Federal Segment Architecture Methodology (FSAM) Case Study:

Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Evaluation Environment (EE)

December 9, 2008
What Is the ISE?

• As defined in Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 as amended (IRTPA), the ISE is …

  “an approach that facilitates the sharing of terrorism and homeland security information, which may include any method determined necessary and appropriate for carrying out this section.”

• Definition further refined in Executive Order 13388 (October 2005) and Presidential Information Sharing Guidelines (December 2005)

• ISE Implementation Plan (November 2006) established a vision, strategic goals, and implementation activities for the ISE

• National Strategy for Information Sharing (NSIS), issued on October 31, 2007 by the President, outlined success and challenges in improving terrorism-related information sharing
Who Is the ISE?

- Multiple Communities of Interest
- Multiple User Types
- Multiple Governmental and Non-governmental Entities

---

The Information Sharing Environment

---

Investigators
Command & Control
Responders
Operators
Collectors
Analysts
What Makes an Activity Suspicious?

• A citizen observes or reports to law enforcement authorities that something is alarming, out of the ordinary, or “just not right”

• Law enforcement or government official observes something
  ➢ Based on training or experience to recognize behaviors and indicators that are associated with a criminal activity associated with terrorism
  ➢ Knowledge of laws and regulations
  ➢ Interactivity with other agencies

• Studies and research done on activities leading to crimes and terrorist acts (e.g., Los Angeles Police Department)
What Do We Know Already?

• Reporting suspicious activity has been an everyday law enforcement function for years
• Reporting suspicious activity is not a “new” type of information gathering
• A number of different reporting mechanisms exist
  ➢ 9-1-1 calls, citizen reports, tips and leads, Internet
• Reported suspicious activity could be
  ➢ A precursor to a criminal act
  ➢ The result of a criminal act
  ➢ A precursor to an act of terrorism
  ➢ Unfounded upon law enforcement’s arrival
  ➢ Legitimate in nature
Introducing the ISE-SAR

• The ISE-SAR process uses existing law enforcement practices—gathering information regarding behaviors and incidents associated with crime—and establishes a process whereby information can be shared to detect and prevent criminal activity, including that associated with domestic and international terrorism.

• An ISE-SAR is a SAR that has been legally gathered and is determined to have a potential nexus with terrorism-related criminal activity.

• Implementation of the ISE-SAR process can be accomplished within the agency’s existing framework to gather, process, analyze, and report behaviors and events that are indicative of criminal activity.

• Standards to give guidance to local, state, and tribal agencies as to when to use discretion.

• Safeguards to protect privacy and civil liberties.

• Technology in place to share terrorism-related SARs across the ISE.

• Individuals are trained to vet ISE-SARs before submission.
ISE-SAR EE
Current & Potential Sites

- Seattle
- Los Angeles
- Las Vegas
- Phoenix
- Houston
- Florida
- Miami Dade
- New York State
- Virginia
- Maryland
- DC (and Federal Shared EE Sites)
- Boston

- Phase 1 Pilot Sites/Data Repositories
- Potential Expansion Sites
FSAM Step 1: Determine Participants and Launch Project

• Determine the Executive Sponsor
  - Office of the Program Manager, Information Sharing Environment
  - Governance Framework: SAR Steering Committee, CTISS Committee

• Develop the Purpose Statement for the Segment
  - A logically arranged compilation of business and functional drivers for building the performance-based, operational ISE-SAR EE

• Solicit Core Team Members
  - Project team formed July 3, 2008 (Federal, State, and local members)

• Create Core Team Charter and Project Plan
  - Schedules, information to capture (EE drivers, constraints, outcomes)

• Establish the Communications Strategy
  - NSI CONOPS, Fact Sheet, communications statement
FSAM Step 2: Define the Segment Scope and Strategic Intent

• Establish Segment Scope and Context
  ➢ Nationwide SAR Cycle, ISE-SAR Exchanges and Information Flow

• Identify and Prioritize Strategic Improvement Opportunities
  ➢ Business needs, performance gaps from ISE-SAR Exchanges and Information Flow

• Define Segment Strategic Intent
  ➢ Performance outcomes (Objective and Threshold) identified, risk mitigation strategies (NIST 800-39, 800-53, 800-60)

• Validate and Communicate the Scope and Strategic Intent
  ➢ White House Office of Management and Budget, PM-ISE, SAR Steering Committee, ISE-SAR EE stakeholders
Nationwide SAR Cycle

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

Supervisory review of the report in accordance with departmental policy

In major cities, SAR reviewed by trained CT expert

Authorized ISE participants access and retrieve ISE-SAR

ISE-SAR posted in an ISE Shared Space

Determination and documentation of an ISE-SAR

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

Suspicious Activity Processing Steps

Planning  Gathering and Processing  Analysis and Production  Dissemination  Reevaluation

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

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

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

Front line LE personnel (FSLT) trained to recognize behavior and incidents indicative of criminal activity associated with terrorism; Community outreach plan implemented

National coordinated information needs on annual and ad hoc basis
A Functional Flow of Information in the ISE
Multiple Processes/SAR Emphasis

Collection Guidance

Private Sector

Federal Field Components

SLT Entities

Collection & Reporting

Fact Info

Federal HQs

SAR Vetting and Standards Application

NCTC (ITACG)

National/Fusion Center Analysis

Fusion Center

Investigative/Threat Mitigation

Guardian/e-Guardian

Federal Intel.

Federal LE

Homeland Security

SLT

Shared SARs

Fusion Cntrs.

JTTF
Information Flow
(from ISE-SAR Functional Standard)

Step 2 is an internal process that prepares fact information to be used in Step 3. It is not reflected in this diagram.
FSAM Step 3: Define Business and Information Requirements

• Determine Current Business and Information Environment Associated with Strategic Improvement Opportunities
  ➢ AS-IS site visits and surveys
• Determine Business and Information Improvement Opportunities
  ➢ Objective and Threshold outcomes cross referenced
• Define Target Business and Information Architecture
  ➢ ISE-SAR Top-Level Business Process, ISE-SAR EE Top-Level Information flow, Business Process Modeling Breakout, SAR Data Model
• Validate and Communicate Target Business and Information Architecture
  ➢ Document reviewed and approved by SAR Steering Committee
ISE-SAR Top-Level Business Process

Feedback
SAR Follow-up and Disposition Process Modification

Information Acquisition
Initial Collection of Raw Data

Organizational Processing
Agency Assessment Against ISE-SAR Criteria

Integration/Consolidation
Data Networked for Accessibility

Data Retrieval/Distribution
Data Customers Access Information

Key Considerations

Raw Data Requirements
ISE-SAR Criteria
Data Record Definition
Availability/Accessibility
ISE-SAR EE Top-Level Information Flow

* The DoD will follow the third party level hosting model for their ISE Shared Space
ISE-SAR Business Process Modeling Breakouts

**Step 1**
Local Source

**Step 2**
Suspicious Activity Event

### Information Acquisition

- Local Source
- Local Source
- Local Source

### Organizational Processing

- Federal LE Agencies
- JTTF
- ISE-SAR

### Integration/Consolidation

- DoD (Antiterrorism/Force Protection)
- ISE Shared Space
- Federal LE Agencies

### Data Retrieval/Distribution

- DoD (Antiterrorism/Force Protection)
- ISE Shared Space
- Federal LE Agencies

*The DoD will follow the third party level hosting model for their ISE Shared Space.*
SAR Data Model  
(from ISE-SAR Functional Standard)
ISE-SAR EE Segment Architecture Layout

• Introduction
  ➢ Scope, participating organizations and sites, references

• Business Outcomes/Performance Goals

• SAR Process
  ➢ Nationwide SAR process
  ➢ ISE-SAR Top-Level Business Process
  ➢ ISE-SAR Information Flow
  ➢ Top Level Business Process Steps
    • Description, Outcomes (Threshold, Objective), Affected CORE service processes, constraints

• Enabling Services to Support Outcomes
  ➢ Privacy and Civil Liberties Protection
  ➢ Access
  ➢ Information Assurance
  ➢ Resource/Network Management
  ➢ Trending/Analysis
FSAM Step 4: Define the Conceptual Solution Architecture

• Assess Systems and Technology Environment for Alignment with Performance, Business, Information Requirements
  ➢ Performance measurement guide, AS-IS questionnaires
• Define the Target Conceptual Solution Architecture
  ➢ In work
• Identify and Analyze System and Service Transition Dependencies
  ➢ Integrated planning document
• Validate and Communicate the Conceptual Solution Architecture
  ➢ SAR Steering Committee
• The FSAM:
  ➢ Aided in developing the ISE-SAR EE Segment Architecture for advancing the Nationwide SAR Initiative
  ➢ Provides an effective, structured approach to arrange business and functional drivers for building executable, operational solutions that meet or exceed mission performance goals
  ➢ Supports long-range, strategic investment planning (including A-11 budget processes), and short-term operational projects and evaluation environments
Ken Clark
ISE Architecture and Standards Programs
Office of the Program Manager, Information Sharing Environment

(202) 331-4060
kennenc0@dni.gov

www.ise.gov