



POLICY

**THE UNDER SECRETARY OF DEFENSE**  
2000 DEFENSE PENTAGON  
WASHINGTON, D.C. 20301-2000

October 1, 2010

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Directive-Type Memorandum (DTM) 10-018 – Law Enforcement Reporting of Suspicious Activity

References: See Attachment 1

Purpose. This DTM:

- In accordance with the authority in DoD Directive 5111.1 (Reference (a)) and Deputy Secretary of Defense Memorandum (Reference (b)), establishes DoD policy and procedures for the documentation, storage, and exchange of suspicious activity reports (SAR) through law enforcement channels to improve the protection of DoD personnel, facilities, and forces in transit.
- Cancels Deputy Secretary of Defense Memorandum (Reference (c)).
- Incorporates and cancels Deputy Secretary of Defense Memorandum (Reference (d)).
- Designates the eGuardian system as the authorized DoD law enforcement SAR system pursuant to Secretary of Defense Memorandum (Reference (e)).
- Is effective upon its publication on the DoD Issuances Website; it shall be converted to a new DoD issuance. This DTM shall expire effective April 5, 2011.

Applicability. This DTM applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the “DoD Components”).

Definitions. For the purpose of this DTM, “suspicious activity” is defined as observed behavior that may be indicative of intelligence gathering or other pre-operational planning related to a terrorist or other security threat to DoD interests

worldwide. See Attachment 2 for the categories of suspicious activity; SARs are a component of the overall category of force protection threat information.

Policy. It is DoD policy that:

- DoD efforts to counter terrorism and terrorist threats shall address protection of DoD personnel, facilities, and activities.
- SARs and other force protection threat information guide DoD efforts to:
  - Identify and address threats to the Department of Defense at the earliest opportunity.
  - Implement information-driven and risk-based detection, prevention, deterrence, response, and protection efforts immediately.
  - Identify persons involved in terrorism-related activities and threats to the Department of Defense.
- To strengthen DoD efforts to fight the terrorist threat:
  - Those responsible for protecting DoD resources must have timely access to properly acquired force protection threat information, particularly information that indicates a potential threat regarding those who want to attack the United States, their plans and activities, and the targets that they intend to attack.
  - SAR and force protection threat information shall be immediately available to, administered by, and shared among appropriate DoD law enforcement and security personnel in support of DoD missions to the maximum extent permitted by law, regulation, Executive order (E.O.), and directives for force protection purposes.
  - This information shall be made available to other DoD personnel to the maximum extent permitted by law, E.O., directives, and regulations for force protection purposes.
- The DoD Components shall collect, use, maintain, and disseminate personally identifiable information concerning U.S. persons in strict compliance with section 552a of title 5, United States Code (U.S.C.) (Reference (f)), implemented in the Department of Defense by DoD Directive 5400.11 and DoD 5400.11-R (References (g) and (h)), other Federal laws, and DoD regulations. The collection, use, maintenance, and

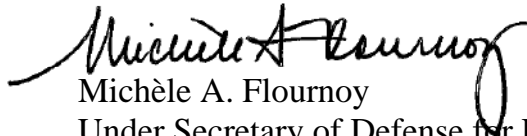
dissemination of information critical to the success of the DoD efforts to counter terrorist threats must comply with all applicable laws, regulations, and policies regarding the safeguarding of personal freedoms, civil liberties, and information privacy.

- When proposing, developing, and implementing DoD legislation, regulations, policies, and guidelines that retain or enhance a particular authority, the DoD Component shall balance the need for the power with the need to protect privacy and civil liberties; provide adequate guidelines and oversight to confine its use properly; and ensure adequate protections exist to protect privacy and civil liberties in accordance with applicable law, including Public Law 110-53 (Reference (i)).
- This policy does NOT affect existing policies governing:
  - DoD Intelligence Component activities. DoD Intelligence Components collect, retain, and disseminate information concerning U.S. persons pursuant to procedures set forth in DoD 5240.1-R (Reference (j)) and E.O. 12333 (Reference (k)).
  - DoD Component acquisition of information concerning non-DoD personnel and organizations and the sharing of terrorism information in accordance with DoD Directive 5200.27 (Reference (l)) and E.O. 13388 (Reference (m)).

Responsibilities. See Attachment 3.

Procedures. See Attachment 4.

Releasability. This DTM is approved for public release and is available on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.

  
Michèle A. Flournoy  
Under Secretary of Defense for Policy

Attachments:  
As stated

**DISTRIBUTION:**

**SECRETARIES OF THE MILITARY DEPARTMENTS  
CHAIRMAN OF THE JOINT CHIEFS OF STAFF  
UNDER SECRETARIES OF DEFENSE  
DEPUTY CHIEF MANAGEMENT OFFICER  
COMMANDERS OF THE COMBATANT COMMANDS  
CHIEF, NATIONAL GUARD BUREAU  
ASSISTANT SECRETARIES OF DEFENSE  
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE  
DIRECTOR, OPERATIONAL TEST AND EVALUATION  
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION  
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE  
ASSISTANTS TO THE SECRETARY OF DEFENSE  
DIRECTOR, ADMINISTRATION AND MANAGEMENT  
DIRECTOR, NET ASSESSMENT  
DIRECTORS OF THE DEFENSE AGENCIES  
DIRECTORS OF THE DoD FIELD ACTIVITIES**

ATTACHMENT 1

REFERENCES

- (a) DoD Directive 5111.1, “Under Secretary of Defense for Policy (USD(P)),” December 8, 1999
- (b) Deputy Secretary of Defense Memorandum, “Delegations of Authority,” November 30, 2006
- (c) Deputy Secretary of Defense Memorandum, “Implementation of Interim Threat Reporting Procedures,” September 13, 2007 (hereby cancelled)
- (d) Deputy Secretary of Defense Directive-Type Memorandum 09-001, “DoD Force Protection Threat Information,” June 19, 2009 (hereby cancelled)
- (e) Secretary of Defense Memorandum, “Law Enforcement Suspicious Activity Reporting (SAR) System – eGuardian,” May 20, 2010
- (f) Section 552a of title 5, United States Code
- (g) DoD Directive 5400.11, “DoD Privacy Program,” May 8, 2007
- (h) DoD 5400.11-R, “Department of Defense Privacy Program,” May 14, 2007
- (i) Public Law 110-53, “Implementing Recommendations of the 9/11 Commission Act of 2007,” August 3, 2007
- (j) DoD 5240.1-R, “Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons,” December 1, 1982
- (k) Executive Order 12333, “United States Intelligence Activities,” December 4, 1981, as amended
- (l) DoD Directive 5200.27, “Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense,” January 7, 1980
- (m) Executive Order 13388, “Further Strengthening the Sharing of Terrorism Information to Protect Americans,” October 25, 2005
- (n) Section 930 of title 18, United States Code
- (o) DoD Instruction 5025.01, “DoD Directives Program,” October 28, 2007
- (p) DoD 5400.7-R, “DoD Freedom of Information Act Program,” September 4, 1998
- (q) Chapter 47 of title 10, United States Code, (also known as “The Uniform Code of Military Justice”)
- (r) “Federal Bureau of Investigation (FBI) System of Records Notice,” November 23, 2008<sup>1</sup>
- (s) “Federal Bureau of Investigation Privacy Impact Assessment,” November 25, 2008<sup>2</sup>
- (t) Chapter 36 of title 50, United States Code (also known as “The Foreign Intelligence Surveillance Act,” as amended)
- (u) Section 1220.32e of title 36, Code of Federal Regulations
- (v) DoD Directive 5015.2, “DoD Records Management Program,” March 6, 2000

---

<sup>1</sup> Available at <http://www.fbi.gov/>

<sup>2</sup> Available at <http://www.fbi.gov/>

ATTACHMENT 2

CATEGORIES OF SUSPICIOUS ACTIVITY

1. ACQUISITION OF EXPERTISE. Unjustified attempts to obtain or conduct specialized training in security concepts, military weapons or tactics, or other unusual capabilities such as specialized transport or handling capabilities that would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.
2. BREACH OR ATTEMPTED INTRUSION. Unauthorized entry or attempted entry into a restricted area or protected site; impersonation of authorized personnel (e.g., police, security, or janitorial personnel).
3. ELICITING INFORMATION. Suspicious questioning of personnel by any means about particular DoD structures, functions, personnel, or procedures at the facility or infrastructure.
4. EXPRESSED OR IMPLIED THREAT. A threat to DoD personnel or threatened damage to or compromise of a DoD facility or infrastructure.
5. FLYOVER OR LANDING. Suspicious overflight of or landing near a DoD facility or infrastructure by any type of flying vehicle (e.g., airplane, helicopter, unmanned aerial vehicle, hang glider).
6. MATERIALS ACQUISITION OR STORAGE. Acquisition of unusual quantities of precursor material (e.g., cell phones, pagers, fuel, and timers); unauthorized or unlicensed individual or group attempts to obtain precursor chemicals, agents, or toxic materials; or rental of storage units for the purpose of storing precursor material, chemicals, or apparatuses for mixing chemicals.
7. MISREPRESENTATION. Misusing or presenting false insignia, documents, or identification or engaging in any other activity to misrepresent one's affiliation.

8. RECRUITING. Building operations teams and developing contacts, or collecting personnel data, banking data, or travel data under circumstances that would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

9. SABOTAGE, TAMPERING, OR VANDALISM. Damaging, manipulating, or defacing part of a DoD facility, infrastructure, or protected site. Acts of vandalism committed by DoD civilian employees, military members, or their dependents should not be reported as suspicious activity unless those acts relate to a pattern of criminal activity or otherwise would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

10. SURVEILLANCE. Monitoring the activity of DoD personnel, facilities, processes, or systems, including showing unusual interest in a facility, infrastructure, or personnel (e.g., observation through binoculars, taking notes, drawing maps or diagrams of the facility, and taking pictures or video of a facility, infrastructure, personnel, or the surrounding environment) under circumstances that would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

11. TESTING OF SECURITY. A challenge to, or a series of interactions with DoD installations, vessels, personnel, or systems that could reveal physical, personnel, or cyber security capabilities or vulnerabilities.

12. THEFT, LOSS, OR DIVERSION. Theft or loss associated with a DoD facility or infrastructure (e.g., of badges, uniforms, identification cards, emergency vehicles, technology, or documents, whether classified or unclassified) that are proprietary to the facility, or a diversion of attention from a DoD facility or infrastructure that is related to a theft or loss associated with that facility.

13. WEAPONS DISCOVERY. Discovery of weapons or explosives, as defined in section 930 of title 18, U.S.C. (Reference (n)). The discovery of personal weapons legally owned by DoD civilian employees, military members, or their dependents should not be reported as suspicious activity if the discovery is solely the result of the owner's failure to properly store or secure the weapon(s).

ATTACHMENT 3

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)). The USD(P) shall establish policies and procedures implementing this DTM consistent with the policies and procedures in References (e) through (m).

2. ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND AMERICAS' SECURITY AFFAIRS (ASD(HD&ASA)). The ASD(HD&ASA), under the authority, direction, and control of the USD(P), as the principal civilian advisor to the USD(P) and the Secretary of Defense for force protection matters, shall:

a. Oversee eGuardian management, including developing and overseeing policy for access and account management controls for the eGuardian system.

b. Establish such guidance and procedures as necessary to ensure that the DoD Components and DoD personnel with access to the eGuardian system receive training in the proper use of and safeguards for the eGuardian system.

c. Develop and oversee information-sharing policies and procedures to provide a mechanism for sharing SARs and force protection threat information among all DoD Components and personnel who support the force protection and/or antiterrorism mission.

d. Establish policies and procedures to analyze SAR data and the fusion of SAR data with other intelligence reporting.

3. DIRECTOR OF ADMINISTRATION AND MANAGEMENT (DA&M). The DA&M shall advise the ASD(HD&ASA) on the requirements of References (e), (f), (g), and (i), DoD Instruction 5205.01 (Reference (o)), and DoD 5400.7-R (Reference (p)), and facilitate compliance by the DoD Components.

4. HEADS OF THE DoD COMPONENTS WITH LAW ENFORCEMENT AGENCIES OR ACTIVITIES. The Heads of the DoD Components with law enforcement agencies or activities shall:

a. Provide adequate funding and personnel to establish and support an effective program for the use of the eGuardian system.



b. Serve as the Component Program Manager for eGuardian and the principal point of contact for law enforcement reporting of suspicious activity. The Component Program Manager or designee shall ensure that the procedures in this DTM are implemented.

c. Establish procedures, as well as rules of conduct necessary to implement procedures established by the USD(P) and this DTM, to ensure Component compliance with the requirements of References (e) through (m) and Reference (p) and such rules and regulations as may be established by the Department of Justice for the use of the eGuardian system.

d. Develop and conduct training, consistent with the requirements of this DTM and References (f) through (m) and (p), for assigned, employed, and detailed personnel with access to eGuardian, including contractor personnel and individuals having primary responsibility for implementing the eGuardian system.

e. Establish Component procedures to ensure only law enforcement personnel and analysts supporting law enforcement activities are granted account access to the eGuardian system, and ensure that all assigned personnel with access to eGuardian maintain the authorization to access the system.

f. Establish Component procedures to monitor the use of the eGuardian system and audit the reports submitted into eGuardian to ensure its use is in compliance with all applicable laws, regulations, and policies.

g. Submit to the eGuardian system all SARs dealing with information regarding a potential threat or suspicious activity, such as those listed in Attachment 2, that are related to DoD personnel, facilities, or forces in transit.

h. Develop Component quality assurance procedures to ensure DoD information reported to the eGuardian system does not violate the parameters established in paragraphs 3.b. and 3.c. of Attachment 4, and to ensure the information is as complete and useable as possible.

##### 5. COMMANDERS OF THE GEOGRAPHIC COMBATANT COMMANDS (GCC).

The Commanders of the GCCs, in addition to the responsibilities in section 4 of this enclosure, shall conduct analysis of SAR and force protection threat information to include fusing SAR reporting with all source intelligence/counterintelligence reporting. Combatant Commands will utilize this analysis to formulate protective measures and implement information-driven and risk-based detection, prevention, deterrence, response, and protection efforts immediately.

ATTACHMENT 4

eGUARDIAN PROCEDURES

1. SYSTEM DESCRIPTION

a. eGuardian is the Federal Bureau of Investigation's (FBI) unclassified, law enforcement-centric threat reporting system. It provides a means to disseminate SARs dealing with information regarding a potential threat or suspicious activity rapidly throughout the national law enforcement community.

b. All reports in the eGuardian system Shared Data Repository (SDR) are viewable through Guardian, the FBI's classified threat reporting system. DoD personnel assigned to joint terrorism task forces (JTTFs) and the National Joint Terrorism Task Force (NJTTF) have access to Guardian.

c. Guardian and eGuardian are not emergency reporting systems. Users must contact their chain of command and local JTTF in accordance with local procedures for any urgent matters with a potential link to terrorism. After emergency reporting is conducted, information may be submitted to the eGuardian system, as appropriate.

d. The eGuardian system functions as an alert, recording, and reporting system, not as a long-term data repository. Decisions regarding the status of eGuardian reports will be made promptly so that data can move quickly through the system.

2. ACCESS PROCEDURES

a. Access to the eGuardian system is via Law Enforcement Online (LEO). DoD personnel whose force protection responsibilities require access to the eGuardian system must first establish access to LEO by applying directly to the FBI for access via the LEO Website at <http://www.leo.gov/>.

b. Applications for eGuardian access shall be routed through the respective DoD Component. The DoD Component shall validate and forward access requests to the FBI eGuardian Program Manager for approval. Access is limited to law enforcement personnel and analysts supporting law enforcement functions. Law enforcement personnel supporting force protection, counterintelligence, and intelligence activities are eligible for the eGuardian system accounts and unrestricted access due to their law enforcement status. Information acquired through the eGuardian system by law enforcement personnel may be shared with counterintelligence and intelligence agencies

conducting force protection and/or counterterrorism missions in compliance with the requirements of References (f) through (m).

c. Initial access to the eGuardian system requires web-based training. All new account holders must complete this training and sign in to the eGuardian system within 30 days of being granted access to the system or their access will be terminated by the FBI. The DoD Component will monitor user training status and deactivate accounts of untrained personnel.

d. All eGuardian system users must sign the eGuardian user agreement, which reflects the conditions of use, privacy, and security requirements of the eGuardian system. Violations of the user agreement will result in the termination of access privileges, and could result in disciplinary action under chapter 47 of title 10, U.S.C., also known as "The Uniform Code of Military Justice" (Reference (q)), or other applicable provisions of law, and/or result in other adverse personnel actions.

e. There are three distinct types of eGuardian accounts approved for use by DoD personnel: user, approver, and read-only. The DoD Component will establish procedures to grant the appropriate level of access to Component personnel.

(1) User account privileges include the ability to draft SARs in the eGuardian system and the ability to view reports in the eGuardian SDR.

(2) Approver account privileges include the same privileges as user accounts, as well as the ability to approve draft SARs in the eGuardian system that are drafted by assigned user account holders.

(3) Read-only accounts will only allow the ability to view reports in the eGuardian SDR.

f. Access to and the use of information contained in the eGuardian system shall be consistent with the authorized purpose of eGuardian as identified in the applicable FBI System of Records Notice (Reference (r)) and Privacy Impact Assessment (Reference (s)).

### 3. REPORTING SUSPICIOUS ACTIVITY

a. The DoD Components with law enforcement agencies/activities shall use the eGuardian system for reporting, storing, and sharing unclassified SARs dealing with information regarding a potential threat or suspicious activity related to DoD personnel, facilities, or forces in transit (see Attachment 2).

b. No entry may be made into eGuardian based on a person's ethnicity, race, religion, or lawful exercise of rights or privileges guaranteed by the Constitution or Federal law, including First Amendment-protected freedoms of religion, speech, press, and peaceful assembly and protest, unless there exists reasonable suspicion of a direct relationship between such information and a specific criminal act or behavior that may pose a threat to DoD personnel, facilities, and forces in transit.

c. The following specific categories of information are not permitted to be entered into eGuardian: classified information; information that divulges sensitive methods and techniques; information derived in accordance with chapter 36 of title 50, U.S.C., also known as "The Foreign Intelligence Surveillance Act" (Reference (t)); grand jury information; Federal taxpayer information; sealed indictments; sealed court proceedings; confidential human source and witness information; and any other information the dissemination of which is prohibited by law. DoD Components will assign personnel to monitor the system to ensure that these categories of information are not included in eGuardian reports.

d. Only DoD law enforcement personnel or analysts supporting law enforcement functions within DoD law enforcement organizations will enter SARs into the eGuardian system. SARs may be reported to law enforcement from private citizens, DoD personnel, or may come directly from law enforcement personnel who observe or investigate activities.

e. Agencies without organic law enforcement organizations or entities will report SARs to their supporting DoD law enforcement element.

f. Once entered, draft eGuardian reports are viewable to the initial drafter, the drafter's supervisor, and the approval authority within the drafter's DoD Component.

#### 4. REVIEW PROCESS

a. DoD Components will establish a workflow that includes a review of draft eGuardian reports written by the eGuardian system users within their Component. Approval authority will not be below the level of the Component criminal investigative organization (DCIO) or designated law enforcement program office. DoD Components without a DCIO or designated law enforcement program office may request that local fusion centers, or the FBI Guardian Management Unit, will serve as the responsible entity to approve eGuardian drafts submitted by Component personnel. All reviews will ensure that the draft eGuardian report complies with the standards established within this DTM.

b. When a SAR is initiated, if the initial investigative process, which will include coordination with the supporting FBI JTTF or NJTTF, finds no link to terrorism, the SAR

will be deleted from the system and not be added to the eGuardian SDR. If a clear determination is made of a link to terrorism, the information will be passed to the eGuardian SDR for further dissemination and on to Guardian for analysis. If no clear determination can be made regarding a link to terrorism but it cannot be discounted, the information will be added to the eGuardian SDR for pattern and trend analysis. These reports will be retained in the eGuardian SDR for a period of 5 years.

c. Suspicious activity, incidents, and threats that are found to warrant investigation due to a likelihood of having a potential terrorism link will be assigned to a Defense Criminal Investigative Organization (DCIO) for investigation. The DCIO shall coordinate its activities with the supporting FBI JTTF.

d. Suspicious activity reports entered into the eGuardian SDR and resolved as having no clear link to terrorism as result of FBI JTTF or DCIO investigation will be removed from the eGuardian system after 180 days.

e. The FBI considers all reports submitted to the eGuardian system to be the property of the submitting agency; therefore, should a submitting agency desire that a report be removed from the system prior to the 5-year mark, the report will be removed. All records created or received must be maintained per authorized records schedules in accordance with section 1220.32e of title 36, Code of Federal Regulations, and DoD Directive 5015.2 (References (u) and (v)).