



**DEPARTMENT OF THE ARMY**

DEPUTY CHIEF OF STAFF, G-2  
1000 ARMY PENTAGON  
WASHINGTON, DC 20310-1000

DAMI-CDS (25-2e)

**21** JUN 2022

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Army Implementation of Security Executive Agent Directive (SEAD) 3, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position

1. References:

a. Office of the Under Secretary of Defense for Intelligence and Security memorandum (Implementation of Security Executive Agent Directive 3: Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position), 2 November 2020

b. Headquarters, Department of the Army (HQDA), Deputy Chief of Staff (DCS), G-2 memorandum (Army Implementation of Security Executive Agent Directive 4: National Security Adjudicative Guidelines), 4 May 2018

c. HQDA, DCS, G-2 memorandum (Army Incident Reporting and Response Requirements) 21 June 2022

d. Security Executive Agent Directive (SEAD) 3 (Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position), 12 June 2017

e. HQDA, DCS, G-2 memorandum (Clarifying Definitions – The Department of the Army's Personnel Security Program), 14 October 2016 (rescinded)

f. Army Regulation 380-67 (Personnel Security Program)

2. Applicability. This memorandum applies to Commanders and Heads of Activities, or authorized designee(s) in the minimum rank of O-4 or minimum grade of GG-13 (hereafter Commander), Security Managers, and all covered individuals as defined in enclosure 1 (Definitions). This memorandum provides implementation guidance for reference 1a and directs reporting requirements for all covered individuals.

3. Effectively immediately, all covered individuals, regardless of access to classified information, will report all reportable activities (enclosure 2) about themselves and their

DAMI-CDS (25-2e)

SUBJECT: Army Implementation of Security Executive Agent Directive (SEAD) 3,  
Reporting Requirements for Personnel with Access to Classified Information or Who  
Hold a Sensitive Position

knowledge of reportable activities regarding other covered individuals to their designated security office. Reporting is not discretionary. If it is proven that a covered individual failed to report facts (consistent with reference 1b and enclosure 2 of this implementing guidance) about a coworker, an adverse national security eligibility action may be initiated against the covered individual who failed to report.

4. Security Managers will:

a. Inform the Commander or designee of the reportable activities of a derogatory nature.

b. Report in accordance with reference 1c and enclosure 2.

c. Maintain responsibility to submit an incident report for reportable activities of a derogatory nature that occurred while the individual was affiliated with their command or activity, even if the information is discovered after the individual out-processes or separates.

5. Commanders will direct reporting of such information in the Defense Information System for Security, or successor system, in accordance with enclosure 2 and make an access retention or suspension determination. All decisions throughout the process will be in writing.

6. Commanders and Security Managers will:

a. Coordinate all reportable activities that may involve counterintelligence (CI) concerns with supporting CI units prior to submitting an incident in the personnel security system of record.

b. Disseminate this guidance to all covered individuals within 30 days of receipt of this memorandum and provide it to new covered personnel within 7 days of in-processing.

7. Commanders and Security Managers, in accordance with reference 1a, are not authorized to mitigate reportable activities nor are they authorized to restrict reporting of information based on its source. Deliberate failure to report information may trigger an adverse security action against the individual that failed to report the information.

8. Provisions of this policy will be included in a future revision of reference 1f, and added to the Security Program Benchmarks for the Headquarters, Department of the Army, G-3/5/7 Army Protection Program Assessment.

DAMI-CDS (25-2e)

SUBJECT: Army Implementation of Security Executive Agent Directive (SEAD) 3,  
Reporting Requirements for Personnel with Access to Classified Information or Who  
Hold a Sensitive Position

9. The point of contact for this action is the Deputy Chief of Staff, G-2, Personnel  
Security Branch at email: usarmy.pentagon.hqda-dcs-g-2.mbx.g-2-personnel-  
security@army.mil.



LAURA A. POTTER  
Lieutenant General, GS  
Deputy Chief of Staff, G-2

Encls

DISTRIBUTION:

PRINCIPAL OFFICIALS OF HEADQUARTERS, DEPARTMENT OF THE ARMY  
COMMANDER

U.S. ARMY FORCES COMMAND

U.S. ARMY TRAINING AND DOCTRINE COMMAND

U.S. ARMY MATERIEL COMMAND

U.S. ARMY FUTURES COMMAND

U.S. ARMY PACIFIC

U.S. ARMY EUROPE AND AFRICA

U.S. ARMY CENTRAL

U.S. ARMY NORTH

U.S. ARMY SOUTH

U.S. ARMY SPECIAL OPERATIONS COMMAND

MILITARY SURFACE DEPLOYMENT AND DISTRIBUTION COMMAND

U.S. ARMY SPACE AND MISSILE DEFENSE COMMAND/ARMY STRATEGIC  
COMMAND

U.S. ARMY CYBER COMMAND

U.S. ARMY MEDICAL COMMAND

U.S. ARMY INTELLIGENCE AND SECURITY COMMAND

U.S. ARMY CRIMINAL INVESTIGATION COMMAND

U.S. ARMY CORPS OF ENGINEERS

U.S. ARMY MILITARY DISTRICT OF WASHINGTON

U.S. ARMY TEST AND EVALUATION COMMAND

U.S. ARMY HUMAN RESOURCES COMMAND

SUPERINTENDENT, U.S. MILITARY ACADEMY

DIRECTOR, U.S. ARMY ACQUISITION SUPPORT CENTER

SUPERINTENDENT, ARLINGTON NATIONAL CEMETERY

COMMANDANT, U.S. ARMY WAR COLLEGE

DIRECTOR, U.S. ARMY CIVILIAN HUMAN RESOURCES AGENCY

CF:

DIRECTOR OF BUSINESS TRANSFORMATION

COMMANDER, EIGHTH ARMY

## DEFINITIONS

1. **Agency.** Any "Executive agency" as defined in Section 105 of Title 5, United States Code (U.S.C.), including the "military department," as defined in Section 102 of Title 5, U.S.C., and any other entity within the Executive Branch that comes into possession of classified information or has positions designated as sensitive.

2. **Classified national security information or classified information.**

Information that has been determined, pursuant to the President Executive Order (EO) 13526 or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure.

3. **Cohabitant.** A person with whom the covered individual resides and shares bonds of affection, obligation, or other commitment, as opposed to a person with whom the covered individual resides for reasons of convenience (e.g. a roommate).

4. **Controlled Substance.** Any controlled substance as defined in 21 U.S.C. 802.

5. **Covered Individual.**

a. A person who performs work for or on behalf of the executive branch who has been granted access to classified information or holds a sensitive position; but does not include the President, or (except to the extent otherwise directed by the President) employees of the President under 3 U.S.C. 105 or 107, the Vice President, or (except to the extent otherwise directed by the Vice President) employees of the Vice President under 3 U.S.C. 106 or annual legislative branch appropriations acts.

b. A person who performs work for or on behalf of a state, local, tribal, or private sector entity, as defined in EO 13549, who has been granted access to classified information, but does not include duly elected or appointed governors of a state or territory, or an official who has succeeded to that office under applicable law.

c. A person working in or for the legislative or judicial branches who has been granted access to classified information and the investigation or determination was conducted by the executive branch, but does not include members of Congress, Justices of the Supreme Court, or Federal judges appointed by the President.

d. Covered individuals are not limited to government employees and include all persons, not excluded under paragraphs (a), (b), or (c) of this definition, who have access to classified information or who hold sensitive positions, including, but not limited to, contractors, subcontractors, licensees, certificate holders, grantees, experts, consultants, and government employees.

6. **Drugs.** Any drug as defined in 21 U.S.C. 321.

7. **Foreign Intelligence Entity.** Known or suspected foreign state or non-state organizations or persons that conduct intelligence activities to acquire U.S.

## DEFINITIONS

information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. The term includes foreign intelligence and security services, and international terrorists.

8. **Foreign National.** Any person who is not a U.S. citizen or a U.S. national.

9. **Media.** Any person, organization, or entity, other than Federal, state, local, tribal, and territorial governments:

a. Primarily engaged in the collection, production, or dissemination to the public of information in any form, which includes print, broadcast, film, and internet; or

b. Otherwise engaged in the collection, production, or dissemination to the public of information in any form related to topics of national security, which includes print, broadcast, film, and Internet.

10. **National Security.** Those activities that are directly concerned with the foreign relations of the United States, or protection of the Nation from internal subversion, foreign aggression, or terrorism.

11. **National Security Eligibility.** Eligibility for access to classified information or eligibility to hold a sensitive position, to include access to sensitive compartmented information, restricted data, and controlled or special access program information.

12. **Reportable Activities.** Activities requiring reporting in accordance with Security Executive Agent Directive (SEAD) 3 and any disqualifiers in the National Security Adjudicative Guidelines. Reminder: Secret/non-critical sensitive has the same SEAD 3 reporting requirements as Top Secret/critical/special sensitive.

13. **Sensitive Position.** Any position within or in support of an agency in which the occupant could bring about, by virtue of the nature of the position, a material adverse effect on national security regardless of whether the occupant has access to classified information and regardless of whether the occupant is an employee, military service member, or contractor.

14. **Unauthorized Disclosure.** A communication, confirmation, acknowledgement, or physical transfer of classified information and Controlled Unclassified Information (as defined in DoD 5200.01M V1), including the facilitation of, or actual giving, passing, selling, publishing, or in any way making such information available to an unauthorized recipient.

## REPORTABLE ACTIVITIES

<b>SECTION A</b> <b>Reportable Activities by Others</b>		<b>Non- Incident: Supplemental Customer Service Request (CSR)</b>	<b>Incident Required</b>	<b>Data Elements</b>  When reporting about others or self-reporting is necessary, the following information must be provided, as available and applicable.
To ensure the protection of classified information or other information specifically prohibited by law from disclosure, covered individuals shall alert Commanders (or the Civilian equivalent) or Security Managers of reportable activities regarding other covered individuals that may be of potential security or counterintelligence (CI) concern:				
A1	An unwillingness to comply with rules and regulations or to cooperate with security requirements.		X	a. Date(s) b. Offense/Infraction/Violation
A2	Unexplained affluence or excessive indebtedness.		X	a. Date(s) b. Amount, if known c. Reason
A3	Alcohol abuse.		X	a. Date(s) b. Offense
A4	Illegal use or misuse of drugs or drug activity.		X	a. Date(s) b. Type of drug/controlled substance
A5	Apparent or suspected mental health issues where there is reason to believe it may impact the covered individual's ability to protect classified information or other information specifically prohibited by law from disclosure.		X	a. Date(s) b. Incident/Concern
A6	Criminal conduct.		X	a. Date of offense b. Offense
A7	Any activity that raises doubts as to whether another covered individual's continued national security eligibility is clearly consistent with the interests of national security.		X	a. Date(s) b. Incident/Concern/Activity
A8	Misuse of U.S. Government property or information systems.		X	a. Date(s) b. Nature of incident
A9	Concerning behavior and/or conduct that may be considered to constitute a disqualifying condition under any of the national security adjudicative guidelines. Reports of concerning behavior or conduct must be based on credible information, not solely on rumor, innuendo or unsubstantiated hearsay (i.e. statement of persons relating what someone else may have heard or observed that have not been independently corroborated by other facts).		X	a. Date(s) b. Issue/Concern c. Location

## REPORTABLE ACTIVITIES

<b>SECTION B</b> <b>Reportable Activities for All Covered Individuals</b> <b>(Including Self-Reporting)</b>		<b>Non- Incident: Supplemental CSR</b>	<b>Incident Required</b>	<b>Data Elements</b> When reporting about others or self-reporting is necessary, the following information must be provided, as available and applicable.
Individuals must report activities by others (Section A). In addition to the reporting requirements in Section A (Reportable by Others) individuals shall self-report reportable activities involving themselves for the following:				
B1	Arrests.		X	a. Date(s) of the incident(s) b. Location(s) of the incident(s) c. Charges and/or circumstances d. Disposition
B2	Alcohol or drug related treatment.		X	a. Reason b. Treatment provider, to include contact information c. Date(s) treatment provided
B3	Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified information or other information specifically prohibited by law from disclosure regardless of means (notify CI or Insider Threat, as appropriate).	X		a. Date(s) of incident b. Name of individual(s) involved c. Nature of incident d. Method of contact e. Electronic address f. Type of information being sought g. Background, circumstances, and current state of the matter
B4	Cryptocurrency. Ownership of foreign state-backed, hosted, or managed cryptocurrency and ownership of cryptocurrency wallets hosted by foreign exchanges. Diversified investments (index funds, mutual funds, etc.) do not need to be reported unless they are entirely composed of holdings in this sector.		X	a. Date(s) b. Type of investment (s) c. Country of Concern d. Name of Currency / Exchange e. Value of Asset f. Foreign nexus (i.e. exchange, host, manager)
B5	Media contacts. If an associated investigation/inquiry reveals a mishandling and/or unauthorized disclosure of classified information.		X	a. Date(s) of contact b. Name of media outlet c. Name of medial representative d. Nature and purpose of contact e. Whether classified information or other information specifically prohibited by law from disclosure was involved in the contact
	Where the media seeks or shows interest in access to classified information, controlled unclassified information or other information specifically prohibited by law from disclosure, whether or not the contact results in an unauthorized disclosure. Media contacts related to the fulfillment of official duties of the	Do not report to Department of Defense Consolidated Adjudications Facility		

## REPORTABLE ACTIVITIES

	position held by the covered individual need not be reported.			f. Current status of the contact
B6	Financial Issues. Includes, but not limited to, bankruptcy; garnishment; over 120 days delinquent on any debt.		X	a. Type of issue or anomaly (bankruptcy, delinquent debt, inheritance, garnishment; tax liens; foreclosures; failure to file/pay Federal or State taxes)
	Financial Anomalies: Any unusual infusion of assets of \$10,000 or greater such as an inheritance, winnings, or similar financial gain.	X		b. Dollar value c. Reason
B7	Financial disclosure reports for covered individuals who have been identified by their respective agency head in accordance with EO 12968, as amended, Section 1.3. (a). (Not reportable to the security office or DCSA Adjudications unless there is derogatory information).		Report only if derogatory	a. Date of completion b. Results
B8	All civil marriages, legally recognized civil unions, and legally recognized domestic partnerships, not already listed on a covered individual's SF 86 or previously reported. Includes a covered individual's spouse/partner who holds foreign citizenship, to include dual citizenship with the United States and a foreign nation.	Foreign Contact Module		a. Name of spouse b. Citizenship of spouse c. Date of Birth d. Place of Birth e. Date of marriage
B9	All persons with whom a covered individual cohabitates, not already listed on a covered individual's SF 86 or previously reported. A cohabitant is defined as a person with whom a covered individual presently resides, other than a spouse or legally recognized civil union/domestic partner, with whom you share bonds of affection, obligation or other commitment. It does not mean persons with whom a covered individual currently resides solely for reasons of convenience (e.g., a roommate). Includes the covered individual's cohabitant(s) who hold(s) foreign citizenship, to include dual citizenship with the United States and a foreign nation.	Foreign Contact Module		a. Name(s) b. Citizenship c. Date of Birth e. Place of Birth f. Duration of contact(s)
B10	Foreign National Roommate(s). Any foreign national(s) who co-occupies a residence for a period of more than 30 calendar days.	Foreign Contact Module		a. Name(s) b. Citizenship(s) c. Date of Birth d. Place of Birth e. Duration of contact(s)



## REPORTABLE ACTIVITIES

B11	Foreign Activities:			
B11a	Application for and receipt of foreign citizenship.		X	a. Country b. Basis for citizenship c. Date of application or receipt
B11b	Application for, possession, or use of a foreign passport or identity card for travel.		X	a. Issuing country b. Number c. Date of application / issuance d. Expiration date e. Reason for application / possession
B11c	Direct involvement in foreign business.		X	a. Nature of involvement b. Countries involved c. Name of business
B11d	Foreign bank accounts.		X	a. Financial institution b. Country
B11e	Ownership of foreign property.		X	a. Location b. Estimated value c. Balance due d. Purpose and use of property e. How acquired
B11f	Voting in a foreign election.		X	a. Date b. Country c. Election
B11g	Adoption of non-U.S. citizens.	X		a. Country involved b. Foreign government organization involved c. Foreign travel required d. Adoption agency or other intermediary e. Adoptive parents' current linkage to foreign country
B12	Unofficial Foreign Travel (FT) a. Pre-approval. Covered individuals shall submit an itinerary for unofficial foreign travel to their agency head or designee and, except as noted in the subparagraphs below, must receive approval prior to the foreign travel. Unanticipated border crossings into any foreign country not included in the traveler's	FT Module		a. Complete itinerary b. Dates of travel c. Mode of transportation and identity of carriers d. Passport date Names and association (business,

## REPORTABLE ACTIVITIES

<p>approved itinerary, regardless of duration, are discouraged. Report all deviations from approved travel itineraries within five business days of return.</p> <p>(1) Personal trips, in conjunction with official U.S. Government business, must be pre-approved and reported.</p> <p>(2) Travel to Puerto Rico, Guam, or other U.S. possessions and territories is not considered foreign travel and need not be reported.</p> <p>(3) Report unplanned day trips to Canada or Mexico upon return. Reporting shall be within five business days.</p> <p>(4) When required by Army policy, covered individuals shall, prior to travel, receive a defensive security and counterintelligence briefing.</p> <p>(5) While emergency circumstances may preclude full compliance with pre-travel reporting requirements, the covered individual, at a minimum, shall verbally advise their supervisor/management chain of the emergency foreign travel with all pertinent specifics and, preferably, a security representative, prior to departure. In any event, full reporting shall be accomplished within five business days of return.</p> <p>(6) Personnel stationed overseas in support of Department of Defense (DoD) missions taking unplanned personal day trips to foreign countries, with the exception of high risk countries listed in the Director of National Intelligence's Worldwide Threat Assessment of the U.S. Intelligence Community (this year's assessment is available at <a href="https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf">https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf</a>) need not report prior to the travel. Instead, these personnel will report a consolidated list of their travel no less than once every 90 days.</p> <p>(7) Personnel employed in the transportation industry (pilots, couriers, etc.) that routinely require non-U.S. government foreign travel do not require pre-approval for trips to foreign countries associated with their employment, with the exception of high risk countries listed in the Director of National Intelligence's Worldwide</p>		<p>friend, relative, etc.) of foreign national traveling companions Foreign government organization involved e. Planned contacts with foreign governments, companies, or citizens during foreign travel and reason for contact (business, friend, relative, etc.) f. Unplanned contacts with foreign governments, companies, or citizens during foreign travel and reason for contact (post-travel reporting) g. Name, address, telephone number, and relationship of emergency point of contact. h. Unusual or suspicious occurrences during travel, including those of possible security or counterintelligence significance (post-travel reporting) i. Any foreign legal or customs incidents encountered (post-travel reporting)</p>
--	--	--

## REPORTABLE ACTIVITIES

	<p>Threat Assessment of the U.S. Intelligence Community, need not report prior to travel. These personnel will report a consolidated list of their travel no less than once every 90 days. Commanders may require their personnel to provide more frequent reports or request pre-approval for additional countries at their own discretion.</p> <p>b. Commanders may disapprove an unofficial foreign travel request when it is determined that such travel presents an unacceptable risk and the physical safety and security of covered individuals or classified information cannot be reasonably ensured. Failure to comply with such disapproval may result in administrative action that includes, but is not limited to, revocation of national security eligibility.</p> <p>c. Official travel is not reportable. Travel solely for U.S. Government business or military overseas assignment on official government orders does not need to be reported. For Sensitive Compartmental Information (SCI) access, refer to DoDM 5105.21, Vol 3.</p>			
B13	Unofficial Foreign Contacts (Incident required unless individual is reporting being approached by a known or suspected foreign intelligence entity):			
B13a	Unofficial contact with a known or suspected foreign intelligence entity.		X	<p>a. Service(s) involved</p> <p>b. Name of individual(s) contacted</p> <p>c. Date(s) of contact</p> <p>d. Nature of contact to include any unusual or suspicious activity</p> <p>e. Likelihood of future contacts</p>
B13b	<p>Continuing association with known foreign nationals that involve bonds of affection, personal obligation, or intimate contact; or any contact with a foreign national that involves the exchange of personal information.</p> <p>(1) This reporting requirement is based on the nature of the relationship regardless of how or where the foreign national contact was made or how the relationship is maintained (i.e. via personal contact, telephonic, postal system, internet, etc.).</p> <p>(2) The reporting of limited or casual public contact with foreign nationals is not required absent any other reporting requirement in this directive.</p> <p>(3) Following initial reporting, updates regarding continuing unofficial association with known foreign nationals shall occur only if and when there is a significant change in the nature of the contact.</p>	Foreign Contact Module		<p>a. Name of foreign national(s)</p> <p>b. Citizenship</p> <p>c. Occupation</p> <p>d. Nature of relationship, i.e. business or personal</p> <p>e. Duration and frequency of contacts(s)</p> <p>f. Current status of the relationship(s)</p>

## REPORTABLE ACTIVITIES

B14	Mental Health Treatment and Counseling. Consistent with Section 21 of the Questionnaire for National Security Positions (SF 86):			
B14a	A court or administrative agency issued order declaring the individual to be mentally incompetent.		X	a. Date(s) b. Name of Court or Administrative Agency
B14b	A court or administrative agency ordering the individual to consult with a mental health professional (psychiatrist, psychologist, licensed clinical social worker, etc.). An order by a military court would fall within the scope of this reporting requirement, but an order for a military member from a superior officer would not.		X	a. Date(s) b. Name of Court or Administrative Agency c. Disposition
B14c	Hospitalization for a mental health condition.		X	a. Voluntary or Involuntary b. Date(s) c. Name Facility
B14d	Diagnosis by a mental health professional (psychiatrist, psychologist, licensed clinical social worker, etc.) of psychotic disorder, schizophrenia, schizoaffective disorder, delusional disorder, bipolar mood disorder, borderline personality disorder or antisocial personality disorder.		X	a. Diagnosis Health Condition b. Date(s) c. Name of Health Care Professional d. Name of Facility
B14e	Occasions within the last seven years where the individual did not consult with a medical professional before altering, discontinuing, or failing to start a prescribed course of treatment for any of the above diagnoses. Include details related to any current treatment.		X	a. Date(s) b. Name of Health Care Professional c. Name of Facility
B14f	Any mental health or other health condition that substantially and adversely affects the individual's judgment, reliability, or trustworthiness regardless of current symptoms.		X	a. Date(s) b. Name of Health Care Professional c. Name of Facility

## REPORTABLE ACTIVITIES

<b>SECTION C. ADDITIONAL REPORTABLE ACTIVITIES FOR COMMANDERS, SUPERVISORS AND SECURITY MANAGERS</b> In addition to the reporting requirements in Sections A and B, Commanders, Supervisors and Security Managers must report concerning behavior or conduct involving covered individuals found in:		<b>Non-Incident: Supplemental CSR</b>	<b>Incident Required</b>	<b>Data Elements</b> When reporting about others or self-reporting is necessary, the following information must be provided, as available and applicable.
C1	Command directed inquiries and investigations.		X	a. Date(s) b. Inquiry/Investigation c. Location
C2	Reports of security violations and compromises of classified information.		X	a. Date(s) b. Violation/Compromise c. Location
C3	Reports of investigation, to include: Law Enforcement reports (final), Inspector General Reports of Investigation, Equal Employment Opportunity violations.		X	a. Date(s) b. Offense c. Report of Investigation summary (upload pertinent documentation) d. Location
C4	Information provided to insider threat programs/officials.		X	a. Date(s) b. Issue/Concern c. Location
C5	Information provided to human resources.		X	a. Date(s) b. Action/incident (i.e. counseling, reprimand, suspension) c. Location