Department of Defense
INSTRUCTION

NUMBER 2000.26
September 23, 2014
Incorporating Change 1, May 12, 2017

USD(P)

SUBJECT: Suspicious Activity Reporting (SAR)

References: See Enclosure 1

1. PURPOSE. This instruction:

a. In accordance with the authority in DoD Directive (DoDD) 5111.1 (Reference (a)) and Deputy Secretary of Defense Memorandum (Reference (b)), reissues DoD Instruction (DoDI) 2000.26 (Reference (c)) to establish policy, assign responsibilities, and provide procedures implementing eGuardian as the DoD Law Enforcement (LE) SAR system.

b. Delegates authorities for the effective administration of this instruction.

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 Defense Agencies with law enforcement authority, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

b. DoD law enforcement officers (LEOs) and those working in a direct LE capacity, and antiterrorism analysts and planners supporting an LE mission, who are assigned, attached, or detailed to law enforcement agencies (LEAs).

c. DoD personnel designated as antiterrorism officers (ATOs) at the geographic Combatant Commands and Military Departments/Services and installations that directly support operations and planning and indirectly support LE missions and agencies.

d. DoD contractors who, on behalf of a DoD Component and sponsored by an LEA, 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.

e. Authorized LE criminal intelligence activities working in a direct LE capacity carried out by the Defense Intelligence Components.

3. POLICY. It is DoD policy that:

a. The eGuardian system will serve as the exclusive DoD unclassified LE SAR system and will be employed by DoD LEOs, antiterrorism operations personnel, planners, analysts supporting an LE mission, and contractors assigned, attached, or detailed to LEAs.

b. SARs and other threat information guide DoD efforts in force protection 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, criminal-related activities, and threats directed against the DoD.

(4) Assist commanders by providing and using criminal intelligence when establishing appropriate force protection conditions in accordance with DoDI 5525.18 (Reference (d)).

c. To strengthen efforts to protect DoD resources from terrorist and criminal threats:

(1) DoD LEOs and ATOs ensure that those responsible for the analysis and planning for the protection of DoD resources have timely threat information, particularly information that indicates a potential threat regarding:

(a) Those who want to attack the United States.

(b) Their plans, capabilities, and activities.

(c) The targets that they intend to attack.

(2) SAR and threat information will be appropriately secured, administered, immediately shared, and made available throughout the information life cycle to:

(a) Any DoD LEOs, ATOs, or those working in a direct LE capacity.

(b) Analysts supporting an LE mission.

(c) Their supporting operations and planning personnel who are assigned, attached, or detailed to LEAs in support of DoD missions for protection purposes to the maximum extent permitted by law, regulation, executive order (E.O.), and DoD issuances.

d. Personally identifiable information concerning individuals will 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," DoDD 5400.11, and DoD 5400.11-R (References (e), (f), and (g)); and other applicable laws; and regulations and policies in accordance with the Director of Administration and Management Memorandum (Reference (h)).

(1) Procedure 12 of DoD 5240.1-R (Reference (i)) applies to DoD intelligence components unless they are authorized by the Secretary of Defense or a designated representative to conduct LE activities in accordance with DoDI 3025.21 (Reference (j)). Authorized Defense Intelligence Component activities under Procedure 12 of Reference (i) include transfer of U.S. personally identifying information, which has been:

(a) Received and inadvertently collected in accordance with Procedures 1 and 2 of Reference (i).

(b) Temporarily retained for determination in accordance with Procedure 3 of Reference (i) to the appropriate LEA for further action.

(2) The collection, use, maintenance, and dissemination of information critical to the success of the DoD efforts to counter terrorist and other criminal threats must comply with all applicable laws, regulations, and policies regarding the safeguarding of personal freedoms, civil liberties in accordance with DoDI 1000.29 (Reference (k)), and information privacy.

e. 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 will 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 and DoDD 5200.27 (References (l) and (m)).

f. This policy does not affect existing policies governing:

(1) Defense Intelligence Component activities that collect, retain, and disseminate information concerning U.S. persons pursuant to and in compliance with procedures in DoDD 5240.06, DoDD 5240.01, E.O. 12333 (References (n), (o), and (p)), and Reference (i).

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

(3) Counterintelligence awareness and reporting requirements in accordance with Reference (p).

g. DoD personnel supporting intelligence missions or conducting intelligence-related activities will not have accounts with or access to the eGuardian system. Such personnel may request information through authorized eGuardian users when the requested information:

(1) Is within the requestor's authorized mission and activities.

(2) Involves DoD equities and has a foreign nexus.

(3) Can be collected, retained, and disseminated in accordance with Reference (i).

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3.

6. RELEASABILITY. **Cleared for public release**. This instruction is available on ~~the Internet from~~ the DoD Issuances Website at http://www.dtic.mil/whs/directives.

7. EFFECTIVE DATE. This instruction~~:~~ *is effective September 23, 2014.*

~~a. Is effective September 23, 2014.~~

~~b. Will expire effective September 23, 2024 if it hasn't been reissued or cancelled before this date in accordance with DoDI 5025.01 (Reference (r)).~~

Christine E. Wormuth
Under Secretary of Defense for Policy

Enclosures
1. References
2. Responsibilities
3. eGuardian Procedures

Glossary

TABLE OF CONTENTS

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) DoD Instruction 2000.26, "Suspicious Activity Reporting," November 1, 2011 (hereby cancelled)
(d) DoD Instruction 5525.18, "Law Enforcement Criminal Intelligence (CRIMINT) in DoD," October 18, 2013
(e) Title 5, United States Code
(f) DoD Directive 5400.11, "DoD Privacy Program," ~~May 8, 2007, as amended~~ *October 29, 2014*
(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) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 7, 1982*, as amended*
(j) DoD Instruction 3025.21, "Defense Support of Civilian Law Enforcement Agencies," February 27, 2013
(k) DoD Instruction 1000.29, "DoD Civil Liberties Program," May 17, 2012*, as amended*
(l) Public Law 110-53, "Implementing Recommendations of the 9/11 Commission Act of 2007," August 3, 2007
(m) DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense," January 7, 1980
(n) DoD Directive 5240.06, "Counterintelligence Awareness and Reporting (CIAR)," May 17, 2011, as amended
(o) DoD Directive 5240.01, "DoD Intelligence Activities" August 27, 2007, as amended
(p) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
(q) Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," October 25, 2005
~~(r) DoD Instruction 5025.01, "DoD Issuances Program," June 6, 2014~~
(~~s~~*r*) DoD Instruction 5240.26, "Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat," May 4, 2012, as amended
(~~t~~*s*) ~~DoD 5400.7-R, "DoD Freedom of Information Act Program," September 4, 1998, as amended~~ *DoD Directive 5400.07, "DoD Freedom of Information Act (FOIA) Program," January 2, 2008*
(~~u~~*t*) DoD Directive 5145.01, "General Counsel of the Department of Defense (GC DoD)," December 2, 2013, as amended
(~~v~~*u*) Chapter 47 of Title 10, United States Code (also known as "The Uniform Code of Military Justice")
(~~w~~*v*) Title 18, United States Code

(~~x~~*w*) Federal Bureau of Investigation, "FBI Privacy Act Systems of Records," current edition,[1] (also known as Federal Register Volume 66, Issue 107, June 4, 2001)

(~~y~~*x*) Federal Bureau of Investigation, "Privacy Impact Assessment for the eGuardian Threat Tracking System," current edition[2]

(~~z~~*y*) Executive Order 13526, "Classified National Security Information," December 29, 2009

(~~aa~~*z*) Chapter 36 of Title 50, United States Code (also known as "The Foreign Intelligence Surveillance Act," as amended)

(~~ab~~*aa*) ~~Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," current edition~~ *Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition*

[1] http://www.fbi.gov/foia/privacy-act/systems-records

[2] http://www.fbi.gov/foia/privacy-impact-assessments/eguardian-threat

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)). The USD(P) establishes policies and procedures implementing this instruction consistent with the policies and procedures in References (f) through (q).

2. ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND ~~AMERICAS' SECURITY AFFAIRS (ASD(HD&ASA))~~ *GLOBAL SECURITY (ASD(HD&GS))*. Under the authority, direction, and control of the USD(P) and as the principal civilian advisor to the USD(P) and the Secretary of Defense for homeland defense activities, the ~~ASD(HD&ASA)~~ *ASD(HD&GS)*:

a. Provides DoD oversight for eGuardian, consistent with Enclosure 3 of this instruction, including developing and overseeing policy for access, programming, and account management controls for the eGuardian system.

b. Develops and manages standardized DoD information-sharing policies and procedures to provide a mechanism for sharing SAR and threat information among all DoD Components and personnel who support the LE, security, Defense Critical Infrastructure, and antiterrorism missions, including the Defense Intelligence Components.

c. In consultation with the Under Secretary of Defense for Intelligence, develops policies and procedures to analyze SAR data and for the fusion of SAR data in accordance with policies governing:

(1) Defense Intelligence Component activities that collect, retain, and disseminate information concerning U.S. persons pursuant to procedures in References (i) and (p).

(2) DoD Intelligence Component acquisition of information concerning non-DoD personnel and organizations and the sharing of terrorism information in accordance with DoDI 5240.26 (Reference (~~sr~~)).

d. Interfaces with the Federal Bureau of Investigation (FBI) on matters related to eGuardian policies, funding, and procedures in accordance with Reference (j).

e. Consults with the Director of Administration*, Office of the Deputy Chief Management Officer,* on the requirements of References (f) through (h), References (k), (m), (p), and ~~DoD 5400.7-R~~ *DoDD 5400.07* (Reference (~~ts~~)) to facilitate compliance by DoD Components.

f. In coordination with the Secretary of the Army:

(1) Interfaces with the FBI on matters related to eGuardian procedures and training.

(2) Coordinates and identifies funding requirements from DoD Components for the use of the eGuardian system and ancillary technical support to the FBI.

(3) Coordinates with the FBI eGuardian Management Unit for the suspension of individual eGuardian system access due to information reported in accordance with paragraphs 6.b. and 6.c. of this enclosure, until the responsible DoD Component provides evidence of remediation.

3. DIRECTOR OF ADMINISTRATION*, OFFICE OF THE DEPUTY CHIEF MANAGEMENT OFFICER*. Under the authority, direction, and control of the Deputy Chief Management Officer, the Director of Administration~~,~~ advises the ~~ASD(HD&ASA)~~ *ASD(HD&GS)* on the requirements of References (f) through (h) (k), (m), and (p), and facilitates compliance by the DoD Components.

4. GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE. In accordance with DoDD 5145.01 (Reference (~~ut~~)), the General Counsel of the Department of Defense provides 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.

5. DoD COMPONENT HEADS WITH LAW ENFORCEMENT AGENCIES OR ACTIVITIES. The DoD Component heads with LEAs or activities:

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 DoD Component's eGuardian program and the oversight of DoD Component LE SAR. The DoD Component heads 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 DoD Component compliance with the requirements of References (f) through (~~ts~~), chapter 47 of Title 10, U.S.C., also known as "The Uniform Code of Military Justice" (UCMJ) (Reference (~~v~~*u*)), 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 (f) through (~~v~~*u*), for assigned, employed, and detailed personnel before initial access to eGuardian.

e. Ensure that LEOs and those working in a direct LE capacity, ATOs and antiterrorism analysts, and planners supporting an LE mission and operations, who are assigned, attached, or detailed to LEAs are granted account access to and are using the eGuardian system, and ensure

that all assigned personnel with access to eGuardian maintain the authorization to access the system.

f. Establish DoD Component procedures to monitor the DoD 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 suspicious activity in the categories listed in paragraph 3.a. of Enclosure 3, that are related to DoD personnel, facilities, or forces in transit.

h. Ensure that eGuardian users are aware that SAR information may be shared with DoD non-Criminal Justice Authorities (CJAs), whose missions include responsibilities for DoD insider terrorist threats, foreign terrorist threats, and antiterrorism and force protection measures as defined by Reference (~~*s*~~*r*). Originating LEAs retain responsibility for their shared SAR with a DoD non-CJA. Additionally, military counterintelligence organizations, including the Air Force Office of Special Investigations, the Naval Criminal Investigative Service, and the Army Criminal Investigation Command, should ensure that information obtained on threats to DoD forces or interests is, if required, reported or tear-lined down to the Unclassified/For Official Use Only (U//FOUO) level to provide awareness of potential threats to U.S. or DoD interests.

i. Develop DoD Component quality assurance procedures to ensure that:

(1) DoD information reported to the eGuardian system does not violate the parameters established in paragraphs 3b and 3c of Enclosure 3.

(2) The information is as complete and useable as possible.

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

k. Coordinate with the Secretary of the Army, who provides overall program management for DoD's use of the eGuardian Program, and report compliance with account management, training, and SAR accountability as part of the quarterly audit process.

6. SECRETARY OF THE ARMY. In addition to the responsibilities in section 5 of this enclosure, the Secretary of the Army:

a. Provides overall program management for the DoD's use of the eGuardian system.

b. Reports violations and investigative findings of References (h) and (m) to the ~~ASD(HD&ASA)~~ *ASD(HD&GS)*.

c. Coordinates with the other DoD Component heads to ensure compliance with the eGuardian system account management requirements, and establishes procedures for the

execution of quarterly audits of all DoD Component accounts to ensure eGuardian system access is limited to authorized personnel.

d. Coordinates with the other DoD Component heads to ensure proper reporting and accounting of SARs within the eGuardian system.

e. Establishes 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.

7. GEOGRAPHIC COMBATANT COMMANDERS. In addition to the responsibilities in section 5 of this enclosure, the geographic Combatant Commanders are responsible for continuously formulating protective measures and implementing information-driven notification and risk-based detection, prevention, deterrence, response, and protection efforts based on the SAR and threat information analysis for force protection purposes.

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. Access to Guardian information is coordinated through the JTTFs or NJTTF.

b. eGuardian is not an emergency reporting system. 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. Law Enforcement personnel must validate eGuardian reports promptly so that data can move quickly through the system.

2. ACCESS PROCEDURES

a. Access to the eGuardian system is online. DoD personnel whose LE responsibilities require access to the eGuardian system must go to the Law Enforcement Enterprise Portal (LEEP) at https://www.cjis.gov and establish an account. Contractors must have a sponsorship from a current FBI employee, with an active LEEP account.

b. Applications for eGuardian access are routed through the respective DoD Component eGuardian Program Manager. The program manager validates and forwards access requests to the FBI eGuardian Management Unit for approval. DoD access is limited to DoD LEOs and those working in a direct LE capacity, who are eligible for eGuardian system accounts and may have unrestricted access due to their LE status. ATOs and antiterrorism analysts and planners supporting LE missions and operations, who are assigned, attached, or detailed to an LEA, will have "read only" access. DoD LE personnel acquiring information through the eGuardian system may share with intelligence component agencies conducting force protection and counterterrorism missions in compliance with the requirements of References (k) through (o) and (~~t~~*s*).

c. Initial access to the eGuardian system requires completion of the SAR Line Officer Training video at http://nsi.ncirc.gov/training_online.aspx 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 Components will monitor user training status and deactivate accounts of untrained personnel.

d. Information obtained through eGuardian will 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 of Title 18, U.S.C. (Reference (~~w~~*v*)).

e. Once the originating agency approves dissemination of eGuardian information to the local Threat Working Group, they may analyze the data to assist commanders with appropriate threat-based risk decisions.

f. There are four distinct types of eGuardian accounts approved for use by DoD personnel: user, supervisor, approver, and read-only. The DoD Components establish procedures to grant the appropriate level of access to DoD 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 before referral to the approver.

(4) Read-only accounts only allow the ability to view reports in the eGuardian SDR. The read-only accounts are appropriate for ATOs, analysts, planners, and support personnel who are not credentialed LEOs.

g. Access to and use of information contained in the eGuardian system is consistent with the authorized purpose of eGuardian as identified in the applicable FBI System of Records Notice (Reference (~~x~~*w*)) and Privacy Impact Assessment (Reference (~~y~~*x*)).

3. REPORTING SUSPICIOUS ACTIVITY

a. The DoD Components with LEAs and activities 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. When submitting a report consider these categories, as defined in the Glossary, when evaluating suspicious activity:

(1) Acquisition of expertise.

(2) Breach or attempted intrusion.

(3) Eliciting information.

(4) Expressed or implied threat.

(5) Flyover or landing.

(6) Materials acquisition or storage.

(7) Misrepresentation.

(8) Recruiting.

(9) Sabotage, tampering, or vandalism.

(10) Surveillance.

(11) Testing of security.

(12) Theft, loss, or diversion.

(13) Weapons discovery.

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 U.S. Constitution or Federal law, including First Amendment-protected freedoms of religion, speech, press, and peaceful assembly and protest, unless expressly authorized by statute, by the person about whom the entry is about, or unless pertinent to and within the scope of an authorized law enforcement activity.

c. The following specific categories of information are not permitted to be entered into eGuardian: classified information pursuant to E.O. 13526 (Reference (~~z~~*y*)); information that divulges sensitive methods and techniques derived in accordance with chapter 36 of Title 50, U.S.C., also known as "The Foreign Intelligence Surveillance Act" (Reference (~~aa~~*z*)); 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 LEOs and those working in a direct LE capacity will enter SARs into the eGuardian system. SARs may be reported to LE by private citizens and all government personnel, or may come directly from LE personnel who observe or investigate activities.

e. DoD Components without organic LE organizations or entities will report suspicious activity to their supporting DoD LE element.

f. Once entered, draft eGuardian reports are viewable by 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 DoD Component. Approval authority will not be below the level of the DoD Component defense criminal investigative organization (DCIO) or designated LE program office. DoD Components without a DCIO or designated LE 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 DoD 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, and any initial investigative process undertaken by the reporting LEA, which will include coordination with the supporting FBI JTTF or NJTTF, finds no suspicious activity, link to terrorism, or criminal activity, the reporting LEA or FBI will delete the SAR from the system. If there is an appearance of terrorism, criminal activity, or suspicious activity, the information will be passed to the eGuardian SDR for further dissemination and on to Guardian for analysis. These reports will be retained in the eGuardian SDR for a period not to exceed 5 years.

c. Reports of suspicious activity, incidents, and threats entered into the eGuardian system are transferred into Guardian. Once in Guardian, a task force officer assigned to a regional JTTF or the NJTTF will conduct an assessment of the incident to determine if there is a nexus to terrorism. A "yes" nexus to terrorism will result in the FBI taking further action as dictated by FBI policy. DoD Component criminal or counterintelligence investigative units may conduct collateral or joint investigations into these incidents. Those SAR assessed to have no nexus to terrorism, but that contain indicators of criminality, will be referred to the appropriate DCIO or LEA for action.

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. DoD LEA will make every effort to enter SARs into the eGuardian system at the local level. If DoD LEA is not available, local civilian LE personnel may enter SARs into the eGuardian system on behalf of the DoD. DoD Components without organic LE organizations or entities will report SARs to their supporting DoD LE element.

f. DoD Components will maintain a record of all SARs entered into the eGuardian system and account for the SARs through the quarterly audit process.

5. QUARTERLY AUDIT PROCESS

a. Participating DoD Components track, compile, and report quarterly eGuardian program information represented below to the designated eGuardian program manager as indicated in section 7 of Enclosure 2 of this instruction.

b. The information in Figures 1 and 2 informs the DoD Components and the ~~ASD(HD&ASA)~~ *ASD(HD&GS)* of how the eGuardian system is used to enable reviews for compliance with training and use requirements, and supports funding requests from the DoD Components for the eGuardian system and FBI technical support.

Figure 1. eGuardian Quarterly Usage Report

eGuardian Quarterly Usage Report

As of

Agency	**# of Accounts**	# of Active / Existing Accounts	# of New Accounts for the FY					# of Accounts inactivated			**Total # of SARS**	# of Active / Existing SARS	# of New DoD SARs Entered into eGuardian for the FY					# of DoD SARS Invest/Terrorist NEXUS
			Year End	QTR 1	QTR 2	QTR 3	QTR 4	Year End	Time	Violation			Year End	QTR 1	QTR 2	QTR 3	QTR 4	
Total																		

Explanition of Termination of eGuardian Account(s) for Non-Compliance with Applicable Law and Policy

Significant Activity/Best Practices

Challenges/Support Required

Figure 2. eGuardian Quarterly Training Report

eGuardian Quarterly Training Report																
As of																
Agency	# of Live Training Events for the FY					# of Telecon/ComputerTraining Events for the FY					# of People Trained				
	Year End	QTR 1	QTR 2	QTR 3	QTR 4	Year End	QTR 1	QTR 2	QTR 3	QTR 4	Year End	QTR 1	QTR 2	QTR 3	QTR 4
Total															
Significant Activity/Best Practices															
Challenges/Support Required															

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

~~ASD(HD&ASA)~~	~~Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs~~
ASD(HD&GS)	*Assistant Secretary of Defense for Homeland Defense and Global Security*
ATO	antiterrorism officer
CJA	Criminal Justice Authorities
DCIO	defense criminal investigative organization
DoDD	Department of Defense directive
DoDI	Department of Defense instruction
E.O.	Executive order
FBI	Federal Bureau of Investigation
GS	General Schedule
JTTF	joint terrorism task force
LE	law enforcement
LEA	law enforcement agency
LEEP	Law Enforcement Enterprise Portal
LEO	law enforcement officer
NJTTF	National Joint Terrorism Task Force
SAR	suspicious activity reporting
SDR	shared data repository
U.S.C.	United States Code
UCMJ	Uniform Code of Military Justice
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.

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.

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).

criminal justice authorities. Personnel that operate under the rule of law and are the principal means of maintaining the rule of law within a society.

defense criminal investigative organizations. The four criminal investigative organizations of DoD are the Defense Criminal Investigative Service, the U.S. Army Criminal Investigations Command, the Naval Criminal Investigative Service, and the Air Force Office of Special Investigations.

Defense Intelligence Component. Refers to all DoD organizations that perform national intelligence, Defense Intelligence, and intelligence-related functions, including: the Defense Intelligence Agency; the National Geospatial-Intelligence Agency, the National Reconnaissance Office, the National Security Agency/Central Security Service, and the intelligence elements of the Active and Reserve Components of the Military Departments, including the U.S. Coast Guard when operating as a service in the Navy.

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

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

Army and Marine Corps Military Police, Air Force Security Forces, and Navy Masters-at-Arms who wear a military uniform with police identification while on duty; and DoD Component civilian police (e.g., 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 (e.g., GS 1811, consistent with the definitions of "law enforcement officer" or "special agents" in Reference (e)) criminal investigators.

eGuardian. The FBI unclassified, LE-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 LE community.

eliciting information. Suspicious questioning of personnel by any means about particular DoD structures, functions, personnel, or procedures.

expressed or implied threat. A threat to DoD personnel or threatened damage to or compromise of a DoD facility or infrastructure.

flyover or landing. A suspicious low flight by any type of flying vehicle (e.g., airplane, helicopter, unmanned aerial vehicle, hang glider) over a DoD facility or infrastructure or nearby landing by such flying vehicle.

force protection. Defined in ~~Joint Publication 1-02~~ *the DoD Dictionary of Military and Associated Terms* (Reference (~~ab~~*aa*)).

fusion center. Focal points within the State and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the Federal Government and State, local, tribal, territorial, and private sector partners.

individual. In accordance with section 552a(a)(2) of Reference (e), a citizen of the United States or an alien lawfully admitted for permanent residence.

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.

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

LEO. A government employee who is responsible for the prevention, investigation, apprehension, or detention of individuals suspected or convicted of offenses against the criminal laws, including an employee engaged in this activity who is transferred to a supervisory or administrative position; or serving as a probation or pretrial services officer.

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

DoD intelligence, analytical, personal security, and contractor personnel who are not employed in support of DoD LEAs.

Antiterrorism and force protection officers who are not assigned, attached, or detailed to LE 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 LEOs.

personnel. Defined in Reference (~~ab~~*aa*).

recruiting. The process of an individual spotting, assessing, and developing contacts in order to establish control over another individual who, wittingly or unwittingly, accepts tasking as a result of the established relationship in order to collect information on structures, functions, personnel, or procedures.

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.

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.

suspicious activity. Observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.

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.

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.

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.

Threat Working Group (TWG). The TWG meets at least quarterly to develop, refine, and review terrorism threat assessments and coordinate and disseminate threat warnings, reports, and summaries throughout the Component. The TWG membership includes the ATO; intelligence, investigative, and LE/security representatives; medical representatives; CBRNE specialists if applicable and appropriate representation from direct-hire, contractor, local, State, Federal, and host-nation LE agencies.

weapons discovery. Discovery of weapons or explosives, as defined in section 930 of Reference (~~v~~*u*). 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.