

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
PROGRAM MANAGER, INFORMATION SHARING ENVIRONMENT
WASHINGTON, DC 20511

May 21, 2009

MEMORANDUM FOR HEADS OF DEPARTMENTS AND AGENCIES

SUBJECT: Release of the Information Sharing Environment (ISE) Functional Standard for Suspicious Activity Reporting, Version 1.5 (ISE-FS-200)

REFERENCE: 1) Presidential Memorandum of December 16, 2005, subject: Guidelines and Requirement in Support of the Information Sharing Environment
2) National Strategy for Information Sharing, October 2007

On January 25, 2008 I issued the first Common Terrorism Information Sharing Standard (CTISS) for Suspicious Activity Reporting (SAR) in accordance with Presidential Memorandum directing the development and issuance of common standards governing how terrorism information is acquired, accessed, shared, and used within the ISE. This updated version of the *ISE-SAR Functional Standard* incorporates suggestions provided by federal privacy and civil liberties attorneys and members of the privacy and civil liberties advocacy community, and:

- 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 is 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.

All CTISS, to include this *ISE-SAR Functional Standard*, will be implemented by ISE participants into supporting infrastructures in accordance with the *ISE Enterprise Architecture*

Framework. This *ISE-SAR Functional Standard* is also in alignment with the *National Strategy for Information Sharing (NSIS)*, which outlines federal, state, local, and tribal responsibilities for sharing ISE-SAR data.

This *ISE-SAR Functional Standard* documents information sharing exchanges and business requirements, and describes the structure, content, and products associated with processing, integrating, and retrieving ISE-SAR by ISE participants. Each Information Sharing Council (ISC) member and other affected agencies responsible for the collection and processing of SARs with a nexus to terrorism must apply this Functional Standard when processing, integrating, and retrieving ISE-SAR, and incorporate this Functional Standard into their business processes development and information resource planning. In particular, ISC agencies should, as appropriate, incorporate this *ISE-SAR Functional Standard* and any subsequent implementation guidance into budgetary planning activities associated with current (operational) and future development efforts associated with relevant mission-specific programs, systems, or initiatives. As appropriate, departments and agencies may consider utilizing this standard as part of the grant application process.

This updated version of the *ISE-SAR Functional Standard* will continue to be tested and evaluated by the user community. Any resulting refinements, including changes to SAR business processes and data elements, will be incorporated in future versions. Privacy assessments will also be performed as appropriate to identify privacy issues that may arise in implementing this *ISE-SAR Functional Standard* and information flow. This *ISE-SAR Functional Standard* is not intended to address all the implementation issues associated with the reporting, tracking, processing, accessing, storage, and retrieval of SAR information within the ISE; it is one component of the overall Nationwide SAR Initiative.

Please address any questions associated with this *ISE-SAR Functional Standard* to your designated ISC Representative (Attachment B) or the Office of the Program Manager.



Thomas E. McNamara

Attachments:

- A. Information Sharing Environment (ISE) Functional Standard (FS) for Suspicious Activity Reporting (SAR), Version 1.5 (ISE-FS-200)
- B. Information Sharing Council Members
- C. Fact Sheet: Update to Suspicious Activity Reporting Functional Standard Provides Greater Privacy and Civil Liberties Protections

cc: Information Sharing Council