

Student Guide

Alternative Compensatory Control Measures (ACCM) Short

Introduction

Welcome to the Alternative Compensatory Control Measures Short!

This Short will discuss the ACCM requirements that may be employed when determining that standard security measures are insufficient.

Hi, I'm Karl, the head of a DOD component I will be guiding you through this Short.

As part of my job, I need to be able to use ACCM accurately and appropriately.

I need to be familiar with:

- What ACCM is
- What factors are required for ACCM approval
- When the use of ACCM is appropriate
- What security measures to follow with an ACCM
- What the provisions are for safeguarding ACCM information and
- When to implement procedures for ACCM termination

Take a moment to review the learning objective.

This Short should take about fifteen minutes to complete.

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.

What is ACCM?

According to Department of Defense Manual (DODM) 5200.01, Alternative Compensatory Control Measures (ACCMs) are security measures used when the policy is insufficient to enforce need-to-know for classified information and Sensitive Compartmented Information (SCI) or Special Access Program (SAP) protections are not necessary.

A Head of a DOD Component with original classification authority (OCA) may employ ACCM when they determine that the standard security measures detailed in DODM 5200.01 are insufficient.

ACCM consists of three measures: creating a specific description of the information subject to the enhanced ACCM control, maintaining a list of personnel to whom the classified information has been or may be provided, and guidelines for the use of unclassified nicknames.

ACCM Proponents

The Office of the Under Secretary of Defense for Policy (or OUSD(P)) is responsible for the management, oversight and Congressional reporting of ACCM.

The Office of the Under Secretary of Defense for Intelligence and Security, the OUSD(I&S), is responsible for the ACCM security policy.

Given this sharing of ACCM responsibilities, staffing elements in both OUSD(P) and OUSD(I&S) work together to ensure transparency of all ACCM actions.

ACCM Approval

As a DOD Component Head, several items must be considered prior to the establishment of an ACCM:

- What is the criticality of the information requiring protection?
- What type of damage could it cause to national security – what is the sensitivity?
- What is the value of the information which needs protection?
- What are the threats, both known and anticipated?
- What are the vulnerabilities for exploitation? And,
- What are the countermeasures based on a cost-benefit analysis?

As you can see, there are numerous considerations before an ACCM is established and approved.

Guidance on ACCM Use

You may ask, “Why would an organization use an ACCM?”

An ACCM is incorporated when normal measures are not sufficient to enforce need-to-know for classified DOD intelligence matters, classified operations, sensitive support, and other non-intelligence activities.

I coordinate with OUSD(P) to avoid duplicating nicknames of other ACCMs to guarantee that nicknames I choose are consistent with policy.

The control officer maintains a roster listing all personnel who have access along with their current status.

Once established, I must continue to maintain a system for recurrent inspection of the approved ACCM to ensure continued compliance with the provisions in DODM 5200.01.

All ACCM documents and materials must be marked as specified in Enclosure 4 of Volume 2 of DODM 5200.01.

ACCMs are not to be used for acquisition programs or activities progressing through the acquisition process.

Prohibited Security Measures

After reviewing policy, it was noted that more stringent security measures that would be used for a SAP or SCI program to establish access eligibility to ACCM-protected information is prohibited. Additionally, code words or other abbreviated approvals of the nickname are not allowed.

Be sure to avoid specialized non-disclosure agreements or any certificates of disclosure or nondisclosure for ACCM access.

Lastly, do not use a rank or position structure to control access to the ACCM.

Prohibited Uses of ACCM

When working with North Atlantic Treaty Organization (NATO) or non-intelligence Foreign Government Information (FGI), ACCM cannot be used, except under the following conditions:

NATO exceptions can be granted only by the Secretary of Defense.

Non-intelligence FGI exceptions can be granted only by the Under Secretary of Defense for Policy (or USD(P)).

If an approval for an exemption is received, I retain the documentation.

ACCMs are not used to protect classified information in acquisition programs or to protect technical or operational requirements of systems in the acquisition process.

When protecting Restricted Data (RD), Formerly Restricted Data (FRD), Communications Security (COMSEC), SCI, SAP, or Nuclear Command and Control Extremely Sensitive Information (NC2-ESI), utilize the appropriate classification rather than ACCM.

An ACCM should not be used to protect unclassified information.

Never use ACCM to preclude or impede Congressional, Office of the Secretary of Defense (OSD), or other appropriate oversight of programs, command functions, or operations.

Lastly, do not use ACCMs to justify funding to procure or maintain a separate ACCM communication system.

Safeguarding ACCM Information

There are several provisions to consider when safeguarding ACCM information.

Top Secret, Secret, and Confidential cover sheets used to cover ACCM material are marked with "ACCM" and the appropriate nickname.

Cover sheets designated for use with ACCM must be approved by the Director of Security and OUSD(I&S) prior to use.

ACCM material is handled and stored based on the security classification of the information contained therein and in a manner that separates it from non-ACCM classified information.

ACCM information is transmitted in the same manner as other classified information at the same classification level with some exceptions.

When packaging ACCM information for transmission, mark the inner envelope with the

- Appropriate classification
- Caveat “ACCM”
- Assigned nickname, and the
- Name of an individual authorized access to the ACCM information

Transmission of Information

Use the ACCM nickname in the text of the message traffic and on cover sheets accompanying secure facsimile transmissions. Before sending, always make sure that the authorized recipient is awaiting the transmission.

When using the Defense Message System (DMS), mark the material as SPECAT (Special Category) and only use one ACCM nickname in the message.

It is your responsibility to configure ACCM-protected information with appropriate discretionary access controls to help ensure that only authorized individuals have access.

When Secret Internet Protocol Router Network (SIPRNET) is used to transmit ACCM information, mark each transmission with ACCM and the authorized nickname. Only transmit information to individuals who are authorized to access that ACCM information.

Transmission of ACCM information, in any form, will be consistent with the security classification assigned. ACCM protection does not require the transmission of the information by methods usually reserved for a higher level of classified information.

ACCM Termination

When ACCM security measures are no longer required, a notification of termination must be submitted in writing.

Knowledge Checks

Question 1

Read the question below and select the best response.

Which policy provides guidance on ACCM?

- NISPOM
- DODM 5200.01
- DD-254
- DODI 5200.48

Question 2

Read the question below and select the best response.

Which office is the DOD staff proponent for ACCM management, oversight, and Congressional reporting?

- Office of the Under Secretary of Defense for Policy (OUSD(P))
- Office of the Under Secretary of Defense for Information & Security (OUSD(I&S))
- National Security Agency (NSA)
- Defense Intelligence Agency (DIA)

Question 3

Read the question below and select the best response.

Which office is responsible for ACCM security policy?

- Office of the Under Secretary of Defense for Policy (OUSD(P))
- National Security Agency (NSA)
- Office of the Under Secretary of Defense for Information & Security (OUSD(I&S))
- Defense Intelligence Agency (DIA)

Question 4

Read the question below and select the best response.

Which of the following is NOT a consideration for ACCM approval?

- Criticality of information
- Vulnerabilities to exploitation
- Source of information
- Sensitivity to national security

Question 5

Read the question below and select the best response.

Which of the following are approved uses of ACCMs?

- Classified DOD intelligence matters
- Classified information in acquisition programs
- Unclassified information
- Classified operations

Question 6

Read the question below and select the best response.

True or False: ACCM can be used to protect classified information in acquisition programs.

- True
- False

Question 7

Read the question below and select the best response.

True or False: Top Secret, Secret, and Confidential cover sheets used to cover ACCM material shall be marked with ACCM and the appropriate nickname.

- True
- False

Question 8

Read the question below and select the best response.

ACCM security measures are terminated:

- When the measure expires
- When they are no longer required
- 10 years after the ACCM is employed
- When the OUSD issues written notification

Summary 1190

You should now be familiar with Alternative Compensatory Control Measures.

You should be able to identify the definition of ACCM, steps in the ACCM approval process, guidance on ACCM use, prohibited security measures, provisions for safeguarding ACCM information, and the procedure for ACCM termination.

To access more information on ACCM, please visit the Course Resources.

Conclusion 1200

You have completed the Alternative Compensatory Control Measures Short.

Select Exit to leave this Short.

Knowledge Check Answers

Question 1

Read the question below and select the best response.

Which policy provides guidance on ACCM?

- NISPOM
- DODM 5200.01**
- DD-254
- DODI 5200.48

Feedback: The DODM 5200.01 provides guidance on ACCM.

Question 2

Read the question below and select the best response.

Which office is the DOD staff proponent for ACCM management, oversight, and Congressional reporting?

- Office of the Under Secretary of Defense for Policy (OUSD(P))**
- Office of the Under Secretary of Defense for Information & Security (OUSD(I&S))
- National Security Agency (NSA)
- Defense Intelligence Agency (DIA)

Feedback: OUSD(P) is the DOD staff proponent for ACCM management, oversight, and Congressional reporting.

Question 3

Read the question below and select the best response.

Which office is responsible for ACCM security policy?

- Office of the Under Secretary of Defense for Policy (OUSD(P))
- National Security Agency (NSA)
- Office of the Under Secretary of Defense for Information & Security (OUSD(I&S))**
- Defense Intelligence Agency (DIA)

Feedback: OUSD(I&S) is responsible for ACCM security policy.

Question 4

Read the question below and select the best response.

Which of the following is NOT a consideration for ACCM approval?

- Criticality of information
- Vulnerabilities to exploitation
- Source of information**
- Sensitivity to national security

Feedback: Source of information is NOT a consideration for ACCM approval.

Question 5

Read the question below and select the best response.

Which of the following are approved uses of ACCMs?

- Classified DOD intelligence matters**
- Classified information in acquisition programs
- Unclassified information
- Classified operations**

Feedback: Classified DOD intelligence matters and classified operations are approved uses of ACCMs.

Question 6

Read the question below and select the best response.

True or False: ACCM can be used to protect classified information in acquisition programs.

- True
- False**

Feedback: ACCM cannot be used to protect classified information in acquisition programs.

Question 7

Read the question below and select the best response.

True or False: Top Secret, Secret, and Confidential cover sheets used to cover ACCM material shall be marked with ACCM and the appropriate nickname.

- True**
- False

Feedback: Top Secret, Secret, and Confidential cover sheets used to cover ACCM material shall be marked with ACCM and the appropriate nickname.

Question 8

Read the question below and select the best response.

ACCM security measures are terminated:

- When the measure expires
- When they are no longer required**
- 10 years after the ACCM is employed
- When the OUSD issues written notification

Feedback: ACCM measures are terminated by the establishing DOD Component when they are no longer required.