



Department of Defense INSTRUCTION

NUMBER 2000.26
November 1, 2011

USD(P)

SUBJECT: Suspicious Activity Reporting

References: See Enclosure 1

1. PURPOSE. This Instruction:

- a. In accordance with the authority in DoD Directive 5111.1 (Reference (a)) and Deputy Secretary of Defense Memorandum (Reference (b)), establishes DoD policy, assigns responsibilities, and prescribes 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.
- b. Delegates authorities for the effective administration of this policy.
- c. Supersedes and cancels Directive-Type Memorandum 10-018 (Reference (c)).
- d. Implements the Secretary of Defense Memorandum (Reference (d)) establishing the eGuardian system to serve as the DoD law enforcement SAR system.

2. APPLICABILITY. This Instruction applies to:

- a. 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 DoD (IG, DoD), the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Components").
- b. DoD law enforcement officers (LEOs), including police officers, investigators, criminal intelligence analysts, and their supporting antiterrorism and force protection planning personnel who are assigned, attached, or detailed to law enforcement agencies.
- c. DoD contractors who, on behalf of a DoD Component and sponsored by a law enforcement official, are involved in the SAR process, including operating a system of records as defined in the Glossary and any of the activities associated with maintaining a system of records

related to SARs, such as collecting and disseminating records, but only to the extent specified by the terms of the relevant contractual vehicle.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. DoD efforts to counter terrorism and terrorist threats shall address protection of DoD personnel, facilities, and activities.

b. The eGuardian system shall serve as the exclusive DoD law enforcement SAR system and shall be employed by DoD LEOs, analysts, and technical contractors assigned, attached, or detailed to law enforcement agencies. The eGuardian system may not be employed by non-DoD LEO personnel as defined in the Glossary.

c. SARs and other force protection threat information guide DoD efforts to:

(1) Identify and address threats to the DoD at the earliest opportunity.

(2) Implement information-driven and risk-based detection, prevention, deterrence, response, and protection efforts immediately.

(3) Identify persons involved in terrorism-related activities and threats to the DoD.

d. To strengthen DoD efforts to fight terrorist threats:

(1) 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, capabilities, and activities, and the targets that they intend to attack.

(2) 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 DoD issuances for force protection purposes.

(3) This information shall be made available to other DoD personnel to the maximum extent permitted by law, regulation, E.O., and DoD issuances for force protection purposes.

e. Personally identifiable information concerning individuals shall be handled in strict compliance with section 552a of title 5, United States Code (U.S.C.) also known as “The Privacy Act of 1974” (Reference (e)), DoD Directive 5400.11, and DoD 5400.11-R, (References (f) and (g)), other applicable laws, and regulations and policies in accordance with Director of Administration and Management (DA&M) Memorandum (Reference (h)). 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.

f. When proposing, developing, and implementing DoD-proposed legislation or DoD issuances pertaining to suspicious activity reporting that retain or enhance a particular authority, the DoD Component shall balance the need for the authority with the need to protect privacy and civil liberties; provide adequate guidelines and oversight to confine properly its use; and ensure adequate protections and training exist to protect privacy and civil liberties in accordance with applicable law, including Public Law 110-53 (Reference (i)).

g. This policy does not affect existing policies governing:

(1) DoD intelligence and counterintelligence component activities. DoD intelligence and counterintelligence 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)).

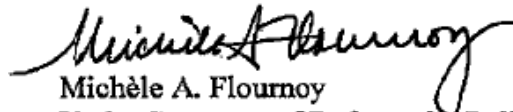
(2) DoD Component acquisition of information concerning non-DoD personnel and organizations and the sharing of terrorism information in accordance with DoD Directive 5200.27 (Reference (l)) and E.O. 13388 (Reference (m)).

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosure 3.

7. RELEASABILITY. UNLIMITED. This Instruction is approved for public release. It is available on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.

8. EFFECTIVE DATE. This Instruction is effective upon its publication to the DoD Issuances Website.


Michèle A. Flournoy
Under Secretary of Defense for Policy

Enclosures

1. References
2. Responsibilities
3. eGuardian Procedures
4. Categories of Suspicious Activities

Glossary

TABLE OF CONTENTS

ENCLOSURE 1. REFERENCES5

ENCLOSURE 2. RESPONSIBILITIES7

 UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)).....7

 ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND
 AMERICAS’ SECURITY AFFAIRS (ASD(HD&ASA)).....7

 DA&M7

 IG, DoD.....7

 GENERAL COUNSEL OF THE DoD7

 HEADS OF THE DoD COMPONENTS WITH LAW ENFORCEMENT
 AGENCIES OR ACTIVITIES8

 SECRETARY OF THE ARMY.....9

 COMMANDERS OF THE GEOGRAPHIC COMBATANT COMMANDS.9

ENCLOSURE 3. eGUARDIAN PROCEDURES10

 SYSTEM DESCRIPTION.....10

 ACCESS PROCEDURES10

 REPORTING SUSPICIOUS ACTIVITY11

 REVIEW PROCESS.....12

ENCLOSURE 4. CATEGORIES OF SUSPICIOUS ACTIVITY14

GLOSSARY16

 PART I. ABBREVIATIONS AND ACRONYMS16

 PART II. DEFINITIONS.....16

ENCLOSURE 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) Directive-Type Memorandum 10-018, “Law Enforcement Reporting of Suspicious Activity,” October 1, 2010 (hereby cancelled)
- (d) Secretary of Defense Memorandum, “Law Enforcement Suspicious Activity Reporting (SAR) System – eGuardian,” May 20, 2010 (hereby cancelled)
- (e) Sections 552a, 5541, and 8401(17)(A) and (17)(D)iii of title 5, United States Code
- (f) DoD Directive 5400.11, “DoD Privacy Program,” May 8, 2007
- (g) DoD 5400.11-R, “Department of Defense Privacy Program,” May 14, 2007
- (h) Director of Administration and Management Memorandum, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII),” June 5, 2009
- (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) DoD Instruction 5025.01, “DoD Directives System,” October 28, 2007
- (o) DoD 5400.7-R, “DoD Freedom of Information Act Program,” September 4, 1998
- (p) Chapter 47 of title 10, United States Code (also known as “The Uniform Code of Military Justice”)
- (q) Sections 641 and 930 of title 18, United States Code
- (r) “Federal Bureau of Investigation (FBI) System of Records Notice,” November 23, 2008¹
- (s) “Federal Bureau of Investigation Privacy Impact Assessment,” November 25, 2008²
- (t) Executive Order 13526, “Classified National Security Information,” December 29, 2009
- (u) Chapter 36 of title 50, United States Code (also known as “The Foreign Intelligence Surveillance Act,” as amended)
- (v) Section 1220.32e of title 36, Code of Federal Regulations
- (w) DoD Directive 5015.2 “DoD Records Management Program,” March 6, 2000
- (x) Department of Homeland Security, “Baseline Capabilities for State and Major Urban Area Fusion Centers,” September 2008³

¹ Available at <http://www.fbi.gov/>

² Available at <http://www.fbi.gov/>

³ Available at http://www.dhs.gov/files/programs/gc_1296491960442.shtm

- (y) Joint Publication 1-02, “Department of Defense Dictionary of Military and Associated Terms,” current edition
- (z) Program Manager for Information Sharing Environment (PM-ISE), “Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5,” May 21, 2009⁴

⁴ Available at http://www.ise.gov/docs/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)). The USD(P) shall establish policies and procedures implementing this Instruction 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 homeland defense activities, shall:

a. Provide DoD policy oversight for eGuardian, consistent with Enclosure 3, including developing and overseeing policy for access and account management controls for the eGuardian system.

b. Develop and manage standardized DoD 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 antiterrorism mission, including the Defense Intelligence Components (DIC).

c. In consultation with the Under Secretary of Defense for Intelligence, establish policies and procedures to analyze SAR data and for the fusion of SAR data with other intelligence reporting.

d. Interface with the Federal Bureau of Investigation (FBI) on matters related to eGuardian policies and procedures.

e. Consult with the DA&M on the requirements of References (e) through (i), (n), and (o) to facilitate compliance by DoD Components.

3. DA&M. The DA&M shall advise the ASD(HD&ASA) on the requirements of References (e) through (i), DoD Instruction 5025.01 (Reference (n)), and DoD 5400.7-R (Reference (o)), and facilitate compliance by the DoD Components.

4. IG, DoD. The IG, DoD shall monitor compliance with this Instruction as it relates to the Defense criminal investigative organizations (DCIOs).

5. GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE. The General Counsel of the Department of Defense shall provide advice and assistance on all legal matters, including the

review and coordination on all proposed policies, DoD issuances, and proposed exceptions to the DoD policies regarding the eGuardian system.

6. 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. Provide for the management of the Component's eGuardian program and the oversight of Component law enforcement reporting of suspicious activity. The DoD Component Head shall ensure that the procedures in this instruction are implemented.

c. Establish procedures, as well as rules of conduct necessary to implement this Instruction, to ensure Component compliance with the requirements of References (f) through (m) and Reference (o) 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 Instruction and References (e) through (m) and (o), for assigned, employed, and detailed personnel prior to initial 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 who are assigned, attached, or detailed to 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 Component's use of the eGuardian system for compliance with use requirements 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 Enclosure 4, 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 Enclosure 3, and to ensure the information is as complete and useable as possible.

i. Develop Component-specific suspicious activity awareness campaigns to enhance detection, prevention, and protection efforts.

7. SECRETARY OF THE ARMY. The Secretary of the Army, in addition to the responsibilities in section 6 of this enclosure, shall:

- a. Provide overall program management for DoD's use of the eGuardian system.
- b. Report violations and investigative findings of Reference (h) to ASD(HD&ASA).
- c. Coordinate with DoD Component Heads to ensure compliance with the eGuardian system account management requirements and establish procedures for the execution of bi-annual audits of all DoD Component accounts to ensure eGuardian system access is limited to authorized personnel.
- d. Establish 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.
- e. Establish and maintain a Secret Internet Protocol Router website for sharing eGuardian SAR and force protection threat information with DICs in accordance with the legal and regulatory requirements in References (f) through (m).
- f. Through the ASD(HD&ASA):
 - (1) Engage with the FBI on matters related to eGuardian procedures and training.
 - (2) Coordinate and identify funding requirements from DoD Components for the use of the eGuardian system and ancillary technical support to the FBI.
- g. Coordinate with the FBI eGuardian Management Unit for the suspension of individual eGuardian system access for failure to comply with paragraphs 7.b. and 7.c. of this enclosure, until the responsible DoD Component provides evidence of remediation.

8. COMMANDERS OF THE GEOGRAPHIC COMBATANT COMMANDS. The Commanders of the Geographic Combatant Commands, in addition to the responsibilities in section 6 of this enclosure, shall conduct analysis of SAR and force protection threat information, including fusing suspicious activity reporting with all source intelligence and counterintelligence reporting. Combatant Commands will utilize this analysis to formulate protective measures and implement information-driven notification and risk-based detection, prevention, deterrence, response, and protection efforts immediately.

ENCLOSURE 3

eGUARDIAN PROCEDURES

1. SYSTEM DESCRIPTION

a. 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.

b. 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.

c. 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. DoD personnel whose law enforcement responsibilities require access to the eGuardian system must first establish access to Law Enforcement Online by applying directly to the FBI for access via the Law Enforcement Online 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 Management Unit (e-guard-mod@leo.gov) for approval. DoD access is limited to law enforcement personnel and analysts assigned, attached, or detailed to support DoD law enforcement organizations. DoD law enforcement personnel and analysts assigned, attached, or detailed to a DoD law enforcement agency supporting force protection, counterintelligence, and intelligence activities are eligible for eGuardian system accounts and unrestricted access due to their law enforcement status. Information acquired through the eGuardian system by DoD law enforcement personnel may be shared with counterintelligence and intelligence agencies conducting force protection and counterterrorism missions in compliance with the requirements of References (e) through (m).

c. Initial access to the eGuardian system requires completion of a training module that addresses standards for reporting and protection of privacy and civil liberties. 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 FBI Information Technology and Information Systems Rules of Behavior for General Users Agreement Form. 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 (UCMJ)” (Reference (p)), or other applicable provisions of law, and result in other adverse personnel actions.

e. Information obtained through eGuardian shall not be disseminated outside of the DoD without the approval of the originating agency, a representative of a fusion or intelligence center, a member of the JTTF, or an FBI eGuardian administrator. The misuse, theft, or conversion of eGuardian records for personal use or the use of another person is a criminal violation of section 641, chapter 31 of title 18, U.S.C. (Reference (q)).

f. There are four distinct types of eGuardian accounts approved for use by DoD personnel: user, supervisor, 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) Supervisor account privileges include the same privileges as user accounts as well as the ability to edit a report and return it to the user for corrections prior to referral to the approver.

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

g. Access to and 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 and activities shall use the eGuardian system exclusively 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 Enclosure 4).

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 pursuant to E. O. 13526 (Reference (t)); 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 (u)); 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 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. DoD Components 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 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 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 Instruction.

b. When suspicious activity is reported, if the initial investigative process by the reporting law enforcement agency, 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 believed to warrant investigation due to the possibility they are an indicator of potential terrorist activity will be referred to the local FBI JTTF and the appropriate DoD criminal investigative unit supporting the DoD Component.

d. SARs entered into the eGuardian SDR and resolved as having no clear link to terrorism as a 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 DoD Component 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 (v) and (w)).

ENCLOSURE 4

CATEGORIES OF SUSPICIOUS ACTIVITY

This enclosure describes the potential categories to consider when evaluating suspicious activity.

a. 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.

b. 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).

c. Eliciting Information. Suspicious questioning of personnel by any means about particular DoD structures, functions, personnel, or procedures at the facility or infrastructure.

d. Expressed or Implied Threat. A threat to DoD personnel or threatened damage to or compromise of a DoD facility or infrastructure.

e. 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).

f. 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.

g. Misrepresentation. Misusing or presenting false insignia, documents, or identification or engaging in any other activity to misrepresent one's affiliation.

h. 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.

i. 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, Service 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.

j. 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.

k. Testing of Security. A challenge to, or a series of interactions with DoD installations, vessels, personnel, or systems that could reveal physical, personnel, or capabilities vulnerabilities.

l. 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.

m. Weapons Discovery. Discovery of weapons or explosives, as defined in section 930 of Reference (q). The discovery of personal weapons legally owned by DoD civilian employees, Service 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 weapons.

n. Unexplained Absences of International Military Students. International military students who are unexpectedly absent from scheduled activities when the absence is without proper authorization and lasts more than 24 hours, and an appropriate official with the host DoD organization determines that the absence is not due to a misunderstanding in scheduling, to sickness, or to another similar reason.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASD(HD&ASA)	Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs
DA&M	Director of Administration and Management
DCIO	Defense criminal investigative organization
DIC	Defense Intelligence Component
E.O.	Executive order
FBI	Federal Bureau of Investigation
GS	General Schedule
IG, DoD	Inspector General of the Department of Defense
JTTF	joint terrorism task force
LEO	law enforcement officer
NJTTF	National Joint Terrorism Task Force
SAR	suspicious activity report
SDR	shared data repository
UCMJ	Uniform Code of Military Justice
U.S.C.	United States Code
USD(P)	Under Secretary of Defense for Policy

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this Instruction.

DoD law enforcement organizations. Organizations, agencies, entities, and offices of the Military Departments and Defense Agencies and the DoD Inspector General that perform a law enforcement function for those departments and agencies and are manned by DoD LEOs.

DoD LEO. In accordance with sections 5541 and 8401(17)(A) and (17)(D)iii of Reference (e), the DoD LEOs defined here are considered Federal LEOs.

Military police (Army and Marine Corps), security forces (Air Force), and Masters-at-Arms (Navy) who wear a military uniform with police identification while on duty; and DoD Component civilian police (General Schedule (GS) 0083 series or equivalent, consistent with the definitions of “law enforcement officer” in Reference (e)) when credentialed to perform those duties in accordance with the UCMJ.

Military and civilian (GS 1811, consistent with the definitions of “law enforcement officer” in Reference (e)) criminal investigators (special agents).

eGuardian. The 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.

fusion center. Defined in Baseline Capabilities for State and Major Urban Area Fusion Centers (Reference (x)).

individual. In accordance with section 522a (a) (2) of Reference (e), a citizen of the United States or an alien lawfully admitted for permanent residence.

non-DoD LEO personnel. The following categories of DoD personnel are not considered to be DoD LEOs or Federal LEOs:

DoD intelligence, analytical, personnel security, and contractor personnel who are not employed in support of DoD law enforcement agencies.

Antiterrorism and force protection officers who are not assigned, attached, or detailed to law enforcement activities.

Persons conducting counterintelligence activities in the Military Department Counterintelligence Organizations, Defense Agencies, Combatant Commands, or DoD Field Activities.

Corrections specialists who are not DoD LEO.

personnel. Defined in Joint Publication 1-02 (Reference (y)).

suspicious activity. Defined in Information Sharing Environment Functional Standard Suspicious Activity Reporting Version 1.5 (Reference (z)).

system of records. In accordance with section 522a (a) (5) of Reference (e), a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.