Student Guide
DOD Activity Security Practices Short

Introduction

Welcome to the DOD Activity Security Practices Short.

The intent of this Short is to provide an overview of the roles and responsibilities of the Department of Defense Activity Security Manager and how they implement the activity's Information Security Program (or ISP) while ensuring its visibility and effectiveness on behalf of the activity leadership.

Here is the learning objective and key topics; take a moment to review them.

Learning Objective:

- Identify the definition of ACCM, steps in the ACCM approval process, guidance on ACCM use, security measures, provisions for safeguarding ACCM information, and procedures for ACCM termination.

Key Topics:

- ISP Policies and Guidance
- ASM Qualifications
- ASM Areas of Responsibility

Policies and Guidance: Executive Order 13526

The driving force behind the DOD ISP comes from Presidential Executive Order, or E.O., 13526. This E.O. states that all U.S. Government departments and agencies will adhere to a "uniform system for classifying, safeguarding, and declassifying national security information." It also lists the priorities for that system.

As ASMs, we meet those priorities through accurate and accountable application of classification standards and routine, secure, and effective declassification.

Executive Order (E.O.) 13526 Priorities:

- Protecting information critical to our nation's security
- Demonstrating our commitment to open government

Policies and Guidance: DODM 5200.01/DODI 5200.48

In response to E.O. 13526, DOD has established its ISP and related requirements in DODM 5200.01, Volumes one through three and DODI 5200.48. We will review the ASM's qualifications and responsibilities that have been delineated in volumes one and three and will provide resources that can assist security managers in meeting their existing and emerging responsibilities.

DOD ISP Policy

DOD Manual 5200.01 DOD Information Security Program:

- Volume 1, Overview, Classification, and Declassification -- Describes the DOD Information Security Program. Provides guidance for classification and declassification of DOD information that requires protection in the interest of the national security.
- Volume 2, Marking of Information -- Provides guidance for the correct marking of classified information.
- Volume 3, Protection of Classified Information -- Provides guidance for the safeguarding, storage, destruction, transmission, and transportation of classified information; details security-related training requirements; prescribes processes for handling security violations and compromises; and addresses information technology (IT) issues.

DOD Instruction 5200.48

- Controlled Unclassified Information (CUI) -- Provides guidance for the identification and protection of CUI.

Appointment of Activity Security Manager

When appointing an ASM, DODM 5200.01,Volume 1 requires heads of DOD activities to designate an ASM in writing, give that security manager the authority to ensure personnel adhere to program requirements, provide them direct access to the activity's leadership, and organizationally align them to ensure prompt and appropriate attention to program requirements.

While the DOD requires every activity that "creates, handles, or stores classified information" to appoint a security manager, it recognizes that one size does not fit all and allows for an activity's appointee to work on a full-time, part-time, or collateral duty basis. The key requirement is that the enumerated ASM's responsibilities be adequately and professionally executed and implemented.

Heads of DOD Activities must:

- Designate the ASM in writing
- Give authority to ensure adherence
- Direct access to leadership
- Align the ASM to requirements

Activity Security Manager Qualifications

The performance of the vital and sensitive responsibilities designated to an ASM requires trained, dedicated, and qualified individuals. DODM 5200.01 defines the minimal qualifications individuals must meet to be designated a DOD ASM. Specifically, they must be a U.S. citizen, have a current security eligibility to the highest level of classification of information being handled within the activity, and have access appropriate to the level of information managed.

ASM Qualifications:

- U.S. citizen
- Current security eligibility to the highest level of classification being handled
- Access appropriate to the level of information managed

NOTE:

Each Service has defined qualifications for their respective ASMs; until recently, the DOD Information Security Program did not set minimal qualifications for ASMs.

Activity Security Manager Rank Requirements

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

In activities with more than 100 personnel, the designated security manager must be, at minimum, a senior non-commissioned officer E-7 or a civilian employee equivalent to a GS-11.

In activities with less than 100 personnel, the designated security manager must be, at minimum, a senior non-commissioned officer E-6 or a civilian employee equivalent to a GS-7.

NOTE:

The DOD recognizes that within large activities, the successful fulfillment of the specified information security management responsibilities may warrant the designation of assistants by the ASM.

DODM 5200.01 specifies that ASMs may designate Activity Assistant Security Managers to assist in program implementation, maintenance, and local oversight, and, as needed, designate Top Secret Control Officers (TSCOs) and assistants to manage and account for Top Secret material. The designation of assistant security managers and TSCOs must be in writing.

Areas of Responsibility

Now that we have covered the Information Security Program guidance and ASM appointment and qualification criteria, let's look at the responsibilities of an ASM. The ASM's responsibilities, enumerated in DODM 5200.01, can be broadly classified into several categories—management and oversight; planning and coordination; compliance; education and awareness; threat and incident response; and some additional responsibilities.

ASM Responsibilities:

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

Management and Oversight

DODM 5200.01 specifies that the ASM is responsible for the management and implementation of the activity's ISP. It further specifies that the ASM is to serve as the principal advisor to the activity head on all information security matters; maintain cognizance of all activity security functions to include information, personnel, information systems, physical, and industrial related functions; and provide guidance, direction, coordination, and oversight to designated security assistants.

Management and Oversight:

- Manage and implement ISP
- Advise on all information security matters
- Maintain cognizance of all activity security functions
- Guide, direct, and coordinate assistants

Planning and Coordination

ASMs must perform a wide variety of implied and specified planning-related activities. The specified planning responsibilities are the development of written instructions for safeguarding classified information during emergencies and military operations, and the development of security procedures regarding visitor access. 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. ASMs must also coordinate and liaise with a broad range of individuals and activity functions.

Coordination:

- DODM 5200.01, Vol 1, Enclosure 2, states the ASM must:
- Maintain communication 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
- Collaborate with Information Systems Security Professionals (ISSPs) as required for effective management, use, and oversight of classified information in electronic form
- Coordinate the preparation, dissemination, and maintenance of Security Classification Guides (SCGs) with Original Classification Authorities (OCAs); correspond, when necessary, with the proper authorities in response to security threats and incidents
- Maintain communication with the Special Security Officer (SSO), as appropriate, on issues of common concern.

Compliance

The ASM's responsibility for the successful implementation of an activity's ISP entails ensuring fundamental compliance with the overarching DOD ISP policies and procedures.

DODM 5200.01 specifies that the security manger must ensure that access to classified information is limited to appropriately cleared personnel with a need-to-know, ensure implementation of and compliance with information security requirements for all uses of information technology, and guarantee compliance with information security requirements when access to classified information is provided to industry contractors.

Education and Awareness

Successful compliance with the DOD ISP 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 ASM. DODM 5200.01 specifically requires the ASM 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

ASMs must manage the activity's response to security threats and incidents. Specifically, DODM 5200.01 specifies that 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.

It is the ASM's responsibility to take appropriate action to mitigate damage and prevent recurrence of security issues.

ASM's must ensure that classified information, security threats and incidents are:

- Reported
- Recorded
- Coordinated
- Investigated

Additional Responsibilities

There are some additional requirements within DODM 5200.01 that have been specifically identified as a responsibility of the ASM.

ASM Additional Responsibilities:

- Security Incident Reporting -- ASMs are critical linchpins in the reporting, recording, and investigation of security incidents involving classified information within an activity. DOD policy requires that anyone who becomes aware of the loss or potential compromise of classified information must immediately report it to the ASM, with the only exception being in cases where the ASM may have been involved. In those cases, higher command reporting is required.

  ASM responsibilities regarding responding to reported security incidents include initiating an inquiry by appointing an uninvolved inquiry officer, who then provides a report of their findings within 10 duty days, and, in the case of security incidents involving on-site contractors, provides a copy of the results of any inquiry to the contracting company and to the Defense Counterintelligence and Security Agency (DCSA). For those incidents over which ASMs do not have cognizance, they must ensure incidents are reported to the appropriate authorities.

- IT -- DODM 5200.01, Volume 3 includes newly specified requirements related to the security issues posed by the variety of information technology used within DOD activities.

  DODM 5200.01 specifies that in the case of data spills, ASMs are responsible for maintaining overall lead for addressing the event, ensuring unauthorized disclosure policy requirements are met, and coordinating closely with information technology and Information Assurance (IA) staff.

  Some of the ASM's other responsibilities related to IT include the requirement in which they must approve and authorize in writing the use of any remote diagnostic or repair capabilities, and ASMs must coordinate with the local designated approval authorities and/or IT staff to ensure procedures for the disposal of computer hard drives appropriately address the removal of U.S. Government data prior to disposal. Some activities may appoint an ISSP that satisfies the IT roles for the activity.

- Training -- The DOD recognizes that the successful fulfillment of all the specified and implied ASM responsibilities requires a highly trained and increasingly professional cadre of security-minded personnel. It has prescribed a wide range of training requirements that security managers must not only personally meet but 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; the marking of classified documents; the proper use, storage, reproduction, transmission, dissemination, and destruction of classified information; the investigation and reporting of instances of actual or potential compromise; and procedures for the secure use of information systems and networks.

Knowledge Checks

Question 1

Read the question below and select the best response.

Who is responsible for the implementation of a DOD activity’s ISP on behalf of the activity head?

- ○ Office of the Under Secretary of Defense for Intelligence & Security (OUSD(I&S))
- ○ National Security Agency (NSA)
- ○ Activity Security Manager (ASM)
- ○ Defense Intelligence Agency (DIA)

Question 2

Read the question below and select all that apply.

Which policy provides guidance on the responsibilities of the ASM?

- ○ DODM 5200.02
- ○ DODM 5200.01, Vol. 1
- ○ DD-254
- ○ DODI 5200.48

Question 3

Read the question below and select the best response.

Who is responsible for designating an ASM in writing?

- ○ Office of the Under Secretary of Defense for Policy
- ○ National Security Agency
- ○ Heads of DOD activities
- ○ Defense Intelligence Agency

Summary

In this Short, we have discussed the policies and guidance that regulate the ISP, reviewed the ASM's qualifications, and examined their areas of responsibility.

To access more information on DOD Activity Security Practices, please visit the Course Resources.

This Short covered the following topics:

- ISP Policies and Guidance
- ASM Qualifications
- ASM Areas of Responsibility

Conclusion

Congratulations! You have completed the DOD Activity Security Practices Short.

Knowledge Check Answer Key

Question 1

Read the question below and select the best response.

Who is responsible for the implementation of a DOD activity’s ISP on behalf of the activity head?

- ○ Office of the Under Secretary of Defense for Intelligence & Security (OUSD(I&S))
- ○ National Security Agency (NSA)
- ● **Activity Security Manager (ASM)**
- ○ Defense Intelligence Agency (DIA)

Feedback: The ASM is responsible for the implementation of a DOD activity’s ISP on behalf of the activity head.

Question 2

Read the question below and select all that apply.

Which policy provides guidance on the responsibilities of the ASM?

- ○ DODM 5200.02
- ● **DODM 5200.01, Vol. 1**
- ○ DD-254
- ● **DODI 5200.48**

Feedback: DODM 5200.01, Vol. 1 and DODI 5200.48 provide guidance on the responsibilities of the Activity Security Manager.

Question 3

Read the question below and select the best response.

Who is responsible for designating an ASM in writing?

- ○ Office of the Under Secretary of Defense for Policy
- ○ National Security Agency
- ○ Heads of DOD activities
- ● **Defense Intelligence Agency**

Feedback: The heads of DOD activities designate the ASM in writing.