

Information Security Webinar Series

DoD Activity Security Manager Responsibilities

All US Government departments and agencies have been prescribed by Presidential Executive Order — “a uniform system for classifying, safeguarding, and declassifying national security information” with the priorities of “protecting information critical to our Nation’s security and demonstrating our commitment to open Government through accurate and accountable application of classification standards and routine, secure, and effective declassification”.



DoD’s Information Security Management Program

The DoD established its Information Security Program policies and guidance in DoD 5200.01-R. This regulation was reissued in 2012 as a DoD manual in four volumes. The new DoDM 5200.01 greatly expanded the DoD Information Security Program guidance and policies.

DoDM 5200.01, Information Security Program

- Volume 1 — program overview, responsibilities, and guidance for classification and declassification
- Volume 2 — marking of classified information
- Volume 3 — guidance for safeguarding, storage, destruction, transmission, and transportation of classified information; training requirements; handling security violations and compromises; and information technology issues
- Volume 4 — guidance for controlled unclassified information

DoD Activity Security Manager Responsibilities

While previous versions of DoD 5200.01-R specified that the head of any DoD activity that “creates, handles or stores classified information” must appoint a security manager, they did not specifically enumerate responsibilities or define minimal qualifications for an activity security manager. Volumes one and three of DoDM 5200.01 specifically delineate the role,

responsibilities, and qualifications of a DoD activity security manager.

While many of these newly delineated responsibilities and requirements may mirror or be exceeded by preexisting Service requirements, they remain significant in that they signify the emerging professionalization of the role a DoD activity security manager.

DoD recognizes activity security managers as the critical linchpin in the effort to operationalize an efficient and effective information security program on a day-to-day basis.

Appointment of Activity Security Managers

DoDM 5200.01 requires the head of a DoD Activity

- designate, in writing, an activity security manager;
- give that security manager the authority to ensure personnel adhere to program requirements;
- provide that activity security manager direct access to the activity’s leadership, and
- organizationally align the security manager to ensure prompt and appropriate attention to program requirements.

While every activity that “creates, handles, or stores classified information” must appoint a security manager, the appointment may be on a full-time, part-time, or collateral duty basis. The key requirement is that the enumerated security manager responsibilities be adequately and professionally executed and implemented.

Security manager responsibilities must be adequately and professionally executed and implemented.

Security Manager AORs

DoD activity security manager responsibilities enumerated in DoDM 5200.01 can be broadly classified into several categories:

- Management and Oversight
- Compliance
- Planning and Coordination
- Education and Awareness
- Threat and Incident Response

Management and Oversight

DoDM 5200.01 specifies that the activity security manager is responsible for the management and implementation of the activity's information security program.

Additionally, the activity security manager is to

- serve as the principle advisor to the activity head on all information security matters;
- maintain cognizance of all activity security functions; and
- provide guidance, direction, coordination, and oversight to designated assistant security assistants

Compliance

The security manager's responsibility for the successful implementation of an activity's information security program entails ensuring fundamental compliance with the DoD Information Security Program's policies and procedures.

DoDM 5200.01 specifies that the security manager must ensure

- access to classified information is limited to appropriately cleared personnel with a need to know;
- implementation of and compliance with information security requirements of for all uses of information technology; and
- compliance with information security requirements when access to classified information is provided to industry contractors.



Planning and Coordination

DoD activity security managers must perform a wide variety of implied and specified planning-related activities. Among the specified planning responsibilities are the development of written instructions for safeguarding classified information during emergencies and military operations; and the development of security measures and procedures regarding visitor access.

Among some of the implied planning responsibilities are those related to managing the activity's security training program; recordkeeping and reporting requirements; and the maintenance of security classification guides under the activity's cognizance.

The successful conduct of security manager responsibilities requires coordination and liaison with a broad range of individuals and activity functions. In particular DoDM 5200.01, specifies that the security manager

- maintain liaison with public affairs and operations security to ensure information intended for public release receives required security reviews;
- coordinate with other activity officials regarding security measures for the classification, safeguarding, transmission, declassification, and destruction of classified information;
- coordinate with information systems security personnel as required for effective management, use, and oversight of classified information in electronic form;
- coordinate the preparation, dissemination, and maintenance of security classification guides with original classification authorities;
- coordinate when necessary with the proper authorities in response to security threats and incidents; and
- maintain liaison with the special security officer, as appropriate, on issues of common concern.

Education and Awareness

Successful compliance with the DoD information security program requires personnel that are security-educated and aware. As such, maintenance of the activity's security awareness, education, and training is among the responsibilities designated to the security manager.

DoDM 5200.01 specifically requires the security manager to formulate, coordinate, and conduct the activity's security education and training program, to include related information systems; and to keep personnel who perform security duties abreast of changes in policies and procedures, and provide them assistance in problem solving.



Threat and Incident Response

DoDM 5200.01 specifies that activity security managers must ensure that security threats and incidents pertaining to classified information are reported, recorded, coordinated with the proper authorities and when necessary investigated.

Additionally, it is the activity security manager's responsibility to take appropriate action to mitigate damage and prevent recurrence of security issues.

Security Manager Qualifications

Qualifications for activity security managers were not defined in DoD 5200.01-R, however, DoDM 5200.01 now defines specific minimal qualifications individuals must meet to be designated a DoD activity security manager.

A DoD activity security manager must be a

- U.S. citizen;
- have a current clearance to the highest level of classification of information being handled within the activity; and
- have access appropriate to the level of information managed.

Required Ranks

A military officer, senior non-commissioned officer, or a civilian employee may be designated as the activity's security manager with the following caveats.

In activities with more than 100 personnel, the designated security manager must be a senior non-commissioned officer E-7 or above or in the case of a civilian employee GS-11 or above.

In activities with less than 100 personnel, the designated security manager must be a senior non-commissioned officer E-6 or above or in the case of a civilian employee GS-7 or above.

Activity Assistant Security Managers and Top Secret Control Officer

The DoD recognizes that within large activities information security management responsibilities may warrant the designation of assistants.

DoDM 5200.01 specifies that activity managers may designate activity assistant security managers to assist in program implementation, maintenance, and local oversight; and as needed designate Top Secret control officers and assistants to manage and account for Top Secret materials. These designations must be in writing and are subject to the following requirements.

Activity assistant security managers must be U.S. citizens with security clearances and accesses appropriate to their assigned responsibilities; their assigned responsibilities must be commensurate with their grade level, experience, and training; and they must report directly to the activity security manager.

When there is a need, Top Secret control officers and Top Secret control assistants may be appointed to facilitate appropriate control of Top Secret material.

These individuals must be favorably adjudicated with a current background investigation and have Top Secret access.

The Top Secret security officer must report directly to the activity security manager or the activity security manager may serve concurrently as the Top Secret control officer.

Additional Specified Responsibilities

Additional responsibilities within DoDM 5200.01 specifically designated to activity security manager.

Security Incidents

DoD policy requires that anyone who becomes aware of the loss or potential compromise of classified information immediately report it to the activity security manager, with the only exception being cases in which a person believes the activity security manager may have been involved. In those cases reporting to higher command is required.

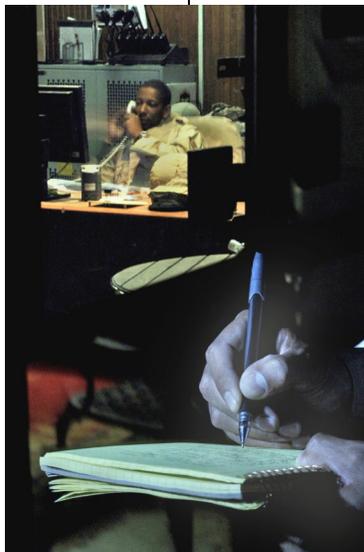
Activity security manager responsibilities in regard to responding to reported security incidents may include

- promptly initiating an inquiry by appointing an uninvolved inquiry officer, who is then to provide a report of findings within 10 duty days; or
- ensuring the incident is reported to the appropriate authority for those incidents over which the security manager does not have cognizance; and
- providing a copy of the results of an inquiry to a contracting company and to the Defense Security Service, in those cases where the security incident involved on-site contractors.

Training Requirements

The successful fulfillment of specified and implied activity security management responsibilities requires a highly-trained professional cadre of security-minded personnel; as such the DoD has prescribed a wide range of training requirements that security managers must not only personally meet, but must also implement and manage within their respective activities.

Among some of the training requirements for personnel whose duties significantly involve managing and overseeing classified information are topics such as the original and derivative classification processes; marking of classified documents; the proper use, storage, reproduction, transmission, dissemination, and destruction of classified information; investigation and reporting instances of actual or potential compromise; and procedures for the secure use of information systems.



Information Technology

DoDM 5200.01 volume 3 includes newly specified requirements related to the security issues posed by the use of information technology within DoD activities.

For example, actual or potential compromises of classified information involving information technology are to be reported through appropriate channels by the information assurance manager to the activity security manager.

And while the inquiry and resolution of these incidents often requires coordination with and assistance from information assurance officials, a prompt resolution is the responsibility of the activity security manager.

DoDM 5200.01 specifies that in the case of data spills activity security managers are responsible for

- maintaining overall lead for addressing the event;
- ensuring unauthorized disclosures policy requirements are met; and
- coordinating closely with information technology and information assurance staff.

Some of the other IT-related activity security managers' responsibilities include the requirement that activity security managers must approve and authorize in writing the use of any remote diagnostic or repair capabilities; and that activity security managers coordinate with the local designated approval authorities and/or IT staff to ensure procedures for disposal of computer hard drives appropriately addresses removal of U.S. Government data prior to disposal.

Prompt resolution of security incidents related to IT is a responsibility of the activity security manager.

How Can CDSE Help?

The Center for Development of Security Excellence (CDSE) produces and provides a wide range of information security training, education, and awareness products to support the DoD Activity Security Manager's mission.

This includes instructor-led training, e-learning courseware, and training products across the entire range of responsibilities assigned to an activity security manager.

On the CDSE website you can find additional information about CDSE products; access e-learning courseware; register for instructor-led training; and download job aids and security awareness materials.

[Learn more @ dssa.dss.mil](http://dssa.dss.mil)

STEPP Learning Management System

A wide-array of information security-related e-learning can be accessed on CDSE's learning management system called STEPP.



The STEPP system not only provides multimedia-rich courseware but also retains and maintains learner records and transcripts. STEPP is available for use by DoD and other US Government personnel and contractors within the National Industrial Security Program.

Job Aides and Awareness Media

CDSE also produces various job aides to assist security professionals, which can be accessed on the public website.

Among the job aids are such topics as Marking Classified Information; Derivative Classification Training; a Procedural Guide for Conducting Classified Conferences; and aids for the operation of standard locks.

Job Aids

www.dss.mil/seta/resources/supplemental-job-aids.html

Awareness Posters

www.dss.mil/seta/security_posters.html

Instructor-Led Training



DoD Security Specialist

Broad survey course that includes general, industrial, personnel, information, and physical security related-topics targeted to those personnel with little or no security-related experience.

www.dss.mil/cdse/catalog/classroom/GS101.html

Information Security Management

Mid-level course intended for personnel who have a functional working knowledge of the DoD Information Security Program.

www.dss.mil/cdse/catalog/classroom/IF201.htm

Instructional Media

In addition to instructor-led and e-learning courses, CDSE also offers a wide variety of other instructional media in support of the DoD Information Security Program. This includes Security Shorts, which are targeted e-learning courses designed to be completed in less than 15 minutes. Podcasts which are audio-only based courses and short training videos on various security processes and procedures.

Security Shorts

www.dss.mil/cdse/shorts

Security Podcasts

www.dss.mil/cdse/catalog/podcasts

Security Training Videos

www.dss.mil/seta/training_videos.html

