DEFENSE SECURITY COOPERATION AGENCY
2800 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-2800

13 MAY 2026

MEMORANDUM FOR DEPUTY UNDER SECRETARY OF THE AIR FORCE FOR INTERNATIONAL AFFAIRS
DEPUTY ASSISTANT SECRETARY OF THE ARMY FOR DEFENSE EXPORTS AND COOPERATION
DEPUTY ASSISTANT SECRETARY OF THE NAVY FOR INTERNATIONAL PROGRAMS
DIRECTOR, DEFENSE CONTRACT MANAGEMENT AGENCY
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, DEFENSE LOGISTICS AGENCY
DIRECTOR, DEFENSE THREAT REDUCTION AGENCY
DIRECTOR, MISSILE DEFENSE AGENCY
DIRECTOR, NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY
DIRECTOR, SECURITY COOPERATION ACCOUNTING DIRECTORATE, DEFENSE FINANCE AND ACCOUNTING SERVICE, INDIANAPOLIS OPERATIONS
DIRECTOR OF CYBERSECURITY DIRECTORATE AND DEPUTY NATIONAL MANAGER FOR NATIONAL SECURITY SYSTEMS, NATIONAL SECURITY AGENCY

SUBJECT: Defense Security Cooperation Agency Policy Memorandum 26-79, Enhanced End Use Monitoring Criteria SAMM Chapter 8 Update [SAMM E-Change 849]

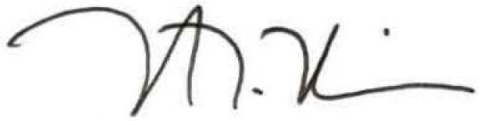
References: (a) DSCA Policy Memorandum 26-63, Authorizing Designated and Appointed U.S. Personnel to Conduct Initial U.S. Defense Article Inventories on Behalf of Security Cooperation Offices, Dated 06 NOV 2023

This memorandum updates the Security Assistance Management Manual (SAMM) Chapter 8 in support of Executive Order 14383, which requires the development of clear criteria for determining whether a defense article requires Enhanced End-Use Monitoring (EEUM).

The key changes in this update are designed to strengthen the EEUM program and include the establishment of a formalized designation process, which requires senior-level (General/Flag Officer or SES) endorsement from Military Departments and Implementing Agencies when recommending defense articles for EEUM designation. The update also defines clearer designation criteria, focusing on articles with Critical Program Information, embedded cryptography, or a high threat of diversion.

If you have questions on this memorandum, please contact DSCA (Office of International Operations, Global Execution Directorate, End Use Monitoring Division (IOPS/GEX/EUM)) at dsca.eumhelpdesk@mail.mil. Please reference the DSCA policy number and memorandum subject. For general questions about the SAMM, please contact DSCA (Office of Strategy,

Plans, and Policy, Execution Policy and Analysis Directorate (SPP/EPA)) at dsca.ncr.spp.mbx.epa@mail.mil.



Michael F. Miller
Director

Attachment: SAMM E-Change 849 - EEUM SAMM Chapter 8 Update

Attachment : Security Assistance Management Manual E-Change 849

EEUM SAMM Chapter 8 Update

1. Update SAMM Section Enhanced End Use Monitoring as follows:

C8.4. Enhanced End Use Monitoring

C8.4.1. Definition. Enhanced End Use Monitoring (EEUM) is a designation mechanism that provides greater USG oversight and more robust assessment of partner compliance with the transfer conditions of Letters of Offer and Acceptance (LOAs) and other government-to-government transfer agreements. Defense articles are designated EEUM based on criteria established in Section C8.4.3. EEUM-designated defense articles require enhanced accountability, which include physical security assessments of partner storage sites and inventories conducted by serial number. EEUM-designated defense articles transferred through the FMS process (see Section C4.3.5.2.) must be sold on defined order lines using an EEUM-coded Military Articles and Services List (MASL) designator and include physical security and accountability notes. The defense articles listed in Table C8.T4. below have been designated for EEUM for all Foreign Military Sales (FMS)-eligible countries. Other defense articles may require Case Unique EEUM and/or additional U.S. control measures (e.g. U.S. custody and/or electronic monitoring) which are determined on a case-by-case basis in the transfer approval process. Contact DSCA (Office of International Operations, Global Execution Directorate, End Use Monitoring Division (IOPS/GEX/EUM)) at dsca.ncr.bpc.mbx.eum-helpdesk@mail.mil for a list of such Case Unique EEUM-designated articles.

Table C8.T4. Defense Articles Designated for Enhanced End Use Monitoring for all Foreign Military Sales-eligible Countries

"Table C8.T4. Defense Articles Designated for Enhanced End Use Monitoring for all Foreign Military Sales-eligible Countries" is located in the Common Access Card (CAC)-Enabled SAMM site, which is located at: https://dod365.sharepoint-mil.us/sites/OSDDSCA-CUI-SAMM.

For information on EUM content in the CAC-Enabled SAMM, contact: DSCA ((IOPS/GEX/EUM)) at dsca.ncr.bpc.mbx.eum-helpdesk@mail.mil. DoW CAC Holders: please contact DSCA Office of Strategy, Plans, and Policy, Execution Policy and Analysis Directorate (SPP/EPA) at dsca.ncr.spp.mbx.epa@mail.mil with any questions regarding access to the site.

C8.4.2. Defense Articles Designated for Case Unique Enhanced End Use Monitoring. For information on defense articles that require Case Unique Enhanced End Use Monitoring, contact DSCA ((IOPS/GEX/EUM)) at dsca.ncr.bpc.mbx.eum-helpdesk@mail.mil.

C8.4.3. Enhanced End Use Monitoring Designation Process. Performing EEUM activities requires commitment of USG and partner resources; therefore, DSCA provides oversight and administration of U.S. provided defense articles designated for EEUM. MILDEP/IAs recommending a defense article to be designated for EEUM must submit a request to DSCA signed at the General Officer, Flag Officer or Senior Executive Service (SES)-level.

C8.4.4. Criteria for Recommending Enhanced End Use Monitoring Designation. DSCA and State PM shall review and approve a MILDEP/IA, Interagency, or Congressional recommendation to designate a defense article for EEUM. A MILDEP/IA recommendation may be justified due to a MILDEP/IA's need for: (1) EEUM to serve a prerequisite requirement for the MILDEP/IA's conditional transfer approval during the release review process; (2) DoW personnel to periodically verify a partner's compliance with specific physical security requirements applicable to the transferred defense article; and/or (3) DoW personnel to accomplish an annual serial number inventory as the only reasonably available and necessary measure to mitigate the risk of an unauthorized transfer causing exceptionally grave or serious damage to U.S. national security interests. When assessing the potential adverse consequences to U.S. national security interests due to an unauthorized disclosure or transfer of a defense article, the MILDEP/IA must consider the following criteria:

1. Critical Program Information: The potential degradation or loss of a U.S. critical military technical or intelligence advantage over adversaries due to the unauthorized disclosure of the transferred defense article's critical program information.

2. Embedded Cryptography: The degradation or compromise of the U.S. military's ability to conduct secure communications due to the unauthorized transfer of a defense article's embedded cryptography.

3. Diversion Threat: The increased threat of hostile acts against U.S. forces, partner forces, or noncombatants due to the unauthorized transfer of a highly portable and concealable defense article which is susceptible for use by entities seeking to commit acts of sabotage, insurrection, or terrorism (e.g. MANPADS).

C8.4.4.1. Sources for Enhanced End Use Monitoring Recommendations. The following sources may potentially condition their transfer approval upon an EEUM designation:

C8.4.4.1.1. Military Department / Implementing Agency Releasability Determination. The MILDEP/IA releasability determination requires EEUM designation to mitigate concerns.

C8.4.4.1.2. Interagency Releasability Determination. An interagency releasability determination (e.g., for the transfer of classified information or sensitive technology) requires EEUM designation to mitigate concerns.

C8.4.4.1.3. Congressional Requirement. EEUM designation is accomplished to resolve U.S. Congressional concerns regarding a proposed transfer.

C8.4.5. Flow Chart of Enhanced End Use Monitoring Designation. Figure C8.F1. depicts the process for defense articles to be designated for EEUM. Figure C8.F2. depicts the execution work flow for defense articles designated as required for EEUM.

Figure C8.F1. Designating Defense Articles for Enhanced End Use Monitoring

See Change #2 for revised figure.

Figure C8.F2. Process Flow of Defense Articles Designation for Enhanced End Use Monitoring

See Change #3 for revised figure.

C8.4.5.1. Controlled Cryptographic Items. All Controlled Cryptographic Items (CCI) are designated for EEUM and are documented in CCI management systems other than SCIP. Transferred CCI are changed from EEUM to Routine EUM in SCIP (unless it is EEUM for additional reasons) but retain the EEUM and documentation requirements, as follows:

C8.4.5.1.1. The assessments and reporting of EEUM for CCI purchased by Partners or Allies and retained by USG or industry for testing, integration, etc., are performed by the USG or industry's respective CCI safeguarding, accountability, and reporting procedures.

C8.4.5.1.2. The assessments and reporting of EEUM for CCI transferred to the North Atlantic Treaty Organization (NATO), NATO member nations, Australia, and New Zealand are performed by the respective partner in accordance with their CCI policies and regulations.

C8.4.5.1.3. The assessments and reporting of EEUM for CCI transferred to international organizations other than NATO and non-NATO member nations except Australia and New Zealand who have signed a Communications Interoperability and Security Memorandum of Agreement (CISMOA) or like agreement is accomplished by the FMS-funded U.S. CCI custodians.

C8.4.5.1.4. The assessments and reporting of EEUM of CCI transferred to non-NATO member nations who have not signed a CISMOA or like agreement is accomplished by the SCOs and reported to their respective theater CCMD Theater CCI Account. CCMDs must ensure SCOs perform the required CCI physical security and accountability assessments.

C8.4.5.1.5. Network Enabled Weapons (NEW) with NSA Type 1 CCI encrypted datalink require CCI EUM in accordance with Section C8.4.1.4. and may require additional monitoring requirements. See Table C8.T4. or contact DSCA (IOPS/GEX/EUM) at dsca.ncr.bpc.mbx.eum-helpdesk@mail.mil for more information on Case Unique EEUM requirements.

C8.4.5.2. Recommending Redesignation of Enhanced End Use Monitoring to Routine End Use Monitoring. Figure C8.F3. depicts the process to re-designate an EEUM-designated defense article to Routine End Use Monitoring (REUM). When a decision is made to re-designate a defense article from EEUM to REUM, DSCA will publish a Policy Memo to indicate the change to remove an EEUM-designated defense article from Table C8.T4. and the respective EEUM Note(s) in Appendix 6. The Policy Memo will direct the MILDEP/IA on the process to remove applicable EEUM language from FMS cases that are closed or in implemented status.

Figure C8.F3. Process Flow for Redesignation of Enhanced End Use Monitoring-designated Defense Articles to Routine End Use Monitoring

See Change #4 for revised figure.

C8.4.5.3. Determining the Military Articles and Services List End Use Monitoring Code. DSCA (IOPS/GEX/EUM), will coordinate with DSCA (Office of Business Operations (OBO)) and the respective MILDEP/IA to determine the defense article's MASL EUM code. The MASL EUM code of a defense article designated as Enhanced for all FMS exports will be coded as "E". The MASL EUM code of a defense article designated for Routine EUM will be coded as "R". If it is determined in the transfer approval process that a defense article that is normally identified as Routine is required to be treated as Enhanced for a specific sale, the MILDEP/IA will request DSCA to use a Case Unique MASL coded "E" for use of the sale.

C8.4.5.4. Developing Letter of Offer and Acceptance Physical Security and Accountability Enhanced End Use Monitoring Note. MILDEP/IAs are responsible for providing DSCA subject matter expert support in drafting security, accountability, and USG control measures included on the LOA to ensure that the parameters levied in the EEUM-designation are met for all EEUM defense articles. This includes the development of physical security and accountability EEUM notes to be incorporated in an LOA or other transfer agreement. The MILDEP/IAs shall provide any desired updates to EEUM notes to DSCA (IOPS/GEX/EUM) for coordination and approval. DSCA (IOPS/GEX/EUM) will coordinate with the other relevant MILDEP/IAs (Headquarters and Program Offices), DSCA (Office of Strategy, Plans, and Policy (SPP)), DSCA (Office of International Operations, Weapons Directorate (IOPS/WPN)), DSCA (Office of International Operations, Global Execution Directorate, Case Writing and Development Division (IOPS/GEX/CWD), and DSCA (Front Office, Office of the General Counsel (FO/OGC)). EEUM Notes that are coordinated and approved by DSCA (IOPS/GEX/EUM) for a Case Unique EEUM defense article will be used each time the same Case Unique EEUM defense article is included on a different LOA.

C8.4.5.5. Incorporation of Physical Security and Accountability Enhanced End Use Monitoring Notes for Letters of Offer and Acceptance. Physical security and accountability EEUM notes will be included in the LOA by the IA responsible for these defense articles. Additional information on EEUM is available on the Common Access Card (CAC)-Enabled SAMM site, which is located at https://dod365.sharepoint-

mil.us/sites/OSDDSCA-CUI-SAMM (accessible to DoW CAC holders only). For additional information on EUM content in the CAC-Enabled SAMM, contact: DSCA (IOPS/GEX/EUM) at dsca.ncr.bpc.mbx.eum-helpdesk@mail.mil.

C8.4.5.6. Developing and Validating Enhanced End Use Monitoring Checklists. DSCA (IOPS/GEX/EUM) will coordinate with the respective MILDEP/IA, as required, to develop and publish in the SCIP EUM database the DoW Golden Sentry EEUM checklists for defense articles or technology designated for EEUM. The relevant SCO and DSCA (IOPS/GEX/EUM) will validate the DoW Golden Sentry EEUM checklists during EEUM checks and will provide the MILDEP/IA recommendations for improvement when required.

C8.4.6. Application of Additional Control Measure Requirements. Select defense articles may require additional U.S. control measures (e.g. U.S. custody, frequent testing, etc.) as a condition of the transfer approval. In these instances, all costs necessary to implement the additional USG control measures, levied as part of the transfer approval, that goes beyond EEUM assessments mentioned in this chapter, will be paid by the partner. The partner's obligation to pay for these additional control measures through either national funds or via grant security assistance funds will be stated in the LOA security and accountability note.

C8.4.7. Review of Enhanced End Use Monitoring-Designated Defense Articles. Each MILDEP/IA must annually assess the applicability of continued EEUM for its respective defense articles in Table C8.T4. and Case Unique EEUM (for Case Unique EEUM requirements, contact DSCA (IOPS/GEX/EUM) at dsca.ncr.bpc.mbx.eum-helpdesk@mail.mil for more information). The MILDEP/IA must notify DSCA IOPS/GEX/EUM upon completion of its assessment.

C8.4.8. Site Surveys/Certification of Storage Sites. With the exception of NVDs, CCI, or DSCA designated hostile environments (See Section C8.5.5.), MILDEP/IAs are responsible for conducting physical security assessments to certify partner storage sites. EEUM-designated defense articles may not be transferred to an uncertified site. MILDEP/IA will certify partner defense article storage sites to standards specified in accordance with Department of Defense Manual (DoDM) 5100.76 "Physical Security of Sensitive Conventional Arms, Ammunition and Explosives," or by other appropriate authorities for EEUM articles not listed in DoDM 5100.76. Discrepancies identified during the physical security storage site assessments shall be corrected or compensatory measures implemented prior to the transfer of any EEUM-designated defense articles.

C8.4.8.1. Security Managers and Storage Site Certification Reports. The MILDEP/IA will ensure DSCA has a current list, by defense article, of all security inspectors/managers responsible for conducting physical security assessments and certifications. The MILDEP/IA will provide DSCA a copy of all site certification reports within 30 calendar days of conducting the site certification by ensuring the reports are uploaded to the site certification repository within the SCIP-EUM database.

C8.4.8.2. Storage Site Certification Costs. Table C9.T2A. (lines L16 and CE43) addresses the proper source of funding to pay for partner site certifications. Certification and re-certification of partner storage sites storing EEUM-designated defense articles shall be case-

funded. FMS admin funds may be used to certify partner storage sites prior to LOA implementation; however, these costs must be reimbursed on the subsequent LOA. If an LOA is never implemented, the IA Pre-Letter of Request (LOR) funds remain the proper funding source.

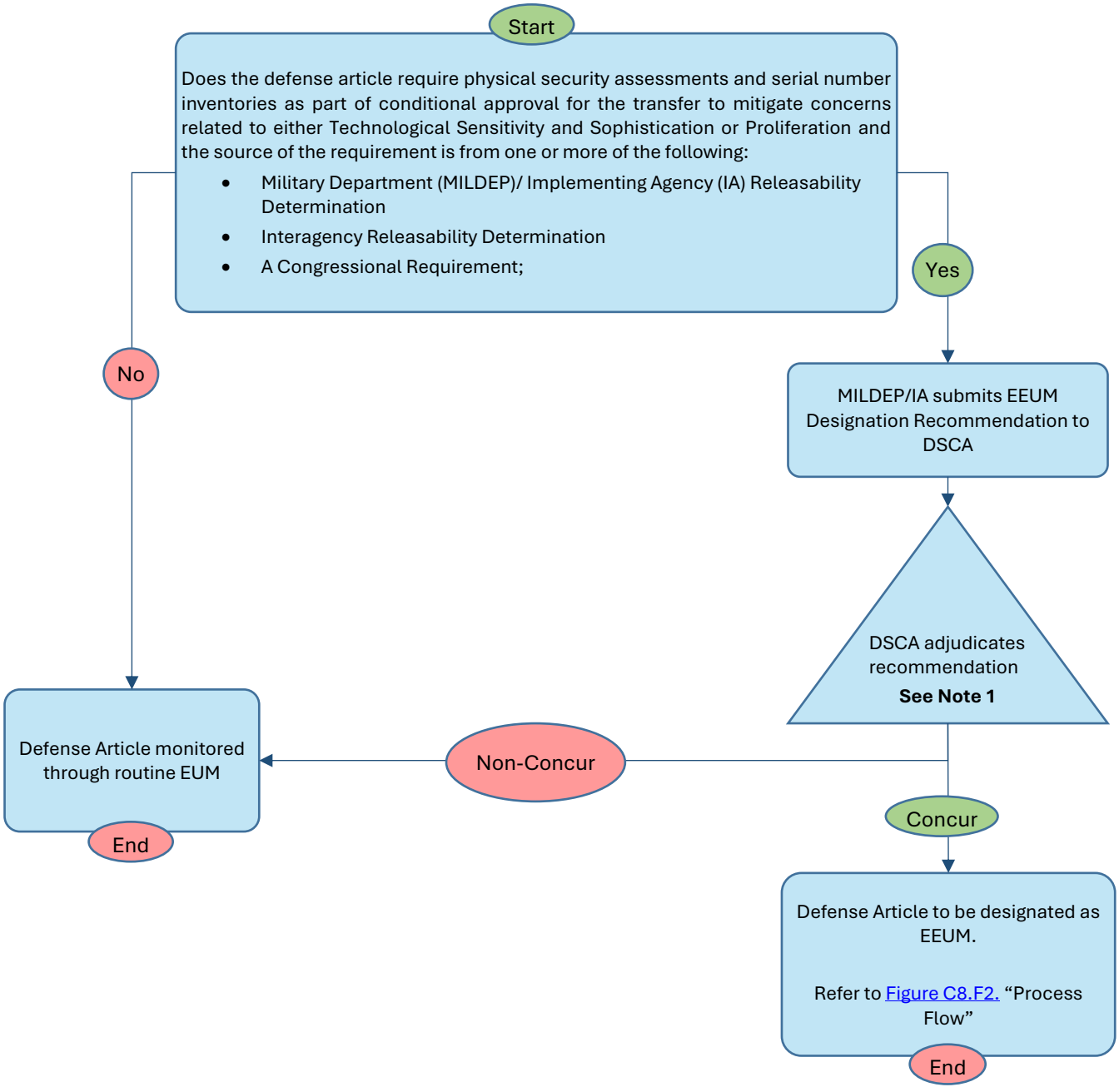
C8.4.8.3. Storage Site Certification Reciprocity. Partner storage site certifications shall be conducted consistently with the appropriate Security Risk Category (SRC) of the defense article to be stored. Including specified storage site compensatory measures, storage site certifications by one MILDEP/IA in one SRC are reciprocally accepted for storage of defense articles offered by another MILDEP/IA in the same SRC. MILDEP/IA security inspectors/managers will coordinate storage site assessment visits with DSCA, SCOs, and other MILDEP/IAs in advance to mitigate duplication when another MILDEP/IA has already certified the same storage site for the associated SRC. The storage site certification repository within the SCIP-EUM database informs whether another MILDEP/IA has previously certified a proposed storage site location. DSCA will work with the MILDEP/IA to ensure standardized physical security assessment/certification checklists are developed.

C8.4.8.4. Storage Site Compensatory Measures. All MILDEP/IA storage site certifications shall be conducted consistently with the appropriate SRC or terms within transfer agreement of the defense articles. The MILDEP/IA must document any areas where partner storage sites do not meet the physical security requirements stated in DoDM 5100.76, by other appropriate authorities, or transfer agreements such as the LOA. Risk management principles may be utilized to identify whether any acceptable compensatory measures are required. SCOs shall verify that compensatory measures remain in place during annual inspections as documented by the MILDEP/IA.

C8.4.9. Storage Site Changes. Changes to previously certified storage sites resulting in non-compliance to physical security requirements will need to be recertified. See Section C8.4.5.2. for guidance on Storage Site Certifications costs.

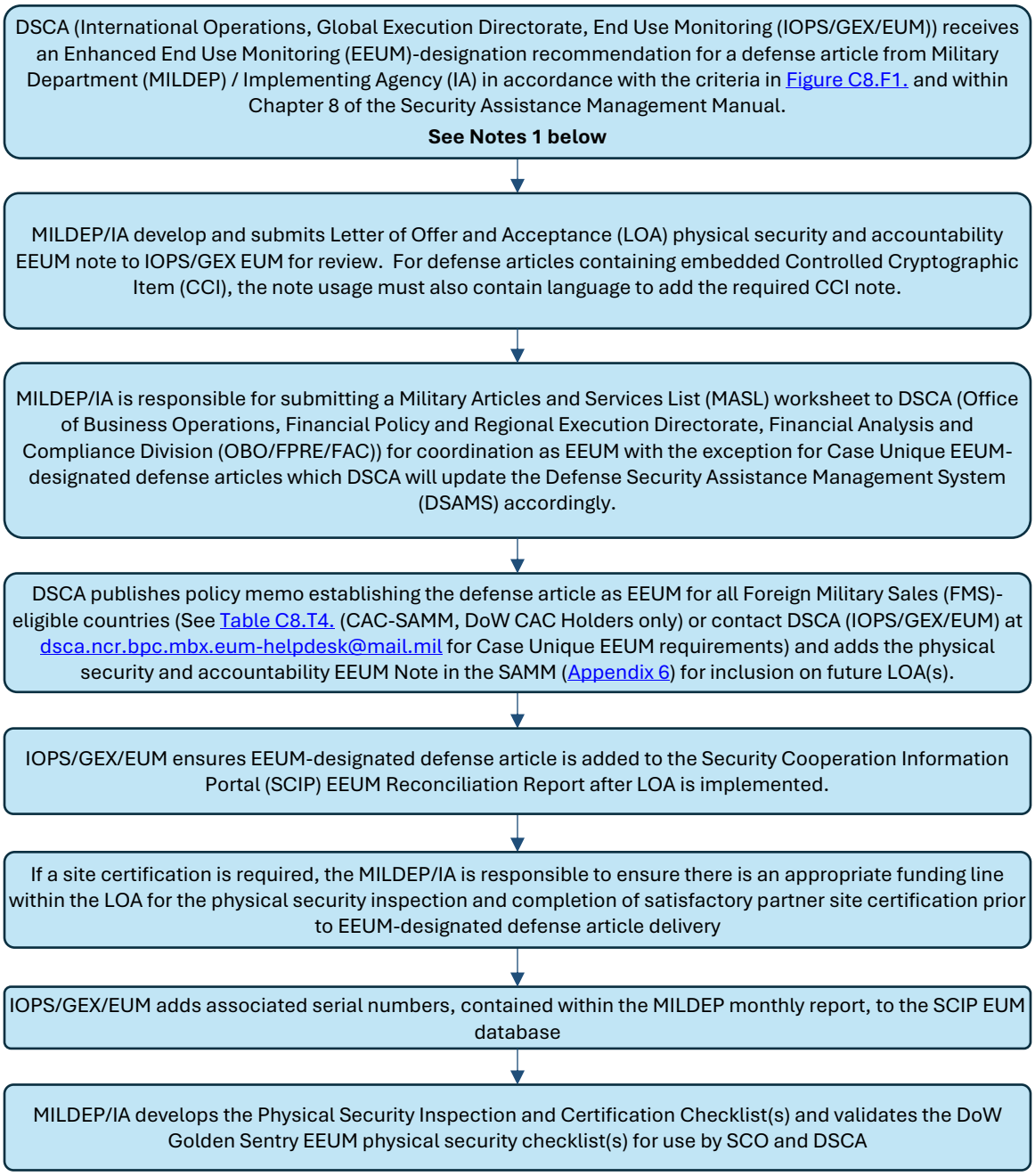
2) Update C8.F1. Designating Defense Articles for Enhanced End Use Monitoring as follows:

Criteria for Enhanced End Use Monitoring (EEUM) Designation



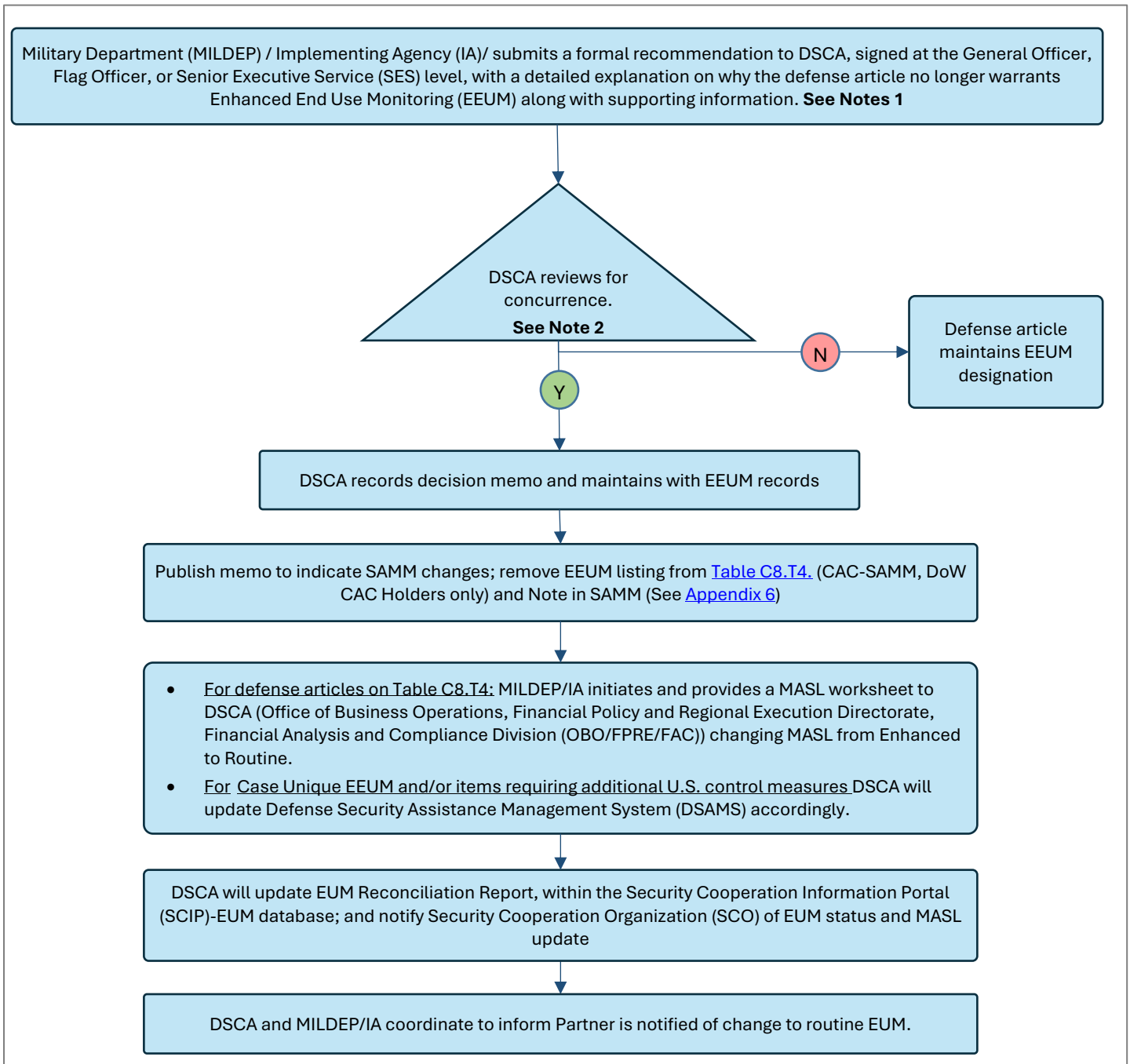
Note 1: Staffing actions are led by DSCA (Office of International Operations, Global Execution Directorate, End Use Monitoring Division (IOPS/GEX/EUM)). DSCA staffing will also include DSCA (Office of International Operations, Weapons Directorate (IOPS/WPN)), DSCA (Office of Strategy, Plans, and Policy (SPP)), DSCA (Front Office, Office of the General Counsel (FO/OGC)), and the appropriate MILDEP.

3) Update Figure C8.F2. Process Flow of Defense Articles Designation for Enhanced End Use Monitoring as follows:



Note 1: Staffing actions are led by DSCA (Office of International Operations, Global Execution Directorate, End Use Monitoring Division (IOPS/GEX/EUM)). DSCA staffing will also include DSCA (Office of International Operations, Weapons Directorate (IOPS/WPN)), DSCA (Office of Strategy, Plans, and Policy (SPP)), DSCA (Front Office, Office of the General Counsel (FO/OGC)), and the appropriate MILDEP.

4) Update Figure C8.F3. Process Flow for Redesignation of Enhanced End Use Monitoring - designated Defense Articles to Routine End Use Monitoring as follows:



Note 1: MILDEP/IAs are responsible for monitoring and reviewing for currency certain interagency release decisions designating defense articles for EEUM. And for providing recommendations for changes to physical security requirements to DSCA; changes to interagency decisions should be included as part of the supporting information.

Note 2: Staffing actions are led by DSCA (Office of International Operations, Global Execution Directorate, End Use Monitoring Division (IOPS/GEX/EUM)). DSCA staffing will also include DSCA (Office of International Operations, Weapons Directorate (IOPS/WPN)), DSCA (Office of Strategy, Plans, and Policy (SPP)), DSCA (Front Office, Office of the General Counsel (FO/OGC)), the appropriate MILDEP, and the Defense Technology Security Administration (DTSA) as appropriate.