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 Incident Reporting and Response Requirements

1. References:

a. Department of Defense (DoD) Instruction 5200.02 (DoD Personnel Security Program)

b. Headquarters, Department of the Army (HQDA), Deputy Chief of Staff (DCS), G-2 memorandum (Army Implementation of Security Executive Agent Directive 3: Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position), 21 June 2022

c. 32 U.S. Code of Federal Regulations Part 117 (National Industrial Security Program Operating Manual)

d. HQDA, DCS, G-2 memorandum (Incident Reporting Requirements and Procedures), 21 February 2017 (hereby rescinded)

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

f. Office of the Under Secretary of Defense for Intelligence and Security memorandum (Responding to Continuous Evaluation Alerts: New Guidance for Department of Defense Components), 18 May 2021

2. Applicability. This memorandum applies to Commanders and Heads of Activities, or authorized designee(s) (hereafter Commander), and Security Managers of Army personnel in national security positions (defined in reference 1a).

3. In accordance with (IAW) reference 1b, covered individuals are required to report information considered as reportable activities, regardless of the source. Sources may include, but are not limited to, self-reported information and concerning behavior or conduct found in: command directed inquiries and investigations; reports of security violations and compromises of classified information; reports of investigation including final Law Enforcement reports and Equal Employment Opportunity violations; information provided to insider threat officials; and information provided to human resource professionals. This memorandum provides guidance on incident reporting

and response requirements when reportable activities are identified on individuals in national security positions.

4. Upon receipt of reportable activities that are derogatory in nature, the Commander will:

a. Inform the Security Manager and direct the Security Manager to enter an incident report in the Defense Information System for Security (DISS), or successor system (hereafter DISS).

b. Make an access determination, in writing, to retain or suspend the individual's access to classified information or performance of sensitive duties. The Commander may elect to change this access determination at any point in the process.

5. The Security Manager will:

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

b. Coordinate all reportable activities that may involve counterintelligence (CI) concerns with supporting CI units prior to submitting an incident report in DISS.

c. Submit the incident report and document the access determination in DISS. Ensure the entry includes all data elements outlined in enclosure 1.

d. If access is suspended, notify the individual, in writing, and include a brief statement of the reason(s) for the access suspension. Debrief the individual.

e. Continue to submit incident updates in DISS when new information is received and until the incident report is closed.

f. Add the requirements in this memorandum to unit-specific initial and annual refresher training.

6. Commanders and Security Managers must complete the above requirements in DISS when reportable activities are derogatory in nature, IAW timelines and additional requirements listed in enclosure 2.

7. A Commander may delegate, in writing, the requirements outlined in paragraph 4 to command or activity designee(s) in the minimum rank of O-4 or minimum grade of GS-13. The written delegation must reference the risks and responsibilities the designee may incur on behalf of the Commander.

8. For Requests for Action (RFAs) in DISS or other notifications of reportable activities from the U.S. Army Intelligence and Security Command (INSCOM), Army Security Office, INSCOM Security Operations Center, the Security Manager must submit

supporting documentation in DISS within 30 calendar days or as specified in the RFA. The supporting documentation must include all information received from the individual and the Commander's recommendation whether to retain the individual's national security eligibility. The command or activity will retain all documentation until final adjudication, which may include due process.

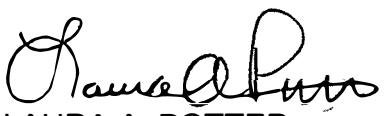
9. When an individual with an open incident transfers to a different command or activity, the losing Security Manager will submit all available information in DISS. This includes the Commander's recommendation regarding eligibility retention and a notification that the individual out-processed. The losing Security Manager will inform the gaining Security Manager of the unresolved incident(s). The gaining Security Manager will be responsible for closing out the incident. Additionally, Security Managers will notify the DoD Consolidated Adjudications Facility if an individual retires or separates from service.

10. Security Managers are responsible for submitting incident reports on contractors in national security positions that do not require access to classified information. For reportable activities involving contractors that require access to classified information, security managers must follow reporting requirements prescribed in reference 1c.

11. Prior to indoctrination, the Special Security Officer (SSO) will coordinate with the Security Manager to verify the individual does not have any derogatory information pending adjudication. In addition, the Security Manager will notify the SSO of incidents on Sensitive Compartmented Information-indoctrinated personnel.

12. Provisions of this memorandum will be included in a future revision of reference 1e. The HQDA, Office of the Deputy Chief of Staff, G-2 provides oversight to ensure compliance with incident reporting requirements. These requirements will be added to Security Program Benchmarks for the HQDA, G-2 Personnel Security Accountability Program and to the HQDA, G-3/5/7 Army Protection Program Assessment.

13. The point of contact for this action is the Deputy Chief of Staff, G-2, Personnel Security Branch, available at: 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

2 Encls
1. Incident Reporting and Response Process Map
2. Incident Reporting and Response Procedures

(see next page)

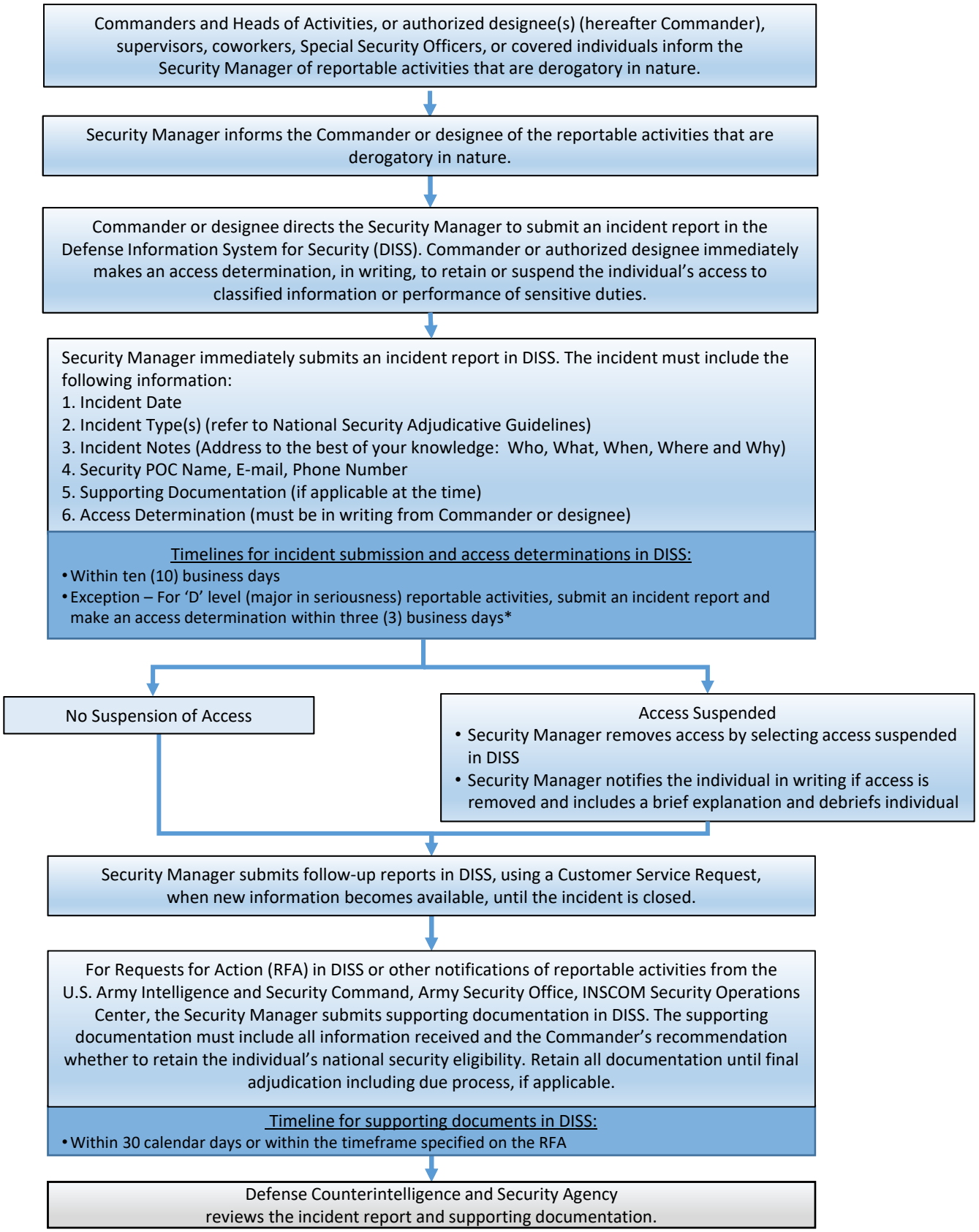
DAMI-CDS (25-2e)
SUBJECT: Army Incident Reporting and Response Requirements

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

Enclosure 1: Incident Reporting and Response Process Map



* Refer to Enclosure 2 for code definitions.

Enclosure 2: Incident Reporting and Response Procedures

The following incident reporting, response procedures, and timelines apply to all Army Commands (ACOMs), Army Service Component Commands (ASCCs), and Direct Reporting Units (DRUs) in response to reportable activities that are derogatory in nature, regardless of the source (e.g. self-reported information, continuous vetting reports, and concerning behavior or conduct found in: command directed inquiries and investigations; reports of security violations and compromises of classified information; reports of investigation including final Law Enforcement reports and Equal Employment Opportunity violations; information provided to insider threat officials; and, information provided to human resource professionals). ACOMs, ASCCs, and DRUs no longer have to submit incident reports on continuous vetting reports; however, they must still make access determinations and provide a response to the continuous vetting reports.

Code	D Level	C Level	B Level
Seriousness	**Major**	**Substantial**	**Moderate**
Description	Issues are of **critical concern**, and the conduct or issue, standing alone, would be disqualifying for eligibility to hold a National Security Position. Examples: felony offenses, sexual assaults, terrorism-related activity, and violent gang activity.	Issues are of **significant concern**, and the conduct or issue, standing alone, would likely be disqualifying for eligibility to hold a National Security Position. Examples: confinement, criminal activity involving minors / weapons / firearms (non-violent), and positive drug tests, domestic violence.	Issues are of **medium concern**, and the conduct or issue, standing alone, would likely not be disqualifying for eligibility to hold a National Security Position. Examples: bankruptcy, delinquent debts, misdemeanor criminal offenses, worthless / bad checks.
Incident Report in the Defense Information System for Security (DISS)	Commander, Head of Activity, or designee(s) (hereafter Commander), directs the Security Manager to enter an incident in DISS within three (3) business days.	Commander directs the Security Manager to enter an incident report in DISS within ten (10) business days.	
Access Determination in DISS	Commander makes an access determination in writing and the Security Manager enters access determination in DISS within three (3) business days. If access is not suspended, the Command must provide the reasons for not suspending access and the mitigation strategy via DISS.	Commander makes an access determination in writing and the Security Manager enters the access determination in DISS within ten (10) business days.	
Response	• Ensure the security office has an owning relationship with the individual's DISS record. • Continue to submit incident updates in DISS when new information is received. • Claim Requests for Action (RFA) in DISS and submit the signed acknowledgement of receipt. • For RFAs in DISS or other notifications of derogatory reportable activities from Army Security Office INSCOM Security Operations Center, Security Manager submits supporting documentation within 30 calendar days (or within the timeline specified in the RFA). Request extensions if necessary.		
Eligibility	If the security office does not enter an access decision into DISS within seven (7) calendar days, DCSA may suspend eligibility. DCSA will adjudicate within ~30 calendar days of adjudicative ready response.	DCSA may suspend eligibility after 30 calendar days if no response to RFA. DCSA will adjudicate within ~30 calendar days of adjudicative ready response.	DCSA will adjudicate within ~30 calendar days of adjudicative ready response.

Code A (minor) derogatory reportable activities are filed in the adjudicative record and do not require an incident or response. Most of this criteria was taken from the OUSD(I&S) memorandum, Responding to Continuous Evaluation Alerts: New Guidance for Department of Defense Components, 18 May 2021. PERSEC added timelines where the OUSD(I&S) memorandum was silent.