

New Suspicious Activity Reporting Standards Offer Model for Information Sharing

Overview

The Director of National Intelligence (DNI) has released a new set of standards for reporting suspicious activity related to terrorism. The new standardized system for exchanging data on potential security threats could provide an important model for effective information sharing in the private sector. The standards describe how Federal, State, and local law enforcement officials should handle the reporting of suspicious activity, from the moment the activity is first observed to the time the information is disseminated to the appropriate agency. By standardizing the process for managing this information, the government can better identify national trends that may otherwise go unnoticed in a single State or region.

Established by the United States Congress in 2004, the DNI functions as the top intelligence authority overseeing all 16 members of the United States intelligence community.

Background

Effective interagency information sharing has long plagued the Federal government. In its 2004 report, the 9/11 Commission identified major intelligence failures leading up to the September 11, 2001 terrorist attacks, and thus, recommended the establishment of a single intelligence authority for the Federal government. The United States Congress acted on this recommendation in 2004 by establishing the Director of National Intelligence (DNI) to oversee all 16 members of the United States intelligence community.

In December 2005, the President called on the counterterrorism community to improve processes for sharing terrorism information. One of the priorities in this effort was to establish a set of common standards for collecting, processing, and sharing information among agencies that may benefit from such information.

In support of the President's information sharing goals, the DNI has released the very first standard governing how to report and share information about suspicious activities that could have a nexus to terrorism. Dubbed the Information Sharing Environment Functional Standard (ISE-FS) for Suspicious Activity Reporting (SAR), the ISE-FS-200 describes how Federal, State, and local officials should acquire, process, share, and use terrorism information within the community known as the Information Sharing Environment (ISE). Standardizing this process could aid in the discovery of national patterns or trends for terrorist-related activities that may not otherwise be apparent within a single State or area.

ISE-FS-200: Definition of Suspicious Activity

According to the standard, "suspicious activity" is defined as "observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention." Examples of criteria that could suggest a terrorism nexus and warrant a report include surveillance, photographing facilities, site breaches or physical intrusions, cyber attacks, and security probes.

ISE-FS-200 is the first of many standards that will constitute the Common Terrorism Information Sharing Standards (CTISS), a set of common processes for handling terrorism information within the ISE. All agencies responsible for collecting terrorism-related Suspicious Activity Reports must apply the ISE-FS-200 when retrieving, processing, and integrating the information, according to a January 25, 2008 memorandum (attached) from the DNI to the heads of Federal departments and agencies. Agencies must also incorporate the standard into their development of business processes and information resource planning, including budgetary planning. The standard is considered an initial version that will continue to be tested and evaluated by the community. The feedback will inform revisions to be made in future iterations.

ISE Functional Standard: 5 Steps

The new standard breaks down the SAR process into five steps:

1. **Information Acquisition:** An agency or organization collects initial raw data by observing suspicious activity that may be linked to terrorism. According to ISE-FS-200, each agency may retain a unique approach to collecting and documenting SAR observations. However, the standard ensures that specific information, such as “Person First Name,” can be acquired by ISE consumers.
2. **Organizational Processing:** A supervisor within the agency or organization assesses and validates the event before sending it to a major fusion center for processing within the ISE. Again, each agency may have its own processes for validating SAR information, as many agencies have broader missions that may include, but not be limited to, terrorism. Though some modification of these processes may be necessary to conform to overall ISE functional standards, the purpose of the standard in this case is to establish common criteria for determining whether a SAR is terrorism-related and should be placed into the ISE.
3. **Integration/Consolidation:** The fusion center evaluates the information to determine whether it meets ISE-SAR criteria for suspicious activity with a potential nexus to terrorism. If so, the information is integrated within the ISE.
4. **Data Retrieval/Distribution:** The fusion center disseminates the information to the organization(s) most likely to be affected by the Suspicious Activity Report.
5. **Feedback:** End users of the information provide feedback on the utility of the information, which informs continued refinement of the SAR process for overall quality and effectiveness.

The ISE-SAR Information Exchange ‘Artifacts’

The ISE-SAR information exchange framework comprises four standardized “artifacts,” or detailed mission documents, that serve as the technical medium for the exchange. These include Extensible Markup Language (XML)-based products that facilitate the storage and organization of data to be processed and integrated in the ISE. The four artifacts are:

- **Component Mapping Template:** A spreadsheet that contains SAR information and links it to corresponding data in the National Information Exchange Model (NIEM). The NIEM is an XML-based information exchange framework used by the United States government. XML is a common markup language that stores, describes, and transmits data.
- **NIEM Wantlist:** An XML-based file that lists NIEM data that will be included in the “Schema Subset.” The subset is a version of the collected data that is compliant with both programs and contains only those elements to be used in the ISE-SAR schema.
- **XML Schemas:** A machine-readable technical representation of the information being collected.

- XML Sample Instance: A sample document formatted to comply with the structures defined in the XML Schema. It provides an example of how the ISE-SAR schema is to be used.

The information exchange process involves three primary actors:

- Source Organization: The agency that files the SAR report (e.g., police department, private security firm).
- Submitting Organization: The organization providing the SAR to the ISE community (which may be the same as the Source Organization).
- Owning Organization: The organization that owns the potential target associated with the Suspicious Activity Report.

Private Sector Implications

By issuing these standards, the Federal government seeks to more effectively manage the volume of security-related information that can originate in agencies and organizations across the country. Doing so enables more efficient processing and effective analysis and distribution of data to agencies most likely to be impacted. As such, the Federal government is better positioned to assess threats from a higher level and make critical linkages among disparate events that, on their own, may not appear to constitute any threat. This system of information exchange offers a model for private sector companies with similar information sharing challenges among their multiple and widespread locations.

Conclusion

The new standard promulgated by the DNI offers an important model for acquiring, processing, and sharing information that could have critical security ramifications. By establishing a common practice for these information exchanges among the vast array of actors in the ISE, the Federal government seeks to more effectively organize and exploit information that could help protect against potential security threats.

Acronyms

CTISS	Common Terrorism Information Sharing Standards
DNI	Director of National Intelligence
ISE	Information Sharing Environment
ISE-FS	Information Sharing Environment – Functional Standard
NIEM	National Information Exchange Model
SAR	Suspicious Activity Reporting
XML	Extensible Markup Language