



Department of Defense **DIRECTIVE**

NUMBER 5210.50

October 27, 2014

Incorporating Change 1, Effective February 16, 2018

USD(I)

SUBJECT: Management of Serious Security Incidents Involving Classified Information

References: See Enclosure 1

1. PURPOSE. This directive:

a. Reissues DoD Directive (DoDD) 5210.50 (Reference (a)) to update established policy and assign responsibilities for the prevention and management of serious security incidents involving information classified in accordance with Executive Order 13526 or *section 2011 et. seq. of Title 42, United States Code (U.S.C.), also known as “the Atomic Energy Act of 1954, as amended”* (referred to in this directive as “serious security incidents”), and congressional notification in accordance with section 2723 of Title 10, ~~United States Code (U.S.C.)~~ (References (b), (c), and (d)).

b. Designates the Under Secretary of Defense for Intelligence (USD(I)), as the senior security official, to manage and provide oversight of serious security incident procedures, and requires the use of a DoD-wide system for reporting serious security incidents in accordance with DoDD 5143.01 and Secretary of Defense Memorandum (References (e) and (f)).

c. Incorporates and cancels USD(I) Memorandum (Reference (g)).

2. APPLICABILITY. This directive:

a. Applies to 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 (IG DoD), the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this directive as the “DoD Components”).

b. Will be made applicable to DoD contractors through appropriate contract clauses.

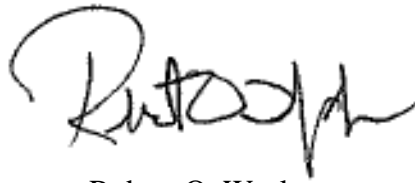
3. POLICY. It is DoD policy that:

- a. Prevention of serious security incidents is a responsibility shared by all DoD personnel.
- b. A DoD-wide system for reporting and managing serious security incidents will be used to compile serious security incident reports, encouraging rapid case resolution.
- c. Training on the prevention, identification, and reporting of serious security incidents will be provided to all DoD personnel who are authorized access to classified information.
- d. Commanders and supervisors at all levels will ensure that serious security incidents are referred as soon as possible to the appropriate security authorities in accordance with Enclosure 6 of Volume 3 of DoD Manual (DoDM) 5200.01 (Reference (h)) and, when appropriate, to the servicing defense criminal investigative organization or other law enforcement organization in accordance with DoD Instruction (DoDI) 5505.03 (Reference (i)).
 - (1) For unauthorized disclosures of classified information to the public or the media, submit a Department of Justice (DoJ) media leak questionnaire in accordance with Enclosure 6 of Reference (h) for referral to the DoJ in accordance with section 535(b) of Title 28, U.S.C. (Reference (j)).
 - (2) Defense Intelligence Components also reporting in accordance with section 1.6(b) of Executive Order 12333 (Reference (k)) will notify the USD(I) through security channels when referring unauthorized disclosures of classified information to DoJ.
- e. Serious security incident investigations and reporting will integrate security, counterintelligence, law enforcement, and other appropriate DoD interests to ensure that the causes of serious security incidents are identified and that all appropriate means are utilized to identify and mitigate damage to national security and avoid similar occurrences.
- f. DoD personnel responsible for serious security incidents may be held accountable, as appropriate, in a criminal proceeding, civil judicial action, disciplinary or adverse administrative action, or other administrative action authorized by federal law or regulations.

4. RESPONSIBILITIES. See Enclosure 2.

5. RELEASABILITY. **Cleared for public release.** ~~This directive is available on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.~~ *This directive is available on the Directives Division Website at <http://www.esd.whs.mil/DD/>.*

6. EFFECTIVE DATE. This directive is effective October 27, 2014.

A handwritten signature in black ink, appearing to read "R. Work". The signature is stylized with a large initial "R" and a long, sweeping underline.

Robert O. Work
Deputy Secretary of Defense

Enclosures

1. References
2. Responsibilities

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5210.50, “Unauthorized Disclosure of Classified Information to the Public,” July 22, 2005 (hereby cancelled)
- (b) Executive Order 13526, “Classified National Security Information,” December 29, 2009, as amended
- (c) *Section 2011 et. seq. of Title 42, United States Code, also known as “the Atomic Energy Act of 1954, as amended”*
- (d) Section 2723 of Title 10, United States Code
- (e) DoD Directive 5143.01, “Under Secretary of Defense for Intelligence (USD(I)),” ~~November 23, 2005~~ *October 24, 2014, as amended*
- (f) Secretary of Defense Memorandum, “Deterring and Preventing Unauthorized Disclosures of Classified Information,” October 18, 2012
- (g) Under Secretary of Defense for Intelligence Memorandum, “Clarification of Policy for Management of Unauthorized Disclosures,” October 2, 2012 (hereby cancelled)
- (h) DoD Manual 5200.01, Volume 3, “DoD Information Security Program: Protection of Classified Information,” February 24, 2012, as amended
- (i) DoD Instruction 5505.03, “Initiation of Investigations by Defense Criminal Investigative Organizations,” March 24, 2011, *as amended*
- (j) Section 535(b) of Title 28, United States Code
- (k) Executive Order 12333, “United States Intelligence Activities,” December 8, 1981, as amended
- (l) DoD Manual 5200.01, Volume 1, “DoD Information Security Program: Overview, Classification, and Declassification,” February 24, 2012
- (m) Directive-type Memorandum 08-052, “DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters,” June 17, 2009, as amended

ENCLOSURE 2
RESPONSIBILITIES

1. USD(I). The USD(I):

- a. Oversees implementation of this directive within DoD.
- b. Authorizes exceptions to this directive. This authority may be delegated to one level below the USD(I).
- c. Establishes policy and provides direction for the identification, reporting, investigation, and referral of serious security incidents.
- d. Monitors, oversees, and ensures the prompt reporting and investigation of serious security incidents throughout DoD and/or within DoD contractor facilities.
- e. Develops and implements a DoD-wide system for reporting and managing serious security incidents.
- f. Assigns investigative and reporting responsibility, in consultation with the affected DoD Component heads, when the responsibility for investigation of a serious security incident is unclear, or is shared by more than one DoD Component.
- g. Reviews findings and recommendations of DoD Component investigations into serious security incidents and follow-on corrective actions to identify root causes, identify and mitigate damage to national security, and avoid similar occurrences. Depending on the results of the initial inquiry and/or investigation, and in consultation with the DoD Component head with original classification authority (OCA) for the information and the General Counsel of the Department of Defense (GC DoD), decides whether investigation beyond that which is already required in Enclosure 6 of Reference (h) is appropriate.
- h. In consultation with the DoD Component head with OCA for the information and the GC DoD, determines whether referral of serious security incidents to the DoJ is appropriate in accordance with References (j) and (k).
- i. In consultation with the Assistant Secretary of Defense for Legislative Affairs, notifies Congress as required by Reference (d) and the Director, Information Security Oversight Office, National Archives and Records Administration as required by section 5.4(d) of Reference (k).
- j. Coordinates with the Office of the Director of National Intelligence, the IG DoD and the inspectors general of the Defense Intelligence Components (e.g., National Reconnaissance Office, National Security Agency, National Geospatial Intelligence Agency, and Defense Intelligence Agency), law enforcement, counterintelligence, and other appropriate organizations

to harmonize procedures within DoD and the intelligence community to ensure that gaps in effective controls and oversight are closed.

2. DoD COMPONENT HEADS. The DoD Component heads:

a. Assign responsibility for directing, administering, and overseeing the implementation of this directive to the senior agency official responsible for the direction, administration, and oversight of the Component's information security program, including classification, declassification, safeguarding, and security education and training programs within their respective Component.

b. Establish a Component point of contact to manage reporting, investigation, referrals, and communication concerning serious security incidents with the Office of the Under Secretary of Defense for Intelligence (OUSD(I)).

c. Promptly report serious security incidents, investigative results, and corrective and/or disciplinary action taken to OUSD(I) in accordance with Enclosure 6 of Reference (h) using the DoD-wide system for reporting and managing serious security incidents.

d. Ensure that all serious security incidents are managed in accordance with Enclosure 6 of Reference (h), corrective actions to prevent recurrence are implemented, and those responsible for serious security incidents are held accountable, as appropriate, in a criminal prosecution, civil judicial action, disciplinary or adverse administrative action, or other administrative action authorized by federal law or regulations.

e. Refer matters to OUSD(I) when the responsibility for investigation of a serious security incident is unclear or is shared with another DoD Component.

f. Ensure senior leadership is accountable for implementation of prevention programs, corrective actions, and end-to-end management of serious security incidents.

g. Direct senior leadership involvement in the management of serious security incident cases to assist with the integration of security, counterintelligence, law enforcement, and other appropriate DoD interests.

h. Provide training to enhance the prevention, identification, and reporting of serious security incidents during initial orientation, annual refresher training, and termination briefings as required by Volume 1 of DoDM 5200.01 (Reference (l)).

i. Report serious security incidents involving an intelligence activity or intelligence personnel to the DoD Senior Intelligence Oversight Officer in accordance with Directive-type Memorandum 08-052 (Reference (m)).

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

DoDD	DoD Directive
DoDI	DoD Instruction
DoDM	DoD Manual
DoJ	Department of Justice
GC DoD	General Counsel of the Department of Defense
IG DoD	Inspector General of the Department of Defense
OCA	original classification authority
OUSD(I)	Office of the Under Secretary of Defense for Intelligence
U.S.C.	United States Code
USD(I)	Under Secretary of Defense for Intelligence

PART II. DEFINITIONS

~~Unless otherwise noted, t~~hese terms and their definitions are for the purpose of this directive.

senior leadership. Personnel in a command or senior management position within a DoD or OSD Component.

serious security incident. A violation or incident involving classified information meeting the thresholds for reporting to OUSD(I), as specified in Enclosure 6 of Reference (h).