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

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 FOR SECURITY ASSISTANCE, DEFENSE FINANCE AND ACCOUNTING SERVICE – INDIANAPOLIS OPERATIONS
DIRECTOR OF CYBERSECURITY DIRECTORATE AND DEPUTY NATIONAL MANAGER FOR NATIONAL SECURITY SYSTEMS, NATIONAL SECURITY AGENCY

SUBJECT: Conducting End Use Monitoring in a Hostile Environment, DSCA Policy 22-87 [SAMM E-Change 609]

REFERENCES:

a) Security Assistance Management Manual (SAMM), Chapter 8, "End Use Monitoring"

Effective immediately, this memorandum incorporates guidance into Chapter 8 of the Security Assistance Management Manual (SAMM) to establish policy and procedures for conducting End Use Monitoring (EUM) in a hostile environment.

The DoD EUM Golden Sentry program is designed to verify Partner Nation (PN) compliance with Section 40A of the Arms Export Control Act, as amended (22 U.S.C. 2785), and Section 505 of the Foreign Assistance Act, as amended (22 U.S.C. 2314). The current EUM policy is designed to be executed in a peacetime environment where U.S. government officials conduct periodic site visits to verify accountability and ensure storage facilities meet physical security requirements. However, a combat/hostile environment significantly impedes the ability of U.S. government officials to conduct site visits where the potential for serious injury or death exists during execution of EUM activities. As a result, DSCA may request that the PN carry out the basic tenets of the DoD EUM Golden Sentry Program to provide reasonable assurance that U.S. defense articles are being stored, secured, and used in accordance with the terms and

conditions of the relevant Letters of Offer and Acceptance (LOA) and equipment transfer agreements. DoD is evaluating additional methods for PN EUM assurances, which will be specifically addressed in future LOA and SAMM changes.

If you have questions regarding this change, please contact Mr. John Oswald, DSCA/IOPS/GEX, at (703) 697-9427 or e-mail: John.A.Oswald2.civ@mail.mil. For general questions concerning the SAMM, please contact Ms. Melissa Dockstader, at (703) 692-6657 or e-mail: Melissa.M.Dockstader.civ@mail.mil. The SAMM is available at https://samm.dsca.mil/.

James A. Hursch
Director

Attachment:
SAMM E-Change 609

Security Assistance Management Manual (SAMM), E-Change 609

Conducting End Use Monitoring (EUM) in a Hostile Environment

1. Add New SAMM Section C8.5.5. – Conducting End Use Monitoring (EUM) in a Hostile Environment:

C8.5.5. Conducting EUM in a Hostile Environment. The following policy sets procedures for the conduct of EUM when force protection limitations exist that could endanger USG personnel performing Routine EUM observations, EEUM inventories, and physical security inspections of Partner Nations' (PN) storage facilities. This process applies to reporting potential violations and the accountability of Enhanced EUM (EEUM) defense articles identified in SAMM Table C8.T4. or other defense articles that require EEUM and / or additional U.S. required control measures as determined in the transfer approval process. To mitigate proliferation and to comply with the requirement in Section 40A of the Arms Export Control Act (22 U.S.C. 2785) that the EUM program provide 'reasonable assurance' that the PN is complying with U.S. End Use requirements, the following procedures are to be implemented.

C8.5.5.1. Accountability of U.S. defense articles deployed to restricted areas that cannot be inventoried due to heightened security risk. When conditions allow, the SCO shall conduct an initial 100% inventory, by serial number, of all EEUM designated articles prior to shipment/delivery into hostile areas. The SCO shall also assist locally employed staff and the PN to improve inventory management and accountability procedures of EEUM designated articles currently in restricted areas.

C8.5.5.2. Partner Nation Self-Reporting. Under certain circumstances, when USG led assessments are not possible, PN '*Self-Reporting*' can be accomplished by providing the SCO with records of inventories, other accountability records, or the use of barcode scanning. PN self-reporting is authorized only when the following criteria are met:

- The CCMD issues a memorandum to the SCO and DSCA, endorsed at the SES/07 General Officer/Flag Officer level, outlining the increased security risk situation, restricted areas, and the necessity to modify standard peacetime accountability and physical security inspection processes outlined in SAMM Table C8.T2.
- The PN shall provide the SCO with a signed Control Plan for each EEUM designated defense article that the USG has transferred to the PN under grant authorities (e.g., title 10 BPC, Presidential Drawdowns, Third Party Transfers). Signed Control Plans of EEUM designated articles are required to establish EUM requirements for item transfers outside of Letter of Offer and Agreements (LOA) EUM assurances. A template is located in the SCIP-EUM database under Support-Policy/Procedures Memos.
- The PN agrees to produce and to sign an EEUM self-reporting Concept of Operations (CONOPS) describing self-reporting procedures with conducting end use monitoring in the absence of USG led observation and assessment.

C8.5.5.3. Acceptable PN Documentation. SCOs shall update, and keep current, the disposition status of U.S. provided EEUM defense articles within the SCIP-EUM database based on PN provided accountability documentation. The disposition status "Observed by Partner Nation" shall be used for defense articles still in PN possession. All documentation shall include the defense article description,

serial numbers, date of observation, and current disposition status (e.g., active, expended, destroyed, or lost). Acceptable PN documentation can be:

- Electronic accountability via barcode scanning technology.
- PN on hand accountability / inventory reports.
- PN loss, damage, and expenditure reports.
- PN hand receipts of deployed USG-provided defense articles.

C8.5.5.4. For sensitive self-reporting data at a classified level, due to OPSEC concerns, the SCOs shall obtain, scan/upload, and forward sensitive PN-provided data to dsca.ncr.iops-gex-amd.mbx.eum@mail.smil.mil.

C8.5.5.5. Frequency of Self-Reporting. Frequency is dependent on the PN's inventory and accountability requirements in accordance with the LOA, the EEUM Control Plan, and the PN self-reporting CONOPs; and subject to USG discretion.

2. Update the SAMM as Follows:

Update	**Current Wording**	**Revised Wording**
Table C8.T2. DoD End-Use Monitoring Responsibilities DSCA (Office of International Operations, Global Execution Directorate, Assistance & Monitoring Division (IOPS/GEX/AMD))	[New]	Establish policy and procedures for conducting EEUM in a hostile environment to ensure signed control plans and CONOPS are in place, and assist the SCO with other responsibilities identified in Section C8.5.5., "Conducting EUM in a Hostile Environment."
Table C8.T2. DoD End-Use Monitoring Responsibilities MILDEPs and Implementing Agencies (IAs)	[New, add after bullet, *"Provide a monthly delivery record with serial numbers of EEUM items to DSCA (dsca.eumhelpdesk@mail.mil) in advanced of shipment of EEUM-designated items for input into the SCIP-EUM database."]*	Provide delivery records with serial numbers of EEUM items that are being transferred to hostile environments (Section C8.5.5.) in advance of shipment to the dsca.eumhelpdesk@mail.mil.
Table C8.T2. DoD End-Use Monitoring Responsibilities MILDEPs and Implementing Agencies (IAs)	Conduct physical security inspections and certifications of partner nations' facilities storing weapons and defense systems designated for EEUM and enhanced case-unique weapons systems and ensuring the reports are uploaded to the site	With the exception of hostile environments (Section C8.5.5.), conduct physical security inspections and certifications of partner nations' facilities storing weapons and defense systems designated for EEUM and enhanced case unique weapons systems and ensuring the

Update	Current Wording	Revised Wording
	certification repository within the SCIP-EUM database.	reports are uploaded to the site certification repository within the SCIP-EUM database.
Table C8.T2. DoD End-Use Monitoring Responsibilities Combatant Commands (CCMD)	[New]	Support DSCA and ensure the SCO is meeting requirements identified in Section C8.5.5., "Conducting EUM in a Hostile Environment," and issue the memorandum required under Section C8.5.5.2.
Table C8.T2. DoD End-Use Monitoring Responsibilities Security Cooperation Organizations (SCOs) (including Defense Attaché Offices and U.S. Diplomatic Missions with Security Assistance responsibilities)	[New]	Ensure procedures for conducting EUM in a hostile environment, identified in Section C8.5.5. are being followed and kept current. This includes working with the CCMD to obtain a CCMD endorsement memorandum, drafting any required EEUM Control Plans, working with the PN in receiving a signed Concept of Operations (CONOPS), and ensuring the latest PN supporting documentation and disposition status is current within the SCIP-EUM database.
C8.4.3. Site Surveys/Certification of Storage Facilities.	With the exception of Night Vision Devices and Communications Security (COMSEC) equipment, Implementing Agencies / Military Departments (IAs / MILDEPs) are responsible for conducting physical security inspections for certifications of partner nations' storage facilities before EEUM designated weapons systems and enhanced case-unique weapons systems are delivered or moved to a new or uncertified facility.	With the exception of Night Vision Devices, Communications Security (COMSEC) equipment, and hostile environments (Section C8.5.5.), Implementing Agencies / Military Departments (IAs / MILDEPs) are responsible for conducting physical security inspections for certifications of partner nations' storage facilities before EEUM designated weapons systems and enhanced case unique weapons systems are delivered or moved to a new or uncertified facility.
C8.6.2. Reporting End-Use Violations	SCOs must report all potential unauthorized end-use, including unauthorized access, unauthorized transfers, security violations or known equipment losses to the CCMD, ~~DSCA (Directorate for Security~~	SCOs shall report all potential unauthorized end use, including unauthorized access, unauthorized transfers, security violations or known equipment losses to the CCMD, DSCA (IOPS/REX/AMD), and DoS (PM/RSAT). SCOs shall

Update	Current Wording	Revised Wording
	~~Assistance (DSA)) and DoS (PM/RSAT). It is particularly important that SCOs are alert to, and report on, any indication that U.S. origin defense articles are being used against anything other than a legitimate military target, are otherwise being used for unauthorized purposes, are being tampered with or reverse engineered, or are accessible by persons who are not officers, employees, or agents of the recipient government. Potential violations can be notified via email or message.~~ SCOs must assess the sensitivity of the potential violation and other factors to determine the means of notification. The DoS investigates and reports potential violations and determines whether the AECA Section 3 (22 U.S.C. 2753) criteria require notification to Congress.	be alert to, and report on, any indication that U.S. origin defense articles are being used for unauthorized purposes, are being tampered with or reverse engineered, or are accessible by persons who are not officers, employees, or agents of the recipient government. Potential violations shall be notified via email or message immediately. SCOs must assess the sensitivity of the potential violation and other factors to determine the means of notification. The DoS investigates and reports potential violations and determines whether the AECA Section 3 (22 U.S.C. 2753) criteria requiring notification to Congress has been met.