

Center for Development of Security Excellence
CDSE
Learn. Perform. Protect.



Alternative Compensatory Control Measures

 **Information Security Webinar** 

Alternative Compensatory Control Measures

Host: Anthony Lane

- Security Specialist Instructor
- Course Manager
- Twenty-two years in U.S. Navy
- Experienced Security Manager

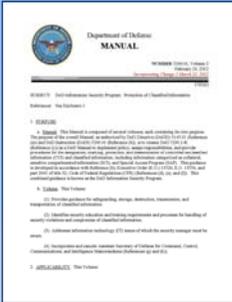


 **Administrative Announcements** 

- Use the Q & A box to ask questions.
- These slides can be downloaded. Select the file in the File Share box below.
- You will also find DoD Manual 5200.01, Volume 3, Enclosure 2, Section 18, which will be referenced during this webinar.
- This webinar will present poll questions.

 **Poll 1** 

 **DoDM 5200.01, Vol. 3, Encl. 2, Sec. 18** 



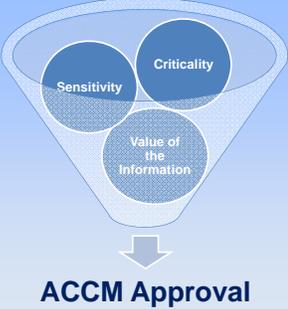
Head of a DoD Component with OCA may employ ACCM when:

- Standard security measures are insufficient
- SCI or SAP protections are not warranted

 **DoD Proponents** 

- **Office of Under Secretary of Defense for Policy (OUSD(P)):** DoD staff proponent for ACCM management, oversight, and Congressional reporting
- **Office of Under Secretary of Defense for Intelligence (OUSD(I)):** Proponent for ACCM security policy

 **ACCM Approval** 



ACCM Approval

 **Guidance on ACCM Use** 

To assist in enforcing need-to-know for classified:

- DoD intelligence matters
- Operations, sensitive support, and other non-intelligence activities



 **Guidance on ACCM Use** 

- Nickname consistent with CJCSM 3590.27D
- Access roster must differentiate active/inactive access
- Not used for acquisition programs or activities



 **Prohibited Security Measures** CDSE

Prohibited security measure:

- Using personnel security investigative or adjudicative standards that are more stringent than those normally required for a comparable level of classified information.



 **Prohibited Security Measures, cont.** CDSE

Prohibited Security Measures:

- Code words
- Any special terminology except nickname
- Specialized non-disclosure agreements
- Billet structure or system



 **Prohibited Uses of ACCM** CDSE



ACCM is prohibited:

- For NATO or non-intelligence Foreign Government Information (FGI)
- To protect classified information in acquisition programs

 Prohibited Uses of ACCM, cont. 



ACCM is **prohibited** to protect:

- Technical or operational requirement of systems in the acquisition process
- RD, FRD, COMSEC, SCI, or SAP
- Unclassified information

 Prohibited Uses of ACCM, cont. 



ACCM is **prohibited** to:

- Preclude or impede congressional, OSD, or other appropriate oversight of programs, command functions, or operations
- Justify funding of procuring or maintaining a separate ACCM communication system

 Poll 2 

 **Poll 3** 

Light blue rectangular area for poll content.

 **Documentation** 

Correspondence includes:

- Designation of ACCM sponsor and control officer
- Effective activation date and duration
- Any planned participation by foreign partners



 **Documentation, cont.** 

ACCM sponsor will develop and distribute:

- Program security plan
- Security classification guide
- Program participant briefing

Special Programs Office, USD(P) maintains repository of records for all DoD ACCM.



 **Annual Reports** CDSE



General data elements:

- Nickname
- Purpose/description
- Duration
- Sponsor
- Control officer(s)

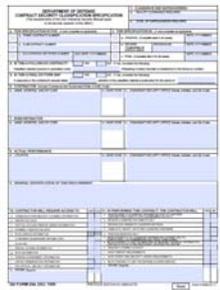
 **Sharing ACCM** CDSE



Recipient organization must abide by ACCM security requirements.

 **Poll 4** CDSE

 **Contractor Access** 



Participation must be identified in DD Form 254, "Contract Security Classification Specification."

 **Program Maintenance** 

Requirements:

- List of ACCM control officers
- Updated access control list
- Specialized training
 - Access procedures
 - Control
 - Transmission
 - Storage
 - Marking



 **Program Maintenance, cont.** 

Requirements:

- Updated documentation every 5 years
- With annual report, the ACCM sponsor provides:
 - List of primary and alternate ACCM control officers
 - Confirmation that documentation is current



 **Safeguarding** 

Requirements:

- Cover sheets overstamped or marked with "ACCM" and appropriate nickname
- Handled and stored in a manner that separates ACCM from non-ACCM classified information
- Use separate folders or drawers



 **Chat Question** 

What are some secure methods for transmitting ACCM?

Enter your responses in the chat box.



 **Transmission and Transportation** 

Transmission methods:

- Inner envelope to be marked with "ACCM," nickname, and addressed to authorized individual
- ACCM nickname will be on text of message traffic and fax coversheets
- Mark "SPECAT" for DMS transmission



Portion Markings CDSE

SECRET//ACCM-FICTITIOUS EFFORT/TEA LEAF
FOR TRAINING PURPOSES ONLY

(S//ACCM) This is the marking for a portion which is SECRET ACCM-protected information with the nicknames "FICTITIOUS EFFORT" and "TEA LEAF" (same as banner marking).

(S//ACCM-TEA LEAF) An ACCM-protected portion requiring only the nickname "TEA LEAF" would be marked as shown in this paragraph.

(S//ACCM-FICTITIOUS EFFORT) This is the marking for a portion which is SECRET ACCM-protected information requiring only the nickname "FICTITIOUS EFFORT."

Classified By: Tom Brown, Chief, Tea Leaf Program Ofc
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20121215

SECRET//ACCM-FICTITIOUS EFFORT/TEA LEAF

From DoD Manual 5200.01, Volume 2, Enclosure 4

Security Incidents CDSE



- Deleting a file or material is normally a sufficient action.
- ACCM sponsor should be notified when inquiry and investigation are completed.
- Damage assessment responsibility is with ACCM sponsor.

Security Incidents CDSE

- Reporting, inquiry, investigation, and damage assessment conducted per DoDM 5200.01, Volume 3, Enclosure 6.
- Inadvertent disclosure forms are not authorized for use with ACCM information.

Department of Defense
MANUAL

SECURITY CLASSIFICATION: SECRET
DATE: 12/15/2007

5200.01-01 (01) Information Security Program: Protection of Classified Information

Reference: 5200.01-01

1. PURPOSE

1.1. (S//ACCM) This manual is a component of the DoD Information Security Program (ISP) and provides the policy, procedures, and standards for the protection of classified information. It is intended to be used in conjunction with DoD Manual 5200.01-01, Information Security Program: Protection of Classified Information, and DoD Manual 5200.01-02, Information Security Program: Protection of Classified Information.

1.2. (S//ACCM) This manual is a component of the DoD Information Security Program (ISP) and provides the policy, procedures, and standards for the protection of classified information. It is intended to be used in conjunction with DoD Manual 5200.01-01, Information Security Program: Protection of Classified Information, and DoD Manual 5200.01-02, Information Security Program: Protection of Classified Information.

1.3. (S//ACCM) This manual is a component of the DoD Information Security Program (ISP) and provides the policy, procedures, and standards for the protection of classified information. It is intended to be used in conjunction with DoD Manual 5200.01-01, Information Security Program: Protection of Classified Information, and DoD Manual 5200.01-02, Information Security Program: Protection of Classified Information.

1.4. (S//ACCM) This manual is a component of the DoD Information Security Program (ISP) and provides the policy, procedures, and standards for the protection of classified information. It is intended to be used in conjunction with DoD Manual 5200.01-01, Information Security Program: Protection of Classified Information, and DoD Manual 5200.01-02, Information Security Program: Protection of Classified Information.

1.5. (S//ACCM) This manual is a component of the DoD Information Security Program (ISP) and provides the policy, procedures, and standards for the protection of classified information. It is intended to be used in conjunction with DoD Manual 5200.01-01, Information Security Program: Protection of Classified Information, and DoD Manual 5200.01-02, Information Security Program: Protection of Classified Information.

1.6. (S//ACCM) This manual is a component of the DoD Information Security Program (ISP) and provides the policy, procedures, and standards for the protection of classified information. It is intended to be used in conjunction with DoD Manual 5200.01-01, Information Security Program: Protection of Classified Information, and DoD Manual 5200.01-02, Information Security Program: Protection of Classified Information.

1.7. (S//ACCM) This manual is a component of the DoD Information Security Program (ISP) and provides the policy, procedures, and standards for the protection of classified information. It is intended to be used in conjunction with DoD Manual 5200.01-01, Information Security Program: Protection of Classified Information, and DoD Manual 5200.01-02, Information Security Program: Protection of Classified Information.

1.8. (S//ACCM) This manual is a component of the DoD Information Security Program (ISP) and provides the policy, procedures, and standards for the protection of classified information. It is intended to be used in conjunction with DoD Manual 5200.01-01, Information Security Program: Protection of Classified Information, and DoD Manual 5200.01-02, Information Security Program: Protection of Classified Information.

1.9. (S//ACCM) This manual is a component of the DoD Information Security Program (ISP) and provides the policy, procedures, and standards for the protection of classified information. It is intended to be used in conjunction with DoD Manual 5200.01-01, Information Security Program: Protection of Classified Information, and DoD Manual 5200.01-02, Information Security Program: Protection of Classified Information.

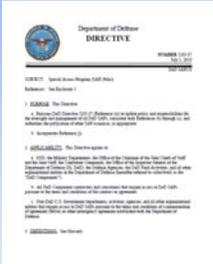
1.10. (S//ACCM) This manual is a component of the DoD Information Security Program (ISP) and provides the policy, procedures, and standards for the protection of classified information. It is intended to be used in conjunction with DoD Manual 5200.01-01, Information Security Program: Protection of Classified Information, and DoD Manual 5200.01-02, Information Security Program: Protection of Classified Information.

 **ACCM Termination** 



- Terminated by establishing DoD Component
- Notification must be submitted in writing

 **Transitioning to a SAP** 



If the DoD Component determines the ACCM requires protection as a SAP, the request must be made in accordance with SAP policy.

 **Contacts and Resources** 

- Slides and frequently asked questions from this webinar will be posted at <http://www.cdse.edu/catalog/webinars/information-security/alternate-compensatory.html>
- Email information security training related questions to DSS at informationsecurity.training@dss.mil
