



Fact Sheet: Update to Suspicious Activity Reporting Functional Standard Provides Greater Privacy and Civil Liberties Protections

Program Manager Updates Privacy & Civil Liberties Elements of ISE-SAR Functional Standard

- On May 21, 2009, Ambassador Thomas E. McNamara, Program Manager, Information Sharing Environment (ISE), updated the *ISE-Suspicious Activity Reporting (SAR) Functional Standard* to incorporate suggestions provided by federal privacy and civil liberties attorneys and members of the privacy and civil liberties advocacy community.
- PM-ISE and its partners have met with privacy and civil liberties advocates and state, local, and tribal law enforcement officials to better understand their concerns and suggestions for improving the Functional Standard. The Functional Standard directly addresses their concerns and incorporates their recommendations.
- The *ISE-SAR Functional Standard, Version 1.5* directly supports local efforts to fight terrorism-related crime, while at same time protecting the privacy and civil liberties of Americans. The *ISE-SAR Functional Standard, Version 1.5*:
 - Refines the definition of Suspicious Activity as, “*observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.*”
 - Clarifies that the same constitutional standards that apply when conducting ordinary criminal investigations also apply to law enforcement and homeland security officers conducting SAR inquiries.
 - Further emphasizes a behavior-focused approach to identify suspicious activity and requires that factors such as race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion (except if used as part of a specific suspect description).
 - Refines the ISE-SAR Criteria Guidance to distinguish between those activities that are Defined Criminal Activity and those that are Potentially Criminal or Non-Criminal Activity requiring additional fact information during investigation.
 - Clarifies those categories of activity which are generally First Amendment-protected activities should not be reported in a SAR or ISE-SAR absent articulable facts and circumstances that support the source agency’s suspicion that the behavior observed reasonably indicative of criminal activity associated with terrorism.
 - Updates the operational process descriptions to align the standard with the *Nationwide SAR Initiative Concept of Operations*, released in December 2008.

ISE-SAR Functional Standard Supports the Nationwide SAR Initiative

- The Nationwide SAR Initiative builds on what law enforcement and other agencies have been doing for years – gathering information regarding the behaviors and incidents associated with crime – and establishes a process for SAR information to be shared to help detect and prevent terrorism-related criminal activity.

- The Nationwide SAR process provides a unified, standardized, and integrated process for federal, state, local, and tribal law enforcement and homeland security officials to gather, document, process, analyze, and share information about suspicious activity in a manner that rigorously protects the privacy and civil liberties of Americans, as called for in the *National Strategy for Information Sharing*.
- A key step in the Nationwide SAR process is a two-part review of the SAR, by an appropriate authority, to determine whether there is a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism). If that determination is made, the SAR is designated an ISE-SAR.
- The ISE-SAR designation offers a standardized means for sharing information regarding behavior potentially related to terrorism-related criminal activity and applying data analysis tools.
- The process recognizes that many terrorism activities are now funded via local or regional criminal organizations whose direct association with terrorism may be tenuous, and therefore requires law enforcement and homeland security professionals to identify suspicious activities or materials as a byproduct or secondary element in a criminal enforcement or investigation activity.
- The effective sharing of ISE-SARs will enable the discovery of patterns and trends by analyzing information at a broader level than typically recognized within a single jurisdiction, state, or territory.
- Any patterns identified during ISE-SAR data analysis may be investigated in cooperation with the reporting agency, Joint Terrorism Task Force (JTTF), or the State or major urban area fusion center in accordance with departmental policies and procedures.
- The *ISE-SAR Functional Standard* allows for this process to occur in a standardized manner by documenting information exchanges and business requirements, and describing the structure, content, and products associated with processing, integrating, and retrieving ISE-SARs by ISE participants.
- The *ISE-SAR Functional Standard* is not intended to address all implementation issues for the gathering, processing, access, storage, and retrieval of SAR; it is one component of the overall Nationwide SAR Initiative.

Information Sharing Environment and The Common Terrorism Information Sharing Standards Background

- The *Intelligence Reform and Terrorism Prevention Act* of 2004, as amended, calls for the development of an ISE to facilitate the sharing of terrorism and homeland security information among Federal, State, local, and tribal governments and, as appropriate, foreign partners and the private sector.
- The Common Terrorism Information Sharing Standards (CTISS) program allows for business process-driven, performance-based "common standards" for preparing terrorism information for maximum distribution and access, to enable the acquisition, access, retention, production, use, management, and sharing of information within the ISE. Two categories of common standards are formally identified under CTISS:
 - Functional Standards – set forth rules, conditions, guidelines, and characteristics of data and mission products supporting ISE business process areas.

- Technical Standards – document specific technical methodologies and practices to design and implement information sharing capability into ISE systems.
- Visit www.ise.gov for more information about the Nationwide SAR Initiative and to view the CTISS Technical and Functional Standards in their entirety.