



# Department of Defense MANUAL

NUMBER 5200.01, Volume 3

February 24, 2012

Incorporating Change 3, Effective July 28, 2020

---

---

USD(I&S)

SUBJECT: DoD Information Security Program: Protection of Classified Information

References: See Enclosure 1

## 1. PURPOSE

a. Manual. This Manual is composed of several volumes, each containing its own purpose. The purpose of the overall Manual, as authorized by DoD Directive (DoDD) 5143.01 (Reference (a)) and DoD Instruction (DoDI) 5200.01 (Reference (b)), is to reissue DoD 5200.1-R (Reference (c)) as a DoD Manual to implement policy, assign responsibilities, and provide procedures for the designation, marking, protection, and dissemination of controlled unclassified information (CUI) and classified information, including information categorized as collateral, sensitive compartmented information (SCI), and Special Access Program (SAP). This guidance is developed in accordance with Reference (b), Executive Order (E.O.) 13526, E.O. 13556, and part 2001 of title 32, Code of Federal Regulations (CFR) (References (d), (e), and (f)). This combined guidance is known as the DoD Information Security Program.

b. Volume. This Volume:

- (1) Provides guidance for safeguarding, storage, destruction, transmission, and transportation of classified information.
- (2) Identifies security education and training requirements and processes for handling of security violations and compromise of classified information.
- (3) Addresses information technology (IT) issues of which the security manager must be aware.
- (4) Incorporates and cancels Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandums (References (g) and (h)).

2. APPLICABILITY. This Volume:

(4) The investigation should be accomplished promptly following appointment of the investigating officer. The results of the investigation shall be documented in writing. The format in Appendix 1 to this enclosure may be used.

7. **INFORMATION APPEARING IN THE PUBLIC MEDIA**

a. If classified information appears in the public media, including on public Internet sites, or if approached by a representative of the media, DoD personnel shall be careful not to make any statement or comment that confirms the accuracy of or verifies the information requiring protection. Report the matter as instructed by the appropriate DoD Component guidance, but do not discuss it with anyone who does not, in the case of classified information, have an appropriate security clearance and need to know.

b. If the fact of an unauthorized public disclosure becomes widely known, the Component senior agency official should consider whether the workforce needs to be reminded of actions to be or not to be taken by individuals in response to the disclosure. Reminders may include such topics as not viewing or downloading the classified information from unclassified IT systems, not confirming the accuracy of the information, and providing a point of contact for media inquiries.

c. Notifications of unauthorized disclosures of classified information in the public media required by subparagraph 3.f.(1)(b) of this enclosure shall include the information specified in subparagraphs 7.c.(1) through 7.c.(7). Initial notifications providing basic information about the incident and a point of contact should be made as quickly as is feasible; complete information should be provided subsequently.

(1) Date, location, and author of the public media item.

(2) Specific information disclosed and its classification level.

(3) Identification of the OCA.

(4) The extent to which the disclosed information was circulated, both within and outside the Department of Defense, and the number of persons known to have had access to the information.

(5) An appraisal of or statement regarding the damage to national defense and/or national security programs caused by the disclosure.

(6) A statement of whether any investigative leads exist and what additional actions, if any, are contemplated (i.e., no further action; administrative investigation by the DoD Component; referral to the cognizant DCIO for criminal investigation; or a request for USD(I&S) referral to DoJ for investigation).

(7) Point of contact for further information.

d. When notified of a suspected compromise of classified information through the public media, the USD(I&S) shall, unless already done by the reporting DoD Component, consult with the Assistant Secretary of Defense for Public Affairs and other officials having a primary interest in the information to determine if the information was officially released under proper authority.

e. When responsibility for an inquiry into an unauthorized public media disclosure is unclear or is shared equally with another DoD Component, refer the matter through security channels to the USD(I&S) who shall decide investigative responsibility in consultation with the affected DoD Components.

f. The decision on whether to initiate an additional investigation by a DCIO or by the Federal Bureau of Investigation through a referral to the DoJ shall be based on the following factors:

(1) The accuracy of the information disclosed.

(2) The damage to national security caused by the disclosure and whether there were compromises regarding sensitive aspects of current classified projects, intelligence sources, or intelligence methods.

(3) The extent to which the disclosed information was circulated, both within and outside the Department of Defense, and the number of persons known to have access to it.

(4) The degree to which an investigation shall increase the damage caused by the disclosure.

(5) The existence of any investigative leads.

(6) The reasonable expectation of repeated disclosures.

g. If the DoD Component's initial inquiry or investigation or a DCIO investigation identifies the person(s) responsible for an unauthorized disclosure of classified information via the public media or Internet, the DoD Component shall notify the Director of Security, OUSD(I&S). This notification shall include responses to the DoJ Media Leak Questionnaire (see Appendix 2 of this enclosure). The USD(I&S), in coordination with the General Counsel of the Department of Defense (GC, DoD) and the Head of the DoD Component having OCA, shall decide whether additional investigation is appropriate and whether to refer the unauthorized disclosure to the DoJ for investigation and/or criminal prosecution. When the initial inquiry or investigation does not identify the person responsible, the Head of the DoD Component, in consultation with the USD(I&S) and the GC, DoD, shall decide if further investigation is appropriate.

## 8. RESULTS OF INQUIRIES AND INVESTIGATIONS