DoD Instruction 2000.26

DoD Use of the Federal Bureau of Investigation (FBI) eGuardian System

Originating Component:	Office of the Under Secretary of Defense for Policy
Effective:	December 4, 2019
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Instruction 2000.26, "Suspicious Activity Reporting (SAR)," September 23, 2014, as amended
Approved by:	John C. Rood, Under Secretary of Defense for Policy

Purpose: This issuance:

- In accordance with the authority in DoD Directive (DoDD) 5111.1 and the November 30, 2006, Deputy Secretary of Defense Memorandum, reissues DoD Instruction (DoDI) 2000.26 to establish policy, assign responsibilities, and prescribe procedures for DoD use of the FBI eGuardian system ("eGuardian");
- Delegates authorities to enable the effective administration of the eGuardian system;
- Designates the Secretary of the Army as the DoD Program Manager for DoD use of the eGuardian system;
- Establishes the eGuardian Working Group (eGWG) to oversee DoD use of the eGuardian system and facilitate compliance with this issuance and all applicable laws and policies; and
- Implements Part 23 of Title 28, Code of Federal Regulations (CFR), as applicable to DoD use of the eGuardian system.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION 3
1.1. Applicability. 3
1.2. Policy. 3
SECTION 2: RESPONSIBILITIES 6
2.1. Under Secretary of Defense for Policy (USD(P)) 6
2.2. Assistant Secretary of Defense for Homeland Defense and Global Security (ASD(HD&GS)). 6
2.3. CMO. 7
2.4. Director, Pentagon Force Protection Agency (PFPA). 7
2.5. General Counsel of the Department of Defense. 7
2.6. DoD Component Heads with LEAs. 7
2.7. DoD Component Heads. 8
2.8. OSD Component Heads. 8
2.9. Secretary of the Army. 8
2.10. Geographic Combatant Commanders. 9
SECTION 3: EGUARDIAN PROCEDURES 10
3.1. Purpose and Use of the eGuardian System. 10
3.2. System Description. 10
3.3. Access Procedures. 10
a. Access Policy. 10
b. General Access Requirements. 11
c. Account Types. 12
d. Application for Access Procedures. 12
3.4. Sharing Information in the eGuardian System. 13
3.5. Reporting Suspicious Activity. 13
3.6. SAR Review Process. 16
3.7. Quarterly Audit Review Process. 17
3.8. eGWG. 17
a. Function. 17
b. eGWG Membership 18
GLOSSARY 20
G.1. Acronyms. 20
G.2. Definitions. 21
REFERENCES 25

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This issuance applies to:

a. The Office of the Secretary of Defense (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 DoD (referred to collectively in this issuance as the "DoD Components").

b. DoD law enforcement officers (LEOs), as prescribed in DoDI 5525.18 and DoD civilian, military, and defense contractor personnel providing direct support to DoD personnel performing law enforcement (LE) or criminal intelligence (CRIMINT) activities.

c. Antiterrorism (AT) operations, information analysts, and planning personnel.

d. DoD personnel who serve as AT officers (ATOs) pursuant to Volume 1 of DoDI O-2000.16.

e. DoD contractors who, on behalf of a DoD Component and sponsored by LE agencies (LEAs), as prescribed in DoDI 5505.17, are involved in the suspicious activity reporting 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 suspicious activity reports (SARs), such as collecting and disseminating records, but only to the extent specified by the terms of the relevant contractual vehicle.

f. DoD personnel who perform physical security or non-LE security duties.

g. Defense intelligence component personnel detailed to DoD LEAs to support CRIMINT analysis, production, and reporting functions.

1.2. POLICY. It is DoD policy that:

a. The eGuardian system will serve as the exclusive unclassified means by which DoD will report suspicious activities to the FBI, military criminal investigative organizations (MCIOs), and Military Department counterintelligence organizations (MDCOs).

b. In order to strengthen efforts to protect DoD personnel and resources from terrorist acts and terrorism-related criminal activities:

(1) Installation ATOs working under the direction and control of an LE authority, such as the installation Directorate of Emergency Services, may have full access to the eGuardian system, but will coordinate their use of the information in the eGuardian system with the LE authority to ensure the use of the information does not adversely affect LE operations.

(2) ATOs not working under the direction and control of an LE authority, including AT operations, information analysis, and planning personnel, will obtain their SAR threat information through the LE member of the Threat Working Group, in accordance with Volume 1 of DoDI O-2000.16.

c. DoD personnel assigned to MCIOs and MDCOs will have access to information stored in the eGuardian system for support while conducting criminal or counterintelligence (CI) investigations.

d. DoD personnel performing physical security activities under the authority, direction, and control of a DoD LEA will have access to the eGuardian system to facilitate their submissions of SARs.

e. The DoD will adopt the requirements prescribed in Part 23 of Title 28, CFR, as applicable to DoD use of the eGuardian system.

f. All SARs must meet the eGuardian reporting criteria, as prescribed in Paragraph 3.5..

g. SARs and other threat information aid DoD efforts in force protection (FP) to:

(1) Identify and address terrorist and other criminal threat activities directed against DoD personnel and resources as early as possible.

(2) Identify persons and organizations involved in terrorism, criminal activity, and threats directed against DoD elements and personnel.

(3) Implement timely information-driven and risk management-based detection, prevention, deterrence, response, and protection efforts.

(4) Assist commanders with establishing appropriate FP condition measures in accordance with Volume 2 of DoDI O-2000.16 by using CRIMINT procedures, as prescribed in DoDI 5525.18, to identify possible criminal activity as defined in the eGuardian Privacy Impact Assessment.

h. SARs and threat information stored in the eGuardian system will be appropriately secured in accordance with Volume 4 of DoD Manual (DoDM) 5200.01.

i. SARs and threat information will be shared to the maximum extent permitted by law, regulation, Executive order (E.O.), and DoD policy throughout the information life cycle.

j. Personally identifiable information will be handled in strict compliance with Section 552 of Title 5, United States Code (U.S.C.), DoDI 5400.11, DoD 5400.11-R, and other applicable laws, regulations, and policies.

k. DoD intelligence and CI personnel providing assistance to DoD LEAs will comply with the provisions in Procedure 12 of DoD 5240.1-R.

l. This issuance will not affect existing policies governing:

(1) Defense Intelligence Component activities that collect, retain, and disseminate intelligence information concerning U.S. persons in accordance with E.O. 12333, DoDM 5240.01, DoD 5240.1-R, and DoDD 5240.06.

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

(3) CI awareness and reporting requirements in accordance with DoDD 5240.06.

SECTION 2: RESPONSIBILITIES

2.1. UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)). In addition to the responsibilities in Paragraph 2.8., the USD(P), in coordination with the Secretary of the Army and other appropriate DoD Component heads, maintains this issuance consistent with the policies and procedures in Part 23 of Title 28, CFR; DoDI 5400.11; DoD 5400.11-R; DoDD 5240.06; DoDD 5200.27; DoDM 5240.01; DoD 5240.1-R; DoDI 3025.21; E.O. 12333; and E.O. 13388.

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

a. Designates a DoD civilian or military member to serve on the eGWG to provide management oversight for DoD use of the eGuardian system. These oversight duties include:

(1) Developing and overseeing policy for program funding to the FBI to support DoD use of the eGuardian system, and access and account management controls.

(2) Coordinating with the Chief Management Officer of the Department of Defense (CMO) to issue guidance to ensure DoD Component compliance with the requirements in DoDI 5400.11, DoD 5400.11-R, and DoDD 5200.27.

b. In coordination with the Under Secretary of Defense for Intelligence, develops policies and procedures for the analysis and fusion of SAR data with other intelligence reporting in accordance with policies governing:

(1) Defense Intelligence Component activities that collect, retain, and disseminate information concerning U.S. persons in accordance with E.O. 12333, DoDM 5240.01, and DoD 5240.1-R.

(2) Defense Intelligence Components conducting CI activities in accordance with DoDD 5240.02 or countering espionage, international terrorism, and the CI insider threat in accordance with DoDI 5240.26.

(3) DoD Component acquisition of information concerning CRIMINT in accordance with DoDI 5525.18.

(4) The DoD Component insider threat activities in accordance with DoDD 5205.16.

c. Interfaces with the FBI on matters related to eGuardian policies, funding, and procedures, in accordance with DoDI 3025.21.

d. In coordination with the Secretary of the Army:

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

(2) Compiles funding requirements from the DoD Components that use the eGuardian system, and from the FBI for their ancillary technical support requirements, and coordinates these with the USD(P) to obtain the funding.

(3) Coordinates with the eGuardian management staff for the suspension of an individual user's eGuardian system access due to information reported in accordance with Paragraphs 2.6.c. and 2.6.h. until the responsible DoD Component provides evidence of remediation.

2.3. CMO. In addition to the responsibilities in Paragraph 2.8., The CMO advises the ASD(HD&GS) on the requirements of DoDI 5400.11, DoD 5400.11-R, and DoDD 5200.27 regarding DoD Component use of the eGuardian system.

2.4. DIRECTOR, PENTAGON FORCE PROTECTION AGENCY (PFPA). In addition to the responsibilities in Paragraph 2.6., the Director, PFPA, under the authority, direction, and control of the CMO and through the Director of Administration of the Office of the CMO, establishes procedures consistent with this issuance to accept, review, and enter into the eGuardian system information on suspicious activities received from DoD personnel working in or visiting the Pentagon Reservation and the National Capital Region for which the Director, PFPA, has security responsibility.

2.5. GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE. In addition to the responsibilities in Paragraph 2.8., and in accordance with DoDD 5145.01, the General Counsel of the Department of Defense provides advice and assistance on all legal matters, including the review of and coordination on all proposed policies, DoD issuances, and proposed exceptions to DoD policies regarding the eGuardian system.

2.6. DOD COMPONENT HEADS WITH LEAs. In addition to the responsibilities in Paragraph 2.7., the DoD Component heads with DoD LEAs:

a. Balance the need for the authority to report, collect, retain, and share information on suspicious activity with the need to protect privacy and civil liberties when developing legislative proposals or DoD implementing regulations or procedures that retain or expand that particular authority.

b. Provide adequate guidelines and oversight to establish appropriate limits on the authority to report, collect, retain, and share information on suspicious activities; and ensure adequate protections and training exist to protect privacy and civil liberties in accordance with applicable requirements, including those in DoDD 5200.27 and Section 485 of Title 6, U.S.C.

c. Establish procedures to comply with and implement the policies and procedures established and prescribed in this issuance, as well as rules of conduct necessary to ensure their

respective component's compliance with such rules and regulations the Department of Justice may establish for the use of the eGuardian system.

d. Provide adequate funding and personnel to enable their components to use the eGuardian system effectively.

e. Designate an LE investigator (Office of Personnel Management Occupational Series 1805 or 1811, or the military equivalent) to serve as their component's eGuardian program manager to provide oversight for their component's use of the eGuardian system and suspicious activity reporting processes, and to ensure compliance with this issuance.

f. Develop and conduct training, consistent with the requirements of this issuance for assigned, employed, and detailed personnel, before approving users' initial access to the eGuardian system.

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

h. In conjunction with the Secretary of the Army, who provides overall program management for DoD use of the eGuardian system, report compliance with account management, training, and SAR accountability to the Secretary of the Army or designee, as part of the quarterly audit review process.

2.7. DOD COMPONENT HEADS. The DoD Component heads:

a. Establish procedures to comply with this issuance and to ensure compliance with Part 23 of Title 28, CFR, and this issuance.

b. Establish procedures to share information in the eGuardian system with other DoD or OSD Component heads, and for maintaining records of the information that is shared.

c. Require all personnel performing CRIMINT activities to complete regular training on Part 23 of Title 28, CFR.

d. Ensure any third-party suspicious activity reporting systems they may acquire, serve as information sources for entering SARs into the eGuardian system. Establish procedures for entering suspicious activity information from the third-party system into the eGuardian system.

e. Establish procedures for personnel performing physical security or non-LE security duties to report SARs in accordance with this issuance.

2.8. OSD COMPONENT HEADS. The OSD Component heads establish procedures to implement this issuance and for their personnel to report suspicious activities.

2.9. SECRETARY OF THE ARMY. In addition to the responsibilities in Paragraphs 2.6. and 2.7., the Secretary of the Army:

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

b. May develop a charter, prescribe operating procedures, and designate a DoD civilian employee or Service member to facilitate and serve as chair of the eGWG.

c. Coordinates with the other DoD Component heads to ensure:

(1) Compliance with the eGuardian system account management requirements and establishes procedures for the execution of quarterly audit reviews of all DoD Component accounts to ensure eGuardian system access is limited to authorized personnel.

(2) Proper reporting and accounting of SARs within the eGuardian system.

d. Establishes guidance and procedures as necessary to ensure DoD Components and DoD personnel with access to the eGuardian system receive training in the safeguards and proper use of the eGuardian system.

2.10. GEOGRAPHIC COMBATANT COMMANDERS. In addition to the responsibilities in Paragraph 2.7., the geographic Combatant Commanders establish procedures to periodically formulate updated protective measures and implement information-driven notification and risk management-based detection, prevention, deterrence, response, and protection efforts based on the SAR and threat information analysis for FP purposes.

SECTION 3: eGUARDIAN PROCEDURES

3.1. PURPOSE AND USE OF THE eGUARDIAN SYSTEM.

a. The purpose for DoD's use of the eGuardian system is to enable DoD personnel to provide tips to criminal investigators on terrorism and criminal activity threats directed against DoD elements and personnel.

(1) The primary purpose is to enable DoD LEAs to enter, review, and share SARs in coordination with one another, and the FBI, as an aid in identifying potential terrorist activities targeting DoD personnel and assets.

(2) The secondary purpose is to enable DoD LEAs to enhance the protection efforts for DoD assets and personnel against all threats and hazards by sharing reports of suspicious activity with DoD LEAs and FBI criminal investigators as an aid in non-terrorism related criminal investigations, including information on potential insider threat activities.

b. In accordance with the two-part vetting process prescribed in Paragraph 3.5.a., DoD LEAs will determine whether reports of suspicious activity have an association or potential association with terrorist or other criminal activity.

3.2. SYSTEM DESCRIPTION.

a. The eGuardian system functions as an alert, recording, and reporting system for suspicious activities, not as a long-term data repository. LE personnel must validate eGuardian reports promptly so that data can move quickly through the system.

b. The eGuardian system is not an emergency reporting system. Users must contact their chain of command and local to joint terrorism task forces (JTTFs) 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 feeds a shared data repository (SDR) viewable through the FBI's classified Guardian threat reporting system. DoD personnel assigned to JTTFs and the National JTTF (NJTTF) have access to this classified Guardian system. Access to Guardian information is coordinated through the JTTFs or the NJTTF.

3.3. ACCESS PROCEDURES.

a. Access Policy.

(1) 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.

(2) DoD Components' access to, and use of, information contained in the eGuardian system will be consistent with the authorized purposes of the eGuardian system, as identified in this issuance and the applicable FBI System of Records Notice and Privacy Impact Assessment.

(3) Unrestricted access to the eGuardian system is limited to DoD LEOs, DoD civilian and military personnel performing LE activities, and defense contractor personnel supporting LE functions who are eligible for eGuardian system accounts.

(4) ATOs who need LE information to carry out AT missions, and who are not working under the direction and control of an LE authority, must coordinate with their installation LE authority for SAR threat information.

(5) DoD personnel assigned to MCIOs will have access to information stored in the eGuardian system at the discretion of their DoD Component eGuardian program manager for supporting DoD personnel conducting LE activities within authorized missions and activities.

(6) DoD personnel assigned to MDCOs will have access to information stored in the eGuardian system at the discretion of their DoD Component eGuardian program manager for the purpose of supporting intelligence missions, provided the information needed can be collected, retained, and disseminated in accordance with DoDM 5240.01 and DoD 5240.1-R.

(7) DoD personnel performing physical security functions under the authority, direction, and control of a DoD LEA will have access to information stored in the eGuardian system for the purpose of supporting the conduct of their authorized physical security activities.

(8) New users can no longer register and be vetted for access to the Part 23 of Title 28, CFR, training through the public portion of the National Criminal Intelligence Resource Center website. Registration and vetting of new users will now be available to authorized personnel only through the secure websites of the Regional Information Sharing Systems or the Criminal Justice Information System (CJIS) Law Enforcement Enterprise Portal (LEEP).

b. General Access Requirements.

(1) Users can only access the eGuardian system online by first accessing the Defense Data Exchange (D-Dex) or the CJIS-LEEP. In cases where DoD LEAs do not have access to D-Dex, or are not authorized access to D-Dex, users must first apply for a CJIS-LEEP account and then request eGuardian.

(2) DoD personnel whose LE responsibilities require access to the eGuardian system must first have access to D-Dex to use CJIS-LEEP to establish an eGuardian account. DoD organizations that are not entitled to D-Dex access will continue to use CJIS-LEEP accounts to access eGuardian.

(3) Contractors must be sponsored by a current DoD employee with an active D-Dex or CJIS-LEEP account to obtain access.

(4) Initial access to the eGuardian system requires completion of the SAR line officer training video, which 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.

(5) Although this is not a requirement, commanders should encourage their personnel to use information stored in the eGuardian system in support of CRIMINT activities or investigations into possible criminal activity, and to complete periodic Part 23 of Title 28, CFR, training.

c. Account Types. There are four distinct types of eGuardian accounts approved for use by DoD personnel. DoD Components will establish procedures to grant the appropriate level of eGuardian access to DoD Component personnel. The four distinct types of eGuardian accounts approved for DoD use are:

(1) Read-only User. Read-only user accounts only allow users the ability to view reports in the eGuardian SDR. Read-only user accounts are appropriate for ATOs, planners, and support personnel, including insider threat analysts, who are not LE analysts or credentialed LEOs.

(2) User. User accounts are generally reserved for individuals who receive reports of suspicious activity and are responsible for investigating or conducting analysis of information related to national security or other federal crimes for their assigned agency. User account privileges include the ability to translate and enter the reports of suspicious activity as draft SARs into the eGuardian system and the ability to view reports in the eGuardian SDR.

(3) Level 1 (L1) Approver. Personnel with L1 approver accounts control the dissemination of all eGuardian system reports within the level of their responsibility. All such work will be electronically submitted by an L1 approver to a fusion center (FC) approver for review and approval to be released into the eGuardian system. L1 approver account privileges include the same privileges as user accounts as well as the ability to approve drafts SARs for release to an FC approver.

(4) FC Approver. The FC approver account is reserved for the individuals assigned to an FC, whose duties are to evaluate incidents and perform other administrative functions with respect to the eGuardian system. The FC approver reviews and approves incidents to be released into the eGuardian system. An FC approver is a designated person who has received the required SAR analyst training.

d. Application for Access Procedures.

(1) Applications for access are routed through the respective DoD Component eGuardian program manager.

(2) The program manager, or designated account manager, uses the "Pending Users" feature within eGuardian to approve or disapprove eGuardian accounts.

3.4. SHARING INFORMATION IN THE EGUARDIAN SYSTEM.

a. DoD LE personnel acquiring information through the eGuardian system may share that information with:

(1) Intelligence component agencies conducting FP and combating terrorism missions in compliance with the requirements of Part 23 of Title 28, CFR, and Section 485 of Title 6, U.S.C..

(2) DoD organizations whose missions include responsibilities for conducting CI in accordance with DoDD 5240.02; countering espionage, international espionage, and the CI insider threat in accordance with DoDI 5240.26; and other insider threats in accordance with DoDD 5205.16.

b. Information obtained from eGuardian reporting and not produced by the user's agency or activity may not be further disseminated (e.g., forwarded or converted into an analytical product) without the approval of the originating DoD LEA, a non-DoD LEA, or eGuardian administrator.

c. DoD Component heads will ensure their components establish procedures to notify the Defense Insider Threat Management and Analysis Center, through their respective DoD Component insider threat hub, of insider threat information, pursuant to DoDD 5205.16 and applicable implementing regulations.

d. DoD Component eGuardian program managers will ensure their components' procedures for sharing information in the eGuardian system include the following minimum standards:

(1) Establish and maintain a records system indicating who has been given information stored in the eGuardian system, the reason for the release of the information, and the date of each dissemination outside their component.

(2) Designate a properly trained person to verify the need-to-know and right-to-know of anyone requesting information in the eGuardian system. Ensure requestors identify their need and right to know through a written inquiry for the eGuardian information.

3.5. REPORTING SUSPICIOUS ACTIVITY.

a. Pursuant to the Information Sharing Environment Functional Standard 200 (known within the suspicious activity reporting community as "ISE FS 200"), DoD personnel with User, L1 approver, or FC approver accounts will vet suspicious activity information through the following two-part process before it is entered as a SAR into the eGuardian system:

(1) Review each report of suspicious activity against the eGuardian reporting criteria in Paragraph 3.5.b.

(2) Enter the report of suspicious activity into the eGuardian system as a SAR if it meets one or more criteria and indicates a potential nexus to terrorism or other criminal activity.

b. DoD personnel with User, L1 approver, or FC approver accounts will review each report of suspicious activity to determine if it identifies one or more of the following criteria, as defined in the Glossary:

(1) Breach or attempted intrusion.

(2) Misrepresentation.

(3) Theft, loss, or diversion.

(4) Sabotage, tampering, or vandalism.

(5) Cyber attacks.

(6) Expressed or implied threat.

(7) Manned aviation activities (including flyovers and landings).

(8) Unmanned aerial systems activities (including flyovers and landings).

(9) Eliciting information.

(10) Testing or probing of security.

(11) Recruiting or providing financial support.

(12) Observation, surveillance, or photography.

(13) Materials acquisition or storage.

(14) Acquisition of expertise.

(15) Weapons collection or discovery.

(16) Incidents specific to the Defense Industrial Base Sector, pursuant to Presidential Policy Directive 21 and DoDD 3020.40.

(17) Unauthorized absences of international military students, pursuant to the Security Assistance Management Manual.

c. Personnel with User, L1 approver, or FC approver accounts will enter into the eGuardian system any suspicious activity reporting generated by a third-party system that is acquired or authorized for such use by a DoD Component head and that matches the criteria in Paragraph 3.5.b.. If the suspicious activity reporting is missing key information to complete the eGuardian report, MCIO or MDCO personnel will contact the person or organization generating the report and attempt to obtain the necessary information to complete the report. These third-party systems may not be used for reporting suspicious activities directly to the FBI, or for collecting, retaining, and disseminating databases of SARs.

d. Ensure no records are maintained on how an individual exercises rights guaranteed by the First Amendment to the Constitution, except when:

(1) Specifically authorized by statute;

(2) Expressly authorized by the individual on whom the record is maintained; or

(3) The record is pertinent to and within the scope of an authorized LE activity.

e. The following specific categories of information must not be entered into the eGuardian system:

(1) Classified information pursuant to E.O. 13526.

(2) 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."

(3) Grand jury information.

(4) Federal taxpayer information.

(5) Sealed indictments.

(6) Sealed court proceedings.

(7) Confidential human source and witness information.

(8) Any other information the dissemination of which is prohibited by law.

f. 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 either their supporting DoD LE element or nearest local LE jurisdiction.

g. FC Approvers will monitor the eGuardian system to ensure the categories of information in Paragraph 3.5.e. are not included in eGuardian reports.

h. Only personnel with User, L1 approver, or FC approver accounts 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.

i. DoD Components without their own LE organizations will report suspicious activity to either their supporting DoD LE element or nearest local LE jurisdiction.

j. Once entered, draft eGuardian reports are viewable by the initial drafter and the user's LQ approver.

3.6. SAR REVIEW PROCESS.

a. DoD Component heads will delegate the authority to an appropriate organization to establish a process to review all SARs their component's users submit for a nexus to terrorism or other criminal activity.

b. DoD Component heads will delegate approval authority for this review process to no lower than a designated eGuardian program office.

c. DoD Component heads whose component does not have an assigned defense criminal investigative organization (DCIO) or designated eGuardian program office may request that local FCs or the eGuardian management staff serve as the responsible entity to approve draft SARs that DoD Component personnel submit. All reviews will ensure the draft SARs complies with the standards established in this issuance.

d. During the review process, if any initial investigative process undertaken by the reporting DoD LEA, in coordination with FBI JTTF or NJTTF, finds a SAR has:

(1) Indicators of terrorism, criminal activity, or suspicious activity, the information will be passed to the eGuardian SDR for further dissemination and on to the FBI classified Guardian system for analysis.

(a) Once in eGuardian, a task force officer assigned to a regional JTTF or the NJTTF will assess the incident to determine if there is a nexus to terrorism. A "yes" nexus to terrorism will enable the FBI to take appropriate action as dictated by FBI policy.

(b) These reports will be retained in the eGuardian SDR for a period not to exceed 5 years.

(2) No nexus to terrorism, but contain indicators of criminal activity, the SAR will be referred to the FBI, PFPA, a DCIO or MCDO, or a DoD LEA, as appropriate. Regional or local offices of PFPA, DCIOs, MCDOs, and other DoD LEAs will maintain relationships with local FBI offices to encourage the exchange of information on the status of these referrals.

(3) No clear link to terrorism or other criminal activity as a result of FBI JTTF, PFPA, or DCIO investigation, will be removed from the eGuardian system no later than 180 days after the date the SAR was entered into the eGuardian system.

e. DoD Component criminal or CI investigative units may conduct collateral or joint investigations on incidents identified in the SAR review process consistent with the requirements of Annex B of the 2011 Memorandum of Understanding Between the FBI and DoD Governing Information Sharing, Operational Coordination, and Investigative Responsibilities.

f. To support the SAR review process, DoD Components will maintain a record of all SARs entered into the eGuardian system and account for the SARs through the quarterly audit review process outlined in Paragraph 3.7.

3.7. QUARTERLY AUDIT REVIEW PROCESS.

a. DoD Components using the eGuardian system will track, compile, and report quarterly the information listed in Paragraph 3.7.b. to their designated eGuardian program manager, pursuant to Paragraph 2.6.h.

b. Each DoD Component will provide the following information through their respective eGuardian program manager, to the DoD eGuardian program manager no later than 10 duty days after the conclusion of each fiscal quarter:

(1) Total number of eGuardian accounts at the end of the quarter.

(2) Information on any users with terminated accounts based on misuse of the system.

(3) The following information for the reporting fiscal quarter only:

(a) Total Number of SARs entered into eGuardian during the quarter.

(b) Number of SARs closed as "Yes Nexus to Terrorism" during the quarter.

(c) Number of SARs remain "Open" or "Under Assessment" during the quarter.

(d) Number of SARs closed as "Inconclusive Nexus to Terrorism" during the quarter.

(e) Number of SARs closed as "No Nexus to Terrorism" during the quarter.

(f) Number of other SAR reports and their specific designation during the quarter.

(4) Electronic copies of the eGuardian report statistics for all "Yes Nexus to Terrorism."

(5) Comments on any new significant activities or best practices.

(6) Comments on challenges or areas needing support.

(7) Number of in-person eGuardian training events during the quarter.

(8) Number of distance learning training events during the quarter.

(9) Total number of personnel trained at all training events during the quarter.

3.8. EGWG.

a. Function. The eGWG meets quarterly, or as needed, to facilitate the development of DoD policy regarding suspicious activity reporting and the DoD Components' access to, training on, and use of the eGuardian system. The eGWG will:

(1) Promote the DoD Components' use of eGuardian capabilities as a value-added means of providing information to commanders in support of their overall FP threat information common operating picture.

(2) Review the quarterly audit review process prescribed in Paragraph 3.7., gather and discuss issues, and recommend courses of action ensure that DoD Components are compliant with this issuance and applicable guidance on the appropriate use of eGuardian.

(3) Function as the decision forum for the DoD Components to report their progress on their use of and training on the eGuardian system, express their best practices, and highlight issues they have with the system's operations and support to its users.

(4) Facilitate coordination and synchronization of current issues and future eGuardian developments with the FBI on matters related to policy, procedures, and training.

(5) Facilitate the identification and coordination of funding requirements to enable DoD Components to train on and use the eGuardian system, and to resource ancillary technical support from the FBI.

b. eGWG Membership. Membership consists of representation from the following organizations:

(1) A management oversight official assigned by leadership of the Office of the ASD(HD&GS).

(2) A chairperson and eGWG coordinator assigned by the leadership of the Army Office of the Provost Marshal General.

(3) The MCIOs.

(4) The National Guard Bureau.

(5) The Combatant Commands.

(6) Defense Agencies and Defense Field Activities with LE activities.

(7) The eGuardian resource management staff.

c. Responsibilities.

(1) The management oversight official will:

(a) Promote DoD Components' use of the eGuardian system as a value-added capability to aid DoD FP, security, LE, and mission assurance efforts.

(b) Approve all eGWG minutes.

(2) The eGWG Chair will:

(a) Coordinate with the eGuardian resource management staff to assist with meeting all DoD information technology and operational support requirements and ensure that strategic issues are discussed and presented to appropriate authorities for resolution.

(b) Provide recommendations to the representative regarding program management.

(c) Provide recommendations for organizations' eGuardian policy and training and access requirements.

(d) Provide recommendations to help ensure the relevancy of DoDI 2000.26.

(3) The eGWG Coordinator will:

(a) Present, with the concurrence of the Office of the ASD(HD&GS), information on any DoD users' non-compliance with this issuance or other applicable guidance to the eGWG for discussion and development of recommended solutions, including recommended updates to DoD eGuardian policy, if appropriate.

(b) Coordinate with the eGWG members to identify issues to discuss regarding DoD Components' eGuardian implementation policies, user accountability, training, and access requirements.

(c) Schedule eGWG meetings as necessary, and develop, publish, and distribute agendas and presentation materials to all members at least 5 days in advance of meetings.

(d) Prepare draft meeting minutes and distribute them to each eGWG member, allowing the members adequate time for review and comment.

(e) Forward draft eGWG meeting minutes to the Office of the ASD(HD&GS) and Office of the Deputy Assistant Secretary of Defense for Defense Continuity and Mission Assurance for final approval.

(f) Maintain and manage the eGWG's charter, operating procedures, and other record publications and distribute copies when necessary.

GLOSSARY

G.1. ACRONYMS.

ASD(HD&GS)	Assistant Secretary of Defense for Homeland Defense and Global Security
AT	antiterrorism
ATO	antiterrorism officer
CFR	Code of Federal Regulations
CI	counterintelligence
CJIS	Criminal Justice Information System
CMO	Chief Management Officer of the Department of Defense
CRIMINT	criminal intelligence
DCIO	defense criminal investigative organization
D-Dex	Defense Data Exchange
DoDD	DoD directive
DoDI	DoD instruction
DoDM	DoD manual
E.O.	Executive order
eGWG	eGuardian Working Group
FBI	Federal Bureau of Investigation
FC	fusion center
FP	force protection
JTTF	joint terrorism task force
LE	law enforcement
LEA	law enforcement agency
LEEP	Law Enforcement Enterprise Portal
LEO	law enforcement officer
MCIO	military criminal investigative organizations
MDCO	Military Department counterintelligence organizations
NJTTF	National Joint Terrorism Task Force
PFPA	Pentagon Force Protection Agency
SAR	suspicious activity report
SDR	shared data repository
U.S.C.	United States Code

USD(P)	Under Secretary of Defense for Policy

G.2. DEFINITIONS. Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

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).

CRIMINT. Information compiled, analyzed, or disseminated in an effort to anticipate, prevent, or monitor criminal activity.

cyber attack. Compromising, attempting to compromise, or disrupting an organization's information technology infrastructure.

DCIO. The Defense Criminal Investigative Service, the Army's Criminal Investigation Command, the Naval Criminal Investigative Service, and the Air Force Office of Special Investigations.

Defense Intelligence Component. Defined in DoDM 5240.01.

DoD LEA. Defined in DoDI 5505.17.

DoD LEO. Defined in Sections 8331 and 8401 of Title 5, U.S.C. and DoDI 5505.17. Based on these sources, and for the purposes of this issuance, a DoD LEO is an employee whose primary duties are the investigation, apprehension, or detention of individuals suspected or convicted of offenses against the criminal laws of the United States, including an employee engaged in this activity who is transferred to a supervisory or administrative position.

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.

FP. Preventive measures taken to mitigate hostile actions against DoD personnel (including family members), resources, facilities, and critical information.

FC. 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 Title 5, U.S.C., a citizen of the United States or an alien lawfully admitted for permanent residence.

information sharing environment-SAR. A SAR that has been determined, pursuant to a two-part process, to have a potential nexus to terrorism (i.e., to be reasonably indicative of criminal activity associated with terrorism).

LE activities. Activities authorized in accordance with Section 2672 of Title 10, U.S.C.

LE information. Means any information obtained by or of interest to a LE agency or official that is related to terrorism or the security of our homeland, and relevant to a LE mission, including but not limited to:

Information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation.

An assessment of or response to criminal threats and vulnerabilities.

The existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct.

The existence, identification, detection, prevention, interdiction, disruption of, or response to, criminal acts and violations of the law.

The identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders.

Victim/witness assistance.

manned aviation activities. Suspicious flight or landing near a DoD facility or infrastructure by any type of flying vehicle (e.g., airplane, helicopter, unmanned aerial vehicle, hang glider).

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 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.

observation. Demonstrating unusual or prolonged interest in facilities, buildings, or infrastructure beyond mere casual (e.g., tourists) or professional (e.g., engineers) interest and in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.

Examples include observation through binoculars, taking notes, and attempting to mark off or measure distances.

personnel. Individuals required in either a military or civilian capacity to accomplish the assigned mission.

photography. Taking pictures or video of persons, facilities, buildings, or infrastructure in an unusual or surreptitious manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include taking pictures or video of infrequently used access points, the superstructure of a bridge, personnel performing security functions (e.g., patrols, badge/vehicle checking), and security-related equipment (e.g., perimeter fencing, security cameras).

physical security activities. The protection, in accordance with DoDI 5200.08, of DoD installations, facilities, information, technology, materiel, and affiliated persons from espionage, sabotage, damage, disruption, surveillance, and theft.

possible criminal activity. Defined in the eGuardian Privacy Impact Assessment.

providing financial support. The provision of financial resources to operations teams and contacts or building operations teams and contacts, compiling personnel data, banking data, or travel data in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.

recruiting. Developing contacts or collecting personnel or travel data under circumstances that would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

sabotage, tampering, or vandalism. Damaging, manipulating, or defacing part of any DoD-owned, -leased, or -occupied 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.

SAR. Official documentation of observed behavior reasonably indicative of pre-operational planning associated with terrorism or other criminal activity.

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 associated with terrorism or other criminal activity.

system of records. In accordance with Section 552a(a)(2) of Title 5, U.S.C., 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 or probing of security. Interactions with or challenges to DoD installations, vessels, personnel, or systems that could reveal physical, personnel, or capabilities vulnerabilities including attempts to compromise or disrupt DoD information technology infrastructures.

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. Defined in Volume 1 of DoDI O-2000.16.

unmanned aerial systems activities. Suspicious flight or landing near a DoD facility or infrastructure by any type of powered Unmanned Aerial System.

weapons discovery. Discovery of weapons or explosives. 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 owners' failure to properly store or secure the weapons.

REFERENCES

Annex B to the Memorandum of Understanding between the FBI and the DoD, December 9, 2011[1]

Code of Federal Regulations, Title 28, Part 23, "Criminal Intelligence Systems Operating Policies," as amended

Deputy Secretary of Defense Memorandum, "Delegations of Authority," November 30, 2006[2]

DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 7, 1982, as amended

DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007

DoD Directive 3020.40, "Mission Assurance (MA)," November 29, 2016, as amended

DoD Directive 5111.1, "Under Secretary of Defense for Policy (USD(P))," December 8, 1999

DoD Directive 5145.01, "General Counsel of the Department of Defense (GC DoD)," December 2, 2013, as amended

DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense," January 7, 1980

DoD Directive 5205.16, "The DoD Insider Threat Program," September 30, 2014, as amended

DoD Directive 5240.02, "Counterintelligence (CI)," March 17, 2015, as amended

DoD Directive 5240.06, "Counterintelligence Awareness and Reporting (CIAR)," May 17, 2011, as amended

DoD Instruction O-2000.16, Volume 1, "DoD Antiterrorism (AT) Program Implementation: DoD AT Standards," November 17, 2016, as amended

DoD Instruction O-2000.16, Volume 2, "DoD Antiterrorism (AT) Program Implementation: DoD Force Protection Condition (FPCON) System," November 17, 2016, as amended

DoD Instruction 3025.21, "Defense Support of Civilian Law Enforcement Agencies," February 27, 2013, as amended

DoD Instruction 5240.26, "Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat," May 4, 2012, as amended

DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Program," January 29, 2019

DoD Instruction 5505.17, "Collection, Maintenance, Use, and Dissemination of Personally Identifiable Information and Law Enforcement Information by DoD Law Enforcement Activities," December 19, 2012, as amended

DoD Instruction 5525.18, "Law Enforcement Criminal Intelligence (CRIMINT) in DoD," October 18, 2013, as amended

DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)," February 4, 2012, as amended

DoD Manual 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities," August 8, 2016

Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended

[1] Available from the Office of the ASD(HD&GS), 2600 Defense Pentagon, Washington, DC, 20301-2600
[2] Available from the Office of the ASD(HD&GS), 2600 Defense Pentagon, Washington, DC, 20301-2600

Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," October 25, 2005

Executive Order 13526, "Classified National Security Information," December 29, 2009

Federal Bureau of Investigation eGuardian Privacy Impact Assessment[3], current edition

Information Sharing Environment Functional Standard 200, "Suspicious Activity Reporting," current edition[4]

Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience," February 12, 2013[5]

Security Assistance Management Manual[6]

United States Code, Title 5, Section 552a (also known as the "Privacy Act of 1974")

United States Code, Title 6, Section 485

United States Code, Title 10

United States Code, Title 18, Section 641

United States Code, Title 50, Chapter 36 (also known as the "Foreign Intelligence Surveillance Act," as amended)

[3] Available on the internet at: https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/eguardian-threat

[4] Available on the internet at: https://nsi.ncirc.gov/

[5] Available on the internet at: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[6] Available on the internet at: https://www.samm.dsca.mil/