

authorization as required by other regulations or policies.

18. ALTERNATIVE COMPENSATORY CONTROL MEASURES (ACCM). A Head of a DoD Component with original classification authority (OCA) may employ ACCM when he or she determines that the standard security measures detailed in this Manual are insufficient to enforce need to know for classified information and SCI or SAP protections are not warranted. The use of an unclassified nickname, obtained in accordance with Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3150.29C (Reference (ae)), together with a list of persons authorized access, and a specific description of information subject to the enhanced ACCM controls, are the three requisite elements of an ACCM.

a. DoD Proponents for ACCM. The DoD staff proponent for ACCM management, oversight and Congressional reporting is the OUSD(P). The proponent for ACCM security policy is the Office of the Under Secretary of Defense for Intelligence (OUSD(I)). Given this sharing of ACCM responsibilities, staff elements in OUSD(P) and OUSD(I) shall implement mechanisms that ensure transparency of all ACCM actions.

b. ACCM Approval. A Head of a DoD Component may approve ACCM use for classified information over which they have cognizance. Prior to approving the establishment of an ACCM, the criticality, sensitivity, and value of the information; analysis of the threats both known and anticipated; vulnerability to exploitation; and a countermeasures cost benefits analysis shall be assessed.

c. Guidance on ACCM Use. Use of ACCM must be consistent with the following guidance:

(1) ACCM may be used to assist in enforcing need to know for classified DoD intelligence matters. The DoD Component Head establishing or terminating any such ACCM shall provide written notification within 30 days to the Director of Security, OUSD(I), and the Director, Special Programs, OUSD(P), who shall maintain this information as long as the ACCM is in use.

(2) ACCM may be used to assist in enforcing need to know for classified operations, sensitive support, and other non-intelligence activities. The DoD Component Head establishing or terminating any such ACCM shall provide written notification within 30 days to the Director, Special Programs, OUSD(P), for review. The Director, Special Programs, OUSD(P), shall maintain this information as long as the ACCM is in use.

(3) ACCM shall not be used for acquisition programs or activities progressing through the acquisition process.

(4) DoD Components shall obtain an unclassified nickname consistent with Reference (ae) and coordinate with OUSD(P) to preclude duplication of nicknames.

(5) A roster or listing of all persons accessed to the ACCM shall be maintained by the ACCM control officer (see subparagraph 18.f.(1)(c) of this section). The access roster will differentiate between those persons actively accessed and those whose accesses are currently

inactive.

(6) ACCM documents and materials shall be marked as specified in Enclosure 4 of Volume 2 of this Manual.

(7) Heads of DoD Components must establish and maintain a system that provides for recurrent inspection of the ACCM they have approved. This mechanism shall ensure compliance with the provisions of this Manual. Each ACCM shall be overseen and inspected on a recurrent basis by the ACCM sponsor or OUSD(P).

d. Prohibited Security Measures. The application of the following security measures with ACCM material is prohibited:

(1) Using personnel security investigative or adjudicative standards that are more stringent than those normally required for a comparable level of classified information to establish access eligibility to ACCM-protected information.

(2) Using code words as defined in Reference (ae).

(3) Using trigraphs, digraphs, or other abbreviations of the approved nickname.

(4) Using specialized non-disclosure agreements or any certificates of disclosure or non-disclosure for ACCM access.

(5) Using a billet structure or system to control the position or numbers of persons afforded ACCM access.

e. Prohibited Uses of ACCM. The following uses of ACCM are prohibited:

(1) Using ACCM for NATO or non-intelligence FGI. For NATO, exceptions to this limitation can be granted only by the Secretary of Defense. For non-intelligence FGI, exceptions to this limitation can be granted only by the USD(P). Request for exceptions shall be forwarded to the Director, International Security Programs, Defense Technology Security Administration, OUSD(P), for action. Such approvals must be documented and retained by the sponsor.

(2) Using ACCM to protect classified information in acquisition programs as defined in DoDD 5000.01 (Reference (af)).

(3) Using ACCM to protect technical or operational requirements of systems in the acquisition process. Systems in operational use are not viewed as being in the acquisition process. Components of operational systems are fielded end items, not items in the acquisition process, and improvements to fielded items are eligible for ACCM status if properly justified.

(4) Using ACCM to protect Restricted Data (RD), Formerly Restricted Data (FRD), COMSEC, SCI, SAP, or Nuclear Command and Control Extremely Sensitive Information.

(5) Using ACCM to protect unclassified information.

(6) Using ACCM to preclude or impede congressional, OSD, or other appropriate oversight of programs, command functions, or operations.

(7) Using ACCM to justify funding to procure or maintain a separate ACCM communication system.

f. Documentation

(1) Use of ACCM must be approved in writing by the cognizant DoD Component Head. The correspondence establishing the ACCM shall be signed by the DoD Component Head and shall include the following information:

(a) Unclassified nickname assigned in accordance with Reference (ae).

(b) Designation of the ACCM sponsor. As a minimum, the sponsor shall be a general or flag officer, or senior executive equivalent, who has OCA at the level of or higher than the information protected by the ACCM.

(c) Designation of an ACCM control officer who shall be the organization's point of contact for all matters concerning the ACCM. Subsequent changes in designated personnel shall be provided, in writing, to the Special Programs Office, OUSD(P).

(d) Description of the essential information to be protected by the ACCM.

(e) Effective activation date and expected ACCM duration.

(f) Any planned participation by foreign partners.

(2) The ACCM sponsor shall develop and distribute a program security plan, security classification guide, and program participant briefing to all participating organizations prior to the activation of the ACCM. As a minimum, the briefing will address the specific information that is subject to ACCM security measures.

(3) The Special Programs Office, OUSD(P), shall maintain a central repository of records for all DoD ACCM.

g. Annual Reports of ACCM Use. Not later than December 15 of each year, the DoD Components shall provide a report to OUSD(P) on all ACCM usage during the previous year. The exact format for this report shall be provided annually by OUSD(P), however, the general data elements include: ACCM nickname; purpose and/or description of the ACCM program; expected duration; and ACCM sponsor and ACCM control officer(s).

h. Sharing ACCM-Protected Information. ACCM-protected information may be shared with

other DoD Components and/or other Federal government departments and agencies only when the recipient organization agrees to abide by the ACCM security requirements stipulated in this enclosure.

i. Contractor Access to ACCM. DoD contractors may participate in ACCMs, or be directed to participate, only when such access and the associated security plan are identified in the DD Form 254, "Contract Security Classification Specification." Care must be taken to ensure identification of the security plan does not disclose ACCM-protected data.

j. Program Maintenance

(1) ACCM sponsors shall maintain an updated listing of primary and alternate ACCM control officers for each organization to which they have extended their program.

(2) Each organization's ACCM control officer shall maintain an updated ACCM access control list for their organization.

(3) Initial contact between organizations will be between each organization's ACCM control officers. ACCM control officers may authorize action officer to action officer contact once access control lists have been exchanged between organizations.

(4) Personnel requiring access to ACCM-protected information shall receive specialized training upon initial access to the program and annually thereafter. Training, as a minimum, shall address the procedures for access, control, transmission, storage, and marking. Individuals may be required to sign an acknowledgement of training should the security plan so specify.

(5) ACCM documentation (i.e., program security plan and security classification guide) must be updated a minimum of once every 5 years.

(6) ACCM sponsors shall provide the following information, through the DoD Component Head, to OUSD(P) concurrently with the ACCM annual report:

(a) A listing of primary and alternate ACCM control officers for each organization managing an ACCM.

(b) Any updated ACCM documentation or confirmation that program documentation has been reviewed and is current.

k. Safeguarding ACCM Information. The provisions of this Manual regarding the safeguarding of classified information are modified with respect to use of ACCM as follows:

(1) Top Secret, Secret, and Confidential cover sheets (i.e., SFs 703, 704, and 705, respectively) used to cover ACCM material shall be over stamped or marked with "ACCM" and the appropriate nickname. Cover sheets specifically designated by the DoD Components for use with ACCM must be approved by the Director of Security, OUSD(I), prior to use.

(2) ACCM material should be 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. Separate GSA approved storage containers are not required so long as everyone with access to container is also approved for access to the ACCM material stored within, but the measures used (e.g., segregated files, separate folders, drawers labeled for ACCM) shall prevent the commingling of ACCM material with other classified documents.

(3) ACCM information shall be transmitted in the same manner as other classified information at the same classification level with the following exceptions:

(a) ACCM information packaged for transmission shall have the inner envelope marked with the appropriate classification, the caveat "ACCM," and the assigned nickname, and shall be addressed to the attention of an individual authorized access to the ACCM information.

(b) The ACCM nickname shall be used in the text of message traffic and on cover sheets accompanying secure facsimile transmissions to assist in alerting the recipient that the transmission involves ACCM-protected information. Senders shall ensure that an authorized recipient is awaiting the transmission when sending via secure facsimile. When using the Defense Message System (DMS), the material must also be marked as "SPECAT" (Special Category) in accordance with the requirements and procedures in CJCSM 5720.01B (Reference (ag)). Due to limits in DMS processing, only one ACCM nickname should be used in a DMS message.

(c) Automated information systems or electronic files containing ACCM protected information shall be configured with appropriate discretionary access controls to ensure that access is restricted to individuals with authorized access.

(d) Secret Internet Protocol Router Network (SIPRNET) or other secure transmission methods authorized for processing information at the required level of classification may be used to transmit ACCM information. Each such transmission must be marked with the caveat "ACCM" and the authorized nickname in accordance with the marking guidance in Volume 2 and transmitted only to those authorized access to the ACCM information.

(e) The method of transmission selected for ACCM information, whether in hardcopy or electronic form, shall be consistent with the security classification assigned. Designation of information as requiring ACCM protection does not, in and of itself, require the transmission of the information by methods usually reserved for a higher level of classified information.

1. Security Incidents. Compromise of ACCM program information can present an immediate and real threat to national security and those personnel involved in mission execution. Anyone finding ACCM material out of proper control shall take actions to safeguard the material and shall immediately notify the local ACCM control officer, if known, or the local security manager.

(1) All reporting, inquiry, investigation, and damage assessment will be conducted per

the guidelines contained in Enclosure 6 of this Volume. Any reports containing ACCM information shall be handled in accordance with the requirements of this Manual as modified by this section.

(2) Section 13 of Enclosure 6 of this Volume states the actions to take if unauthorized personnel are inadvertently afforded access to ACCM information. Inadvertent disclosure forms, commonly used with compartmented information, are not authorized for use with ACCM information.

(3) Because ACCM program information is not SCI or SAP, reasonable risk management procedures should be followed when ACCM program information is incorrectly placed on non-approved electronic processing systems or electronically transmitted to non-authorized personnel and/or systems. Deleting the file or material from all affected systems is normally a sufficient action unless the material in question is classified at a higher level of classification than that for which the system is accredited.

(4) The ACCM sponsor should be notified when the local inquiry and investigation is completed. Resolution will be in accordance with current guidance contained in Enclosure 6 of this Volume and must consider the guidance contained in the ACCM program security plan. Responsibility for the damage assessment remains with the ACCM sponsor. Any additional action will be as directed by the ACCM sponsor and the local security manager.

m. ACCM Termination. ACCM shall be terminated by the establishing DoD Component when ACCM security measures are no longer required. Notification of ACCM termination must be submitted, in writing, as required by paragraphs 18.c.(1) and 18.c.(2) of this enclosure.

n. Transitioning an ACCM to a SAP. If, at any point in time, the DoD Component Head determines that information protected by ACCM requires further protection as a SAP, authorization to establish a DoD SAP must be requested in accordance with DoD Directive 5205.07 (Reference (ah)).