DEPARTMENT OF THE ARMY
HEADQUARTERS, 10TH MOUNTAIN DIVISION (LIGHT INFANTRY) AND FORT DRUM
FORT DRUM, NEW YORK 13602-5000

AFDR-CG 09 September 2022

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Command Policy Memorandum #21, Unauthorized Disclosure of Classified Information (UDCI) and Other Security Incidents

1. References:

a. Army Regulation (AR) 380-5, Information Security Program, 25 March 2022

b. Department of Deffense (DoD) Manual 5200.1, Volume 1, 2 and 3

c. DoD Manual 5200.45, Instructions for Developing Security Classification Guides, 2 April 2013, incorporating Change 2, effective 15 September 2020.

2. Purpose. Unauthorized disclosure or compromise of classified material can result in an increased risk to our national security, sensitive military operations, and endanger the lives of military personnel. It is imperative that all members of the Department of Defense protect classified military information (CMI) and material entrusted to them. This policy letter is intended to guide unit commanders and leaders in the event of a UDCI.

3. A UDCI can involve any number of circumstances. This includes, but is not limited to:

a. CMI sent or stored on unclassified systems and networks;

b. CMI or classified material not stored IAW the minimum security standards established in references a and b (GSA-approved container, 24/7 guard, etc.);

c. Allowing uncleared personnel to participate in classified meetings and discussions or, allowing them to carry CMI without proper courier authorization;

d. Failure to use GSA-approved locks for storage devices;

e. Loss of control or accountability of CMI or classified material.

4. Commanders will report all UDCIs and other relevant security violations based on the Commanders Critical Information Requirements (CCIR) standards of 10th Mountain Division CCIR #19. Unit Commanders or S3s will notify the Mountain Operations Center (MOC) within 1 hour of an occurrence or discovery via 7Ws, and follow up with a SIR and updated 7Ws within 7 hours IAW CCIR #19. Unit S2 will notify the 10th Mountain Division G2 Command Security Manager within 24-hours IOT facilitate notification to XVIII Airborne Corps G2. The ACoS G6 and DIV CoS will be notified of any incident involving the mishandling of classified digital media.

5. Discussions regarding the details of UDCIs is considered classified at the level of the classified system where in the incident occurred, or the level of the information involved. All reports containing more information than the fact that a UDCI has occurred, must be handled at the level of the highest classification system involved.

6. The ACoS G6 and NEC will immediately suspend the implicated user(s) accounts on SIPR and NIPR until the user's Brigade Commander notifies the Division Commanding General (CG) that the investigation and remediation is complete. Exceptions to this policy will be limited to those deemed Mission Critical such as Commanders, Executive Officers, S3s, Command Sergeants Major, and First Sergeants. For exceptions, the Brigade Commander will notify the CG of the incident and his/her justification for postponing the requirement for access suspension. The user's access will remain active for 20 working days to allow for the completion of the investigation. If after 20 days the investigation is not complete, the user's access will be disabled.

7. The unit commander, as the Appointing Authority (AA), will appoint an Investigating Officer (IO) to investigate the circumstances of the incident. The IO must be of higher rank than anyone involved in the incident and not assigned to the implicated user's unit. DODM 5200.1 Volume 3 Appendix 1 to Enclosure 6, contains a sample investigation report outlining how to conduct an investigation and the issues that must be answered. The IO or unit S2 will provide updates on the status of the investigation to the G2 Command Security Manager every three days.

8. During the investigation, the IO will make a determination if a compromise of classified information occurred, and if so, whether there is damage or potential damage to national security. The determination made by the IO must articulate personnel involved, situation, and/or conditions responsible for or contributing to the incident.

9. The IO will return the results of their investigation to the AA within 20 working days of being appointed. Within three days of receipt from the IO, the AA will submit the report to the G2 for review of accuracy and compliance with the above listed regulations. Upon completion of their review, the G2 will forward the results to the Division SJA for legal review. After legal review, the G2 will brief the investigative packet to the CG unless otherwise directed by the CG. In those other circumstances, the Division G2 will review the packet and determine whether to close the investigation or provide instruction for further necessary actions.

10. The point of contact for this memorandum is the Matthew Madson, the Command Security Manager at 772-1626 or email: matthew.s.madson.civ@army.mil.

GREGORY K. ANDERSON
Major General, USA
Commanding

DISTRIBUTION:
A