BY ORDER OF THE COMMANDER AIR FORCE SPECIAL OPERATIONS COMMAND

AIR FORCE SPECIAL OPERATIONS COMMAND INSTRUCTION 16-1404

12 JULY 2022

Operations Support

ALTERNATIVE COMPENSATORY CONTROL MEASURES PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at www.e-Publishing.af.mil.

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: USAF/AFSOC/SA STO

Certified by: AFSOC/SA STO (GS-13, Larry Wood)

Supersedes: AFSOCI16-703, 14 MAY 2018

Pages: 14

This publication implements DoDM5200.01V3_AFMAN16-1404V3, *Information Security Program: Protection of Classified Information,* and Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3213.O2D, *Joint Staff Alternative Compensatory Control Measures (ACCM) Program*. It provides guidance and procedures for persons assigned to or working for Headquarters (HQ) Air Force Special Operations Command (AFSOC) and AFSOC assigned units. The Joint Staff ACCM Program applies to AFSOC-gained Air Force Reserve Command and Air National Guard units. This publication does not apply to the United States Space Force. This publication may be supplemented at any level, but all direct supplements must be routed to the OPR of this publication for coordination prior to certification and approval. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the DAF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 through the appropriate functional's chain of command. The authorities to waive wing, unit, level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the publication OPR for non-tiered compliance items. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW AFI 33-322, *Records Management and Information Governance Program*, and disposed of IAW Air Force Records Disposition Schedule located in the Air Force Records Information Management System. This publication requires the collection and/or maintenance of information protection by the Privacy Act of 1974 authorized by Title 10 U.S.C. Sec 9013, *Secretary of the Air Force*. The applicable System of Records Notice (SORN) DUSDI 02-DoD, *Personnel Vetting*

Records System, is available at **https://dpcld.defense.gov/privacy/SORNS.aspx**. Compliance with **Attachment 2** and **Attachment 3** is mandatory.

1. General Information.

1.1. CJCSM 3213.02D.

1.1.1. CJCSM 3213.02D, *Joint Staff Alternative Compensatory Control Measures (ACCM) Program Management Manual*, establishes broad ACCM program procedures for the entire Department of Defense (DOD). This instruction provides specific guidance on ACCM procedures for HQ AFSOC, and all AFSOC subordinate units. The ACCM checklist listed in **Attachment 2** provides the framework of the Management Internal Control Toolset for each AFSOC unit to conduct a preliminary inquiry. The Management & Internal Control Tool checklists will be the basis for any Staff Assistance Visit or inspection.

1.2. ACCMs.

1.2.1. ACCMs are a unique security control for the protection of classified information when other security measures detailed in Executive Order No. 12958 and DOD Directive 5200.1-R, are determined to be insufficient for that purpose and where Special Access Program (SAP) controls are not warranted or approved. ACCMs use an unclassified nickname and only the Vice Director Joint Staff can approve creation of an ACCM program. All requests to create ACCMs will be forwarded to AFSOC/SA for review and to be submitted to the Joint Staff through United States Special Operations Command (USSOCOM) J33 for approval.

1.3. ACCM Coordination Officers (ACCM COORDs).

1.3.1. ACCM Coordination Officers (ACCM COORDs) are access controllers required to enforce strict Need-to-Know (NTK) and material contribution policies for each ACCM as defined by the Program Sponsor for all personnel. No persons shall be accessed for expedience or convenience.

1.4. USSOCOM.

1.4.1. The USSOCOM integrated security system for managing access to ACCM material is the "Need-to-Know Managers Module" (NTKMM). NTKMM is the USSOCOM-approved tool used to track access to ACCM material on the Secret Internet Protocol Router Network (SIPR). NTKMM feeds Access Control Lists (ACLs) into the backside security tool; Secure Email Marking Program. NTKMM & Secure Email Marking Program allow ACCM access to indoctrinated personnel, while denying ACCM access to non-indoctrinated personnel.

2. Roles and Responsibilities.

2.1. AFSOC ACCM COORD.

2.1.1. Will perform all Major Command level ACCM COORD duties required to maintain ACCM sponsorship from USSOCOM ACCM COORD (USSOCOM /J33) and Headquarters Air Force ACCM COORD (HAF/A3O).

2.1.2. Will establish AFSOC ACCM policy for subordinate units via this instruction and policy letters signed by AFSOC/CC or AFSOC/CoS.

2.1.3. Will establish and maintain ACCM relationships between AFSOC and other commands.

2.1.4. Will maintain an ACCM portal on Network Internet Protocol Router to post unclassified guidance and material for ACCM Coordinators.

2.1.5. Will maintain access to USSOCOM's ACCM portal on Secure Internet Protocol Network (SIPR) to post classified guidance and material for ACCM Coordinators.

2.1.6. Will collect and post appointment letters for all AFSOC sponsored ACCM COORDs. Appointment letters must be updated annually.

2.1.7. Will provide and post ACCM Extension letters for every AFSOC sponsored ACCM COORD. These letters must specify what permissions are granted to each ACCM COORD for each ACCM extended. Will be reviewed annually and updated as required.

2.1.8. Will facilitate AFSOC sponsored units' access to USSOCOM's NTKMM via appointment letters and designated administrators.

2.1.9. Will provide Management & Internal Control Tool inspection checklists to AFSOC sponsored ACCM Coordinators.

2.1.10. Will assist subordinate units in all ACCM matters as requested by sponsored ACCM COORDs.

2.2. **Wing Commanders.**

2.2.1. Will designate a primary and an alternate ACCM COORD in accordance with CJCSM 3213.02D to receive ACCM sponsorship from AFSOC. The Primary ACCM COORD will be an O-3, civilian equivalent, or higher. Alternate ACCM COORDs will be NCOs (E-5 and above or civilian equivalents). AFSOC units will appoint only one primary ACCM COORD. Multiple alternate COORDs are allowed but should be limited to a reasonable number to allow for proper ACCM management. The primary ACCM COORD is responsible for all aspects of ACCM management at his/her unit. ACCM management will not be delegated below the Wing level. Groups and squadrons will be administered by their respective Wings.

2.2.2. Will appoint the unit ACCM COORDs in writing and annotate who is authorized to brief personnel into ACCM programs.

2.2.3. Will establish an ACCM policy in writing which provides detailed guidance on who, based on need-to-know and material contribution, should be accessed to what ACCM (s). The guidance will address active duty military, government civilians, contractors, and Air Force Reserve Command/Air National Guard augmentees. This will ensure commander's intent and provide senior leadership with visibility of all briefed personnel in the organization. The number of accessed personnel should be kept to the absolute minimum required to perform the mission.

2.3. **AFSOC Sponsored Organizational ACCM COORDs.**

2.3.1. Will enforce Major Command and Wing ACCM policies. ACCM COORDs will inform the Major Commands should the Geographic Combatant Command or Theater Special Operations Command (TSOC) ACCM COORD initiate a policy that is not compatible with this instruction.

2.3.2. ACCM COORD will notify AFSOC ACCM COORD of any ACCM program being considered for extension to them for management & distribution from someone other than the AFSOC ACCM COORD. Permission to disseminate access to an ACCM program must come from an authorized Program Sponsor and must be auditable according to CJCSM 3213.02D.

2.3.3. Will not establish any ACCM Memoranda of Agreement between units without AFSOC ACCM COORD approval.

2.3.4. Will manage when, how, and who is briefed into any ACCMs. **(T-3)**

2.3.5. Will maintain and enforce an ACCM training program to retrain 100% of accessed personnel annually in accordance with CJCSM 3213.02D.

2.3.6. Will record all ACCM indoctrinations and debriefs in USSOCOM's NTKMM access database. This allows all USSOCOM locations to share indoctrination records and verify ACCM accesses. It also allows USSOCOM to perform CJCSM mandated audits with minimal interruption to unit ACCM COORDs.

2.3.7. Will debrief personnel, ensure member's access to ACCM material is removed, and will remind individuals that the member is required to protect ACCM information.

2.3.8. Will monitor AFSOC's ACCM portals for ACCM updates.

2.3.9. Will allow security managers access to ACCM credentials on NTKMM to facilitate visit requests. Additional coordination may be required when visiting sites like Ft Bragg, who do not use SOCOM's NTKMM as their primary ACCM tracking mechanism. **(T-3)**

2.3.10. Will contact external unit ACCM COORDs to verify ACCM credentials when USSOCOM's access database is not sufficient. This is meant to ease coordination between units while conducting joint exercises. **(T-3)**

2.3.11. Will maintain a network account for each network they authorize their users to process ACCM material on (not every network is authorized to handle every ACCM).

2.3.12. Will maintain a network account for JSOC Information Automated Network Terminal network to access the remaining legacy USSOCOM ACCM access database. **(T-3)**

2.3.13. Will contact AFSOC if there are any security incidents involving spillage and/or inadvertent disclosure of ACCM material via classified network systems. COORD will route appropriate inquiry (as required) documentation to AFSOC for approval/signature

3. Access Procedures.

3.1. Authority to Operate.

3.1.1. ACCM COORDs will be appointed in writing by their Special Operations Wing/CC, CV, or CoS with a copy on file with the AFSOC ACCM COORD. AFSOC

sponsored units below group level will appoint ACCM COORDs in writing by their unit commander if approved by the AFSOC ACCM COORD.

3.1.2. ACCM COORDs will provide a copy of unit level ACCM policy memorandums to the AFSOC ACCM COORD.

3.1.3. All ACCM ACLs will be tracked in USSOCOM's consolidated ACCM access database, NTKMM. If an ACCM COORD cannot access the database, it is his/her responsibility to work through his ACCM Sponsor to get all ACL updates into USSOCOM's approved database immediately following ACCM briefing or debriefing.

3.1.4. ACCM COORDs will not create Access Control Lists (ACL) without ACCM Sponsor oversight and approval. **(T-3)**

3.2. **Access to Programs.**

3.2.1. Commanders, not ACCM COORDs, will establish policies granting access to ACCM material. At a minimum, all HQ AFSOC personnel and unit operational crew members will be briefed to ACCM IVORY VALOR.

3.2.2. No persons will be granted access to ACCM material before they are indoctrinated to the program and recorded in USSOCOM's consolidated ACCM access database.

3.2.3. Unit security managers will schedule personnel for ACCM access briefing on AFSOC ACCM SharePoint, verify member has a current security clearance, and Continuous Evaluation (CE) date. If member must send and receive ACCM emails, then a SIPR email account is required prior to being scheduled for ACCM briefing. Exception to this is granted to commanders, deputies, and HQ AFSOC staff directors. If not, SIPR email not required will be annotated. **(T-3)**

3.2.4. Security managers or ACCM COORDs will complete the AFSOC Form 10, Alternative Compensatory Control Measure Access Request Worksheet to gain accesses above IVORY VALOR. A valid justification for access is required and be approved by the commander or authorized designee 0-5 and above. Security managers will delete the ACCM worksheet after member gains access to requested ACCMs.

3.2.5. ACCM COORDs, before indoctrinating individuals to an ACCM program, will verify security clearances through Defense Information System for Security (DISS) via security managers. ACCM COORDs will not brief individuals if information is incomplete or incorrect. In this case they should contact unit security manager to correct this information. A SECRET clearance is the minimum required to access ACCM material. However, more restrictive ACCMs may require a TOP SECRET clearance.

3.2.6. Before indoctrinating individuals to an ACCM program above IVORY VALOR, unit ACCM COORDs will verify the member has a valid need-to-know and has been approved for the ACCM by the commander or authorized designee (0-5 and above). ACCM Worksheet will be maintained in a folder on AFSOC SIPR SharePoint page when completed. It is at the ACCM COORD's discretion to allow or deny access to ACCM material in compliance with CJCSM 3213.02D.

3.2.7. Contractors will not be accessed to ACCM material unless their DD254 shows access to ACCM material is required in accordance with CJCSM 3213.02D. (Typically written as "ACCM access required")

3.2.8. ACCM COORDs will use the SOCOM approved ACCM briefing slides but may augment this with slides tailored to the needs of their individual unit. At a minimum, briefers will cover the critical information the audience must protect under the ACCM program as dictated by the program security classification guide.

3.2.9. Under no circumstances will Special Access Programs (SAPs) controls be applied to ACCM management. Federal law forbids Special Access Program Indoctrination Agreements, billet structures, or other SAP-like controls on ACCM programs.

3.3. **Tracking User Access.**

3.3.1. All AFSOC sponsored ACCM COORDs will use USSOCOM's consolidated ACCM access database to track all ACCMs within the purview of USSOCOM. Currently the approved database is NTKMM. ACCM COORDs must ensure member information is immediately entered in NTKMM after read-in.

3.3.2. ACCM COORDs not operating on USSOCOM's secret network (SOFNET-S) will apply for and maintain an external USSOCOM network account. Use the USSOCOM ACCM COORD as the account sponsor.

3.3.3. USSOCOM allows any user to verify ACCM access on their network, ACCM COORDs should provide the link for access which is also located on SOCOM ACCM SharePoint.

3.3.4. Permanent Change of Station (PSC), Separation or Retirement. Military personnel PCSing to another AFSOC organization or installation can maintain access to IVORY VALOR if briefed. Gaining & losing organization ACCM COORD must provide justification to AFSOC ACCM COORD to maintain access to other ACCM's beyond IVORY VALOR. **(T-3)**

3.4. **Training.**

3.4.1. Indoctrinated members will complete ACCM refresher training annually to maintain continued access to any ACCM material in accordance with CJCSM 3213.02D. At a minimum, refresher training will include the following: labeling, storage, network usage, and how to report security incidents. This training is provided through NTKMM on SOFNET-S and located on the ACCM SIPR portal.

3.4.2. ACCM COORDs will monitor training records and remove ACCM access for individuals who fail to accomplish annual refresher training. **(T-3)**

4. Security.

4.1. **Storage of Material.**

4.1.1. ACCM material will be marked: [TOP] SECRET//ACCM "PROGRAM NICKNAME"

4.1.2. ACCM material will be covered by the appropriate cover sheet in accordance with CJCSM 3213.02D (ENCLOSURE H-2). Specialized cover sheets are not normally authorized for use with ACCMs, unless approved by the Joint Staff. However, the USSOCOM cover sheet (**Attachment 3**) is an approved ACCM cover sheet. Use standard form cover sheets for TOP SECRET, SECRET, and CONFIDENTIAL over-stamped and marked "ACCM" with the "PROGRAM NICKNAME." **(T-0)**

4.1.3. ACCM material should not be left unattended unless stored in an approved safe with access by only those with NTK and clearance. If multiple ACCMs are stored in the same security container, only personnel cleared for all ACCMs contained will be allowed access. ACCM material should not be comingled with other classified material.

4.1.4. ACCM material will only be stored electronically on SOCOM ACCM Portal. Material will be stored in a folder with restricted file level permissions to allow only the ACCM COORD and authorized users access. AFSOC COORDs will run weekly checks to validate protection of ACCM information stored electronically. Additionally, this will also be a time to determine current need of ACCM information. ACCM information dated five years or more should be considered for destruction. Storing ACCM material on hard drives or share drives is not authorized.

4.1.5. In an Open Storage Facility, ACCM material should not be left unattended unless stored in an approved safe in accordance with CJCSM 3213.02D.

4.1.6. In an Open Storage Facility approved for open storage of ACCM material, the ACCM COORD will maintain an authorization letter from the AFSOC ACCM COORD. Open Storage of ACCM authorization letters will designate which specific ACCMs are authorized for Open Storage and in which specific spaces. **(T-3)**

4.1.7. In an Open Storage Facility approved for Open Storage of ACCM material, the ACCM COORD will ensure that no person is allowed unescorted access, unless accessed to all ACCMs approved for Open Storage in that Open Storage Facility. **(T-3)**

4.2. **Network Use.**

4.2.1. ACCM COORDs will ensure ACCM material is processed only on networks approved by the Program Sponsor of each specific ACCM program. **(T-3)**

4.2.2. ACCM COORDs will ensure any ACCM material allowed on a network is protected by that network's integrated security system for managing access to ACCM material. **(T-3)**

4.2.3. Individuals will use only networks approved by their authorizing ACCM COORD for handling ACCM material. **(T-3)**

4.2.4. E-mail between network enclaves of the same classification can be sent if the message is properly labeled, and the sender has verified through ACCM COORDs that the receiver and receiver's network are both cleared for that ACCM material. The sender is required to manually protect the ACCM material when they override the integrated security system. **(T-3)**

4.3. **Official Message Traffic.**

4.3.1. ACCM information is protected as classified national security information, and when transmitted by an Organizational Messaging System (OMS) (Automated Message Handling System, Decision Agent (DA), OMS Outlook, etc.), is handled under the Special Category caveat. The nickname is the key field on which delivery of special category message traffic will be controlled.

4.3.2. ACCM COORDs will ensure their organization can receive Official Message traffic classified as ACCM. **(T-3)**

4.3.3. ACCM COORDs will ensure their organization's Command Post / Operations Center / office receiving Official Message traffic has personnel cleared to receive ACCM message traffic for the organization. **(T-3)**

4.3.4. ACCM COORDs will ensure their organization's Official Message traffic classified as ACCM has the same level of protections required for printed ACCM material. **(T-3)**

4.3.4.1. Any OMS system used for ACCM messages must restrict access to only personnel cleared for that ACCM while in draft, during transfer, and in receive phases of messaging. **(T-3)**

4.3.4.2. Any OMS system used for ACCM messages will apply appropriate markings and labels to indicate that the message is special category. **(T-3)**

4.3.4.3. Any OMS system used for ACCM messages must route and profile ACCM messages to only those personnel authorized to receive messages for each specific ACCM. **(T-3)**

4.3.4.4. Due to limitations of most message processing systems, Official Messages should only contain one ACCM. If more than one ACCM is contained in the message, other transmission means (e-mail, fax, etc.) should be explored to ensure appropriate discretionary access control levels are met.

4.4. **Transport.**

4.4.1. ACCM COORDs must be informed when ACCM material is transported off station. **(T-3)**

4.4.2. Couriers will follow the procedures in DOD 5105.21-M-1, Chapter 3, Section S (sealed envelope in a locked container, etc.). However, unless the ACCM program has Secure Compartmented Information handling restrictions, the courier does not require Secure Compartmented Information transportation training. A unit courier letter for the collateral classification of the material is sufficient. **(T-3)**

4.5. **Security Incidents.**

4.5.1. Individuals discovering a compromise of ACCM material will immediately inform their ACCM COORD and commander. **(T-3)**

4.5.2. The unit ACCM COORD will immediately e-mail the AFSOC ACCM COORD with the information requested in "Preliminary Inquiry" as found in Chapter 10 of DOD 5200.1-R. This information will be sent over SIPR to the AFSOC ACCM COORD. The ACCM COORD will provide a list of ACCM briefed candidates to the unit commander to appoint as the investigating officer. The ACCM COORD will assist the investigating officer as required. **(T-3)**

4.5.3. The security investigation will be conducted IAW AFI 16-1404 and DOD 5200.1-R. **(T-3)**

4.5.4. The investigating officer will complete the detailed "Security Violation Investigation Report" as prescribed by Chapter 10 of DOD 5200.1-R (the format in DOD 5105.21-M-1 is recommended), along with the memorandum for record authorizing the investigation and forward them via SIPR or Joint Worldwide Intelligence Communication System, depending on the overall security level, to the AFSOC ACCM COORD. **(T-3)**

THOMAS R. ROBBINS, GS-15, USAF
Director, Sensitive Activities

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTIVE INFORMATION

References

Executive Order No.13526, Classified National Security Information, *29 Dec 2009*

CJCSM 3213.02D, Joint Staff Alternative Compensatory Control Measures (ACCM) Program Management Manual, *16 Aug 2016*

DOD Manual 5200.01 Volumes 1-3, DOD Information Security Program, *28 Jul 2020*

DOD Manual 5105.21 Volume 3, Sensitive Compartmented Information Administrative Security Manual: Administration for Personnel Security, Industrial Security, and Special Activities, *14 Sep 2020*

DoDM5200.01V3_AFMAN16-1404V3, Information Security Program: Protection of Classified Information, *11 Apr 2022*

Prescribed Forms

AFSOC Form 10, *Alternative Compensatory Control Measures (ACCM) Access Request Worksheet*

Adopted Forms

DAF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

ACCM—Alternative Compensatory Control Measure

ACCM COORD—ACCM Coordination Officer

ACL—Access Control List

AFSOC—Air Force Special Operations Command

CJCSM—Chairman of the Joint Chief of Staff Manual

DoD—Department of Defense

HQ—Headquarters

NTK—Need to Know

NTKMM—Need to Know Manager's Module

OPR—Office of Primary Responsibility

SAP—Special Access Program

SIPR—Secure Internet Protocol Router

USSOCOM—United States Special Operations Command

Terms

Alternative Compensatory Control Measure (ACCM)—A unique security control measure for the protection of classified information when other security measures are determined to be insufficient. ACCM material is handled in a more controlled fashion than its root collateral classification (CONFIDENTIAL, SECRET, TOP SECRET) based on NTK, but is not controlled so tightly as Special Assess Program (SAP) material.

Access Control List (ACL)—A list used to control access to restricted information. Personnel will be added or removed from the ACL based on their NTK.

Comingling—Storing unrelated material in the same container because it is of like classification.

Spillage—Inadvertent transfer of classified material from one classified electronic system to another system of lower classification.

ACCM Program—A Chaiman of the Joint Chiefs of Staff-directed system that applies handling restrictions on operationally sensitive information necessary to support the war fighter. A pyramid of ACCM COORDs are established under each ACCM's Program Sponsor to push material to subordinates based on NTK.

Need to Know (NTK)—A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform a lawful and authorized government function.

Special Access Program (SAP)—Any DOD program or activity, employing enhanced security measures exceeding those normally required for collateral information at the same level of classification shall be established, approved, and managed as a DOD SAP.

Attachment 2

SECURITY INCIDENT PRELIMINARY INQUIRY

A2.1. Security Incident Preliminary Inquiry Checklist.

A2.1.1. When, where, and how did the incident occur? What persons, conditions caused or contributed to the incident?

A2.1.2. Was classified information compromised?

A2.1.3. If a compromise occurred, what specific classified information and/or material was involved?

A2.1.4. If classified information is alleged to have been lost, what steps were taken to locate the material?

A2.1.5. In cases of compromise of classified information to the public media, the inquiry should determine:

A2.1.5.1. In what specific medial article or program did the classified information appear?

A2.1.5.2. To what extent was the compromised information disseminated?

A2.1.5.3. Was the information properly classified?

A2.1.5.4. Was the information officially released?

A2.1.6. If there was no compromise, was there a failure to comply with established security practices and procedures that could lead to compromise if left uncorrected? Is there a weakness or vulnerability in established security practices and procedures that could result in a compromise if left uncorrected? What corrective action is required?

Attachment 3

SAMPLE ACCM COVERSHEET

Figure A3.1. Sample ACCM Coversheet. **Example only - This page is unclassified**