Department of the Interior
Law Enforcement Policy

Effective Date: June 4, 2012
Series: Law Enforcement and Security
Chapter 37: Suspicious Activity Reporting

Originating Office: Office of Law Enforcement and Security

37.1 **Purpose.** This chapter establishes Department of the Interior (DOI/Department) policy for Suspicious Activity Reporting (SAR). SAR is a component of the Nationwide SAR Initiative (NSI) which consists of local, state, tribal and federal partners involved in the gathering, documenting, processing and analyzing of *terrorism-related* suspicious activities which may ultimately result in the potential identification of terrorism-related activity.

The purpose of SAR is not to replicate any other DOI serious incident reporting procedures or policies. SAR is an independent requirement that, while it frequently may identify the same incident or event, has a separate and distinct reporting requirement, the purpose of which is to identify and share information about suspicious activities which may be potential indicators of *terrorism-related* criminal activity.

37.2 **Scope.** This policy applies to all bureaus/offices.

37.3 **Authority.** This policy is issued pursuant to 112 DM 17 and 212 DM 17.

37.4 **Responsibilities.**

A. Director, Office of Law Enforcement and Security (OLES) is responsible for policy development, program guidance and oversight of the Department's law enforcement programs.

B. Bureaus/Office Heads are responsible for promulgating any counterpart policy or procedures required to implement the policy established in this chapter.

C. Bureau Directors of Law Enforcement (BDLE) are responsible for developing any counterpart training policies or procedures to this chapter and complying with both Department and bureau/office policies and procedures.

37.5 **Definitions.** For the purpose of this chapter, the terms below are defined as follows:

A. Suspicious Activity: Observed or reported behavior that may be indicative of intelligence gathering, pre-operational planning, or other criminal activity with a potential nexus to domestic or international terrorism. For the purposes of this policy, suspicious activities may

include, but are not limited to: specific activities relating to weapons of mass destruction; making threats; conducting surveillance; planning cyber attacks; probing security; or, atypical photography. SAR will not be based solely on the ethnicity, race, or religion of an individual or solely on the exercise of rights guaranteed by the First Amendment or the lawful exercise of any other rights secured by the Constitution or laws of the United States. (For examples of potential suspicious activity, see Appendix 1).

B. LEO. A commissioned DOI employee sworn to enforce criminal statutes and authorized to carry firearms, execute and serve warrants, search, seize, make arrests and perform such duties as authorized by law.

37.6 **Policy.**

A. All bureaus/offices will implement a SAR procedure conforming, at a minimum, to the requirements set forth herein to ensure that the Department and OLES are properly notified of all criminal and non-criminal incidents that represent indicators of potential domestic or international terrorism in a timely manner.

B. Bureau/office SAR reporting procedures will incorporate processes for gathering, processing, reporting, sharing, updating, and maintaining information contained in such reports.

C. SAR procedures will be carried out in a manner that protects the privacy and civil liberties of U.S. citizens and lawful permanent residents. Such information will be recorded and maintained in strict compliance with existing federal law and Department guidelines including the DOI privacy policy for the Information Sharing Environment (ISE).

D. This policy does not relieve employees of their obligation to report information, allegations, or complaints of fraud, waste, abuse, or mismanagement in Department programs or operations directly to the Office of Inspector General in accordance with 355 DM 2, or to provide Serious Incident Reports to OLES in accordance with 446 DM 17.

E. Nothing in this chapter should be construed to delay immediate notification to management and emergency personnel in the case of imminent danger.

37.7 **Background.** Department personnel, including contractors and visitors to Department facilities, play a critical role in reporting suspicious activities which may prevent crimes and acts of terrorism. *The 9/11 Commission Report*, although not specifically using the term "suspicious activity reporting," describes many examples of lost opportunities because existing information was inaccessible outside a specific agency or narrow community of interest because of what the Commission referred to as "the human or systemic resistance to sharing information." The 9/11 Commission recognized that federal, state, local, and tribal governments have access to information that could, when synthesized with information from other sources, help identify precursor activities of terrorist attacks or activities. The Department's SAR Policy, as described in this chapter, builds on what law enforcement and other agencies have been doing for years—gathering information regarding behaviors and incidents associated with crime—and establishes

a process whereby SAR information can be shared to help detect and prevent terrorism-related criminal activity.

37.8 **OLES Responsibilities.**

A. Oversee the implementation of the Department's SAR policy and provide guidance to bureaus/offices,

B. Represent the Department on interagency SAR-related committees and groups.

C. Review the internal SAR reporting and review procedures developed by bureaus/offices to assure compliance with this policy.

D. Coordinate with the FBI to utilize its *eGuardian* system to report, collect, and share SAR data among law enforcement elements within the Department as well as across various federal, state, local and tribal jurisdictions.

E. Ensure the Department's Incident Management, Analysis, and Reporting System (IMARS) provides the capability of reporting SAR incidents within the Department.

F. OLES may request copies of supporting documentation related to a SAR. Upon such request, the bureau/office will forward the requested documents to the Interior Operations Center (IOC) as soon as practicable.

G. OLES will assist and facilitate follow-up activity on the SAR, as appropriate.

37.9 **IOC Reporting.** Upon receipt of a SAR, the IOC will make immediate notification to OLES and others as appropriate depending upon the nature of the SAR incident in accordance with 446 DM 17.6 (Serious Incident Reporting). In addition, the IOC will immediately distribute the report to:

A. the *e-Fusion* Center for entry into the FBI *e-Guardian* Database;

B. the DOI National Threat Coordinator (DOI NTC) for situational awareness and any necessary follow-up; and,

C. the primary state fusion center within the state where the SAR occurred.

37.10 **Bureau/Office Reporting.**

A. Bureaus/offices will develop an internal SAR format and review procedure, which will include a supervisory or second-level review process to ensure that the report is reviewed in a timely manner by a supervisor with knowledge of the reporting officer's job function and worksite. The secondary reviewer will determine whether the information contained in the report warrants entry into the *e-Guardian* database as a SAR.

B. Bureaus/offices will develop internal processes outlining how their law enforcement or support personnel report and enter information.

C. Bureaus/offices may also elect to disseminate SAR reports to state and major urban area fusion centers with a geographic nexus to the reported incident, as deemed appropriate.

D. In addition to reporting to the IOC, bureau/office personnel will refer suspicious activities requiring immediate action to their local FBI Joint Terrorism Task Force and their appropriate state or major urban area fusion center. OLES will be promptly notified if such action is taken.

37.11 **Flow of Information.**

A. Upon learning of a suspicious activity or incident, bureau/office personnel will submit a report in accordance with the SAR reporting policies established by the bureau/office.

B. Designated and appropriately trained bureau/office personnel will conduct a supervisory or second-level review of all potential SAR reports to ensure the incidents meet the definition of a SAR.

C. After determining the report meets the definition of a SAR in their secondary review, designated bureau/office personnel will then forward those SAR reports to the IOC as soon as possible.

D. The IOC will forward approved SAR reports to: the *e-Fusion* Center for entry into the FBI *e-Guardian* database; the DOI National Threat Coordinator for follow-up; and, other entities, as appropriate.

E. In the unlikely event that a secondary review cannot be performed, to ensure timeliness, bureau/office personnel will forward the potential SAR report to the IOC which will obtain secondary review from the DOI National Threat Coordinator or personnel assigned to the *e-Fusion* Center.

37.12 **Privacy and Civil Liberties.**

A. This policy will be carried out in a manner that protects the information privacy and legal rights of U.S. citizens and lawful permanent residents, and therefore such information will be recorded and maintained in strict compliance with existing federal, state, and Department guidelines.

B. During the creation, dissemination and use of SAR data, the privacy and civil liberties of U.S. citizens and lawful permanent residents will be upheld, in conformity with the DOI *ISE Privacy Policy*. At a minimum, DOI personnel engaging in SAR will: receive adequate training to safeguard privacy and civil liberties; use appropriate physical, technical, and administrative measures to safeguard SAR information from unauthorized access; ensure that questionable SAR data includes a cautionary note about its content or credibility; and, ensure

that individuals seeking redress on any privacy issues will be directed to the DOI Privacy Officer for follow-up.

37.13 **Training.**

A. All new law enforcement personnel will receive SAR training as part of their initial basic training, whether at the Federal Law Enforcement Training Center or equivalent training venue, as appropriate.

B. Basic training will focus on enriching the critical role LEOs have in the effective implementation of the SAR process. Participants will be trained to recognize those behaviors and incidents that could indicate possible terrorism activity.

C. Bureaus/offices will determine which of their employees, to include non-law enforcement personnel, require SAR training, and will maintain records of all personnel who receive training.

D. Bureaus/offices will ensure that personnel receive annual refresher SAR training as appropriate.

Suspicious Activity Reports

Suspicious activity is observed behavior that may be indicative of intelligence gathering or pre-operational planning with a potential nexus to domestic or international terrorism. Observers must be vigilant regarding any type of activity or circumstance that seems atypical or unusual during the normal routine performance of their duties. In most cases, the observer or reporting officer best understands the context and circumstances surrounding the observation; accordingly, bureaus/offices are expected to utilize professional judgment, experience, and common sense in determining the need to report. Unusual or suspicious activity does not necessarily mean that terrorist activity is occurring or about to occur. Be aware of the following types of suspicious behaviors including, but not limited to:

- Breach or attempted intrusion
  - Unauthorized personnel attempting to, or actually entering, a restricted area or protected site
  - Individuals impersonating authorized personnel

- Misrepresentation
  - Use of false or misleading identification or documents
  - Attempting to hide affiliation to cover possible illicit activity

- Theft/Loss/Diversion
  - Stealing or diverting something associated with a facility or location (uniforms, badges, ID cards, etc.) that could allow access

- Sabotage/Tampering/Vandalism
  - Damaging, defacing, or manipulating criticial parts of a facility or protected site

- Expressed or implied threat
  - Communicating a spoken or written threat to persons or facilities
  - Individuals bragging or talking about plans to harm citizens in violent attacks or claims membership in a terrorist organization that espouses killing innocent people

- Cyber attack
  - Compromising or attempting to compromise IT infrastructure

- Aviation activity
  - Operating aircraft including radio-controlled or unmanned aerial vehicles in a suspicious manner (entering restricted airspace) or posing a threat to persons or facilities.

- Maritime activity
  - Vessels including radio-controlled vessels in unusual or restricted locations
  - Anchoring in areas not typically used for or authorized for anchoring
  - Persons attempting to buy or rent fishing or recreational boats/vehicles with cash for short term, undefined use
  - Recovering or throwing suspicious items into the water
  - Atypical light signals between boats
  - Unusual diving or night operations
  - Transferring people or things between ships and/or shore that seem unusual

- Eliciting information
  - Questioning at a level beyond mere curiosity or related to topics outside those normally raised at a facility or location by the general public
  - Questioning related to security procedures, shift changes, size of guard force, etc.
  - Questions regarding employment opportunities at locations not associated with personnel hiring

- Testing or probing of security
  - Deliberate interactions with, or challenges to personnel or facilities in an effort to reveal physical, personnel, or security capabilities
  - Testing security systems, responses and reaction times at a facility
  - Attempts to test or penetrate physical security barriers or procedures
  - Individuals in places where they do not belong
  - Individuals departing quickly when seen or approached
  - Individuals dressed inappropriately for the location or weather
  - Missing fencing or lighting near sensitive locations
  - Unattended vehicles

- Atypical photography
  - Taking pictures of buildings, facilities, or locations that would arouse suspicion in a reasonable person, e.g., visitors to a national monument or icon taking photographs of security screening points or security cameras instead of the monument or icon itself.

- Observation or surveillance inconsistent with the locale
  - Demonstrating an unusual interest in facilities, buildings, or locations beyond mere casual or professional interest.
  - Annotating maps, note-taking, or diagram drawing
  - Use of binoculars or night vision devices
  - Individuals loitering within a visitor center, parking lot, or government facility
  - Fishing or hunting in locations not typically used for those activities

- Materials acquisition/storage
  - Acquisition and storage of unusual quantities of materials causing a reasonable person to suspect possible criminal activity

- Acquisition of expertise
  - Attempts to obtain or conduct training in security concepts
  - Military weapons or tactics
  - Other unusual capabilities

- Weapons discovery

References

1. External References:

   A. *Information Sharing Environment (ISE) Functional Standards*
   <http://nsi.ncirc.gov/documents/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf>

   B. *Nationwide SAR Initiative*
   <http://nsi.ncirc.gov/documents/NSI_Overview.pdf>

   C. *Privacy, Civil Rights, and Civil Liberties Protections: A Key Component of the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)*
   <http://nsi.ncirc.gov/documents/NSI_Privacy_Briefing.pdf

   D. *NSI Training Overview*
   <http://nsi.ncirc.gov/documents/NSI_Training_Overview.pdf>

   E. *Suspicious Activity Reporting Process Implementation Checklist*
   <http://it.ojp.gov/docdownloader.aspx?ddid=1147>

   F. *Nationwide Suspicious Activity Reporting Initiative Concept of Operations*
   <http://nsi.ncirc.gov/documents/NSI_CONOPS_Version_1_FINAL_2008-12-11_r4.pdf>

   G. *National Strategy for Information Sharing*
   <http://nsi.ncirc.gov/documents/National_Strategy_for_Information_Sharing.pdf>

   H. Other on-line resources may be found at: <http://nsi.ncirc.gov/>

2. Internal References:

   DOI ISE Privacy Policy, dated September 30, 2009