police Chiefs Association, Major County Sheriffs and Global Justice's Criminal Intelligence Coordinating Council (CICC).