



DEFENSE SECURITY COOPERATION AGENCY

2800 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-2800


02 JUL 2019

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 FOR SECURITY ASSISTANCE, DEFENSE FINANCE
AND ACCOUNTING SERVICE-INDIANAPOLIS OPERATIONS
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, DEFENSE LOGISTICS AGENCY
DIRECTOR, DEFENSE LOGISTICS INFORMATION SERVICE
DIRECTOR, DEFENSE LOGISTICS AGENCY DISPOSITION
SERVICES
DIRECTOR, DEFENSE THREAT REDUCTION AGENCY
DIRECTOR, MISSILE DEFENSE AGENCY
DIRECTOR, NATIONAL GEOSPATIAL-INTELLIGENCE
AGENCY
DEPUTY DIRECTOR FOR INFORMATION ASSURANCE,
NATIONAL SECURITY AGENCY

SUBJECT: Mandatory Enhanced End-Use Monitoring (EEUM) for Advanced Threat Infrared Countermeasure System (DSCA 19-27) [SAMM E-Change 432]

Effective immediately, this memorandum incorporates E-Change 432 into the Security Assistance Management Manual (SAMM) and adds the Advanced Threat Infrared Countermeasures (ATIRCM) system to the list of defense articles identified for Enhanced End-Use Monitoring in table C8.T4. Appendix 6 of the SAMM will include the attached physical security and accountability note for the ATIRCM System and its components.

If you have questions regarding this change, please contact Mr. George Lumpkins, DSCA/DSA/AMP, at (703) 697-9151 or e-mail: george.a.lumpkins.civ@mail.mil. For general questions relating to the SAMM, please contact Mr. Mike Slack, DSCA/SPP/SPI, at (703) 697-9058 or e-mail: michael.d.slack.civ@mail.mil. Implementing Agencies should ensure dissemination to supporting activities. The SAMM is available at www.dsca.mil/SAMM/


Charles W. Hooper
Lieutenant General, USA
Director

Attachment:
As stated.

cc:

AFRICOM

CENTCOM

EUCOM

NORTHCOM

SOUTHCOM

INDOPACOM

TRANSCOM

SOCOM

STATE/PM-RSAT

USASAC

TRADOC SATFA

USACE

NAVSUP

WSS

NETSAFA

AFSAC

AFSAT

DISCS

MARCOR IP

SCETC

USCG International Affairs (G-CI)

Security Assistance Management Manual (SAMM), E-Change 432
Advanced Threat Infrared Countermeasures System (ATIRCM)

1. Add the following line to Table C8.T4. Defense Articles Designated for EEUM for all FMS-eligible Countries

EEUM-Designated Defense Articles	Description
ATIRCM	Advanced Threat Infrared Countermeasures (ATIRCM) System

2. In Appendix 6, add the following note:

Advanced Threat Infrared Countermeasures System (ATIRCM) and/or Key ATIRCM Components

Note Usage
FMS: Yes
BPC: No
Note Input Responsibility
CWD
Note Usage
Mandatory for all FMS LOAs that include the Advanced Threat Infrared Countermeasures (ATIRCM) System, or the ATIRCM Infrared Jam Head (IRJH) or ATIRCM Multi-Band Laser (MBL) when sold separately as spares.
Mandatory for all Amendments that add ATIRCM, or the ATIRCM Infrared Jam Head (IRJH) or ATIRCM Multi-Band Laser (MBL) when sold separately as spares if not previously included on the case.
References
N/A
Note Text
<p>ADVANCED THREAT INFRARED COUNTERMEASURES (ATIRCM) SYSTEM SECURITY NOTES.</p> <p>a) The Purchaser agrees to the Advanced Threat Infrared Countermeasures (ATIRCM) system security requirements incorporated in a Purchaser/U.S. Government (USG) ATIRCM Security Plan as described in this security note and coordinated and approved by Project Manager, Aircraft Survivability Equipment (PM ASE). The Purchaser agrees to be a member of a joint security team led by PM ASE with team members from Deputy Assistant Secretary of the Army for Defense Exports and</p>

Cooperation (DASA (DE&C)) to define and document the security plan. The following ATIRCM components are designated as requiring Enhanced EUM: Infrared Jam Head (IRJH), which tracks the threat and directs the laser; energy and the Multi-Band Laser (MBL), which is the laser energy generator for the system.

- b) **Aircraft Security:** The requirement and intent of the following procedures are to prevent unauthorized access to ATIRCM equipment. While on the ground, the Purchaser will restrict physical access to ATIRCM equipment to authorized personnel. Only authorized personnel with an appropriate security clearance and a need-to-know will perform operations or maintenance functions on or near ATIRCM equipment and components. Passengers traveling on ATIRCM equipped aircraft without appropriate clearance or a need-to-know will not be granted access to ATIRCM equipment and components. Flight line security will comply with the following requirements:
1. The Purchaser will establish a permanent restricted area around the aircraft's home station parking location. The restricted area will be appropriate to prevent unauthorized access to ATIRCM equipment and components.
 2. The restricted area will be kept as small as possible to support the security of base aircraft and should be at least 250 feet (76.2 meters) from the base perimeter or property line. Access to the restricted area will be through a minimum number of entry control points as defined in the ATIRCM Security Plan.
 3. The Purchaser will provide positive entry control and surveillance of the restricted area when ATIRCM equipped aircraft are present.
 4. If the home station facility does not provide 24/7 armed flight line security, the Purchaser will provide at least one armed guard for immediate response/surveillance of the aircraft and a minimum of an external two person response element available to respond within 5 minutes to the aircraft location.
 5. If an ATIRCM aircraft lands at a location without security comparable to home station, a temporary restricted area will be established. The temporary restricted area will be put in place immediately after the aircraft is secured at its parking location. In the case of Head of State aircraft, establishment of the temporary restricted area may be delayed until after the Head of State has departed the flight line. The temporary restricted area will prevent unauthorized access to ATIRCM equipment.
- c) **Hardware Storage:** When not installed on the aircraft, ATIRCM system and sub-components (including fly away kits) shall be stored in 24/7 secure facility. The purchaser agrees to provide the U.S. Embassy's SCO access for physical security inspections of the secure facility. When ATIRCM equipped aircraft are scheduled for periodic or depot level maintenance outside of normal restricted parking sites ATIRCM B-Kit hardware will be removed and stored in a 24/7 secure facility. Affected B-Kit hardware is defined as the Infrared Jam Head (IRJH) and the Multi-Band Laser (MBL).
- d) **Accountability Records:** Purchaser will maintain strict accountability records on all classified information provided by the USG related to ATIRCM extracts and copies. These records will also include documentary evidence of any ATIRCM that are lost or destroyed. Such records shall, to the extent possible, be centralized.

- e) **System Hardware Transportation:** Ground transportation used for movement of the ATIRCM system or subcomponents that deviates from the ATIRCM Security Plan must be coordinated and approved by PM ASE.
- f) **Periodic Inventory:** The Purchaser agrees all ATIRCM B-Kit hardware systems will receive a 100% serial number inventory on an annual basis. Purchaser will use procedures to provide continuous accounting of receipt, transfer, storage, shipment, and/or destruction/demilitarization of ATIRCM systems. Inventory and accountability documentation maintained by the Purchaser shall be retained throughout the period of ownership and will be made available for review upon USG request.
- g) **System Access:** All ATIRCM B-Kit components requiring maintenance will be repaired only by the original equipment manufacturer (OEM). Only military or civilian employees of the purchaser's government or contractors specifically authorized by the Department of State under a Retransfer Approval for access to ATIRCM equipment will accomplish operational level maintenance. No one outside of the Purchaser's government, the USG or OEM will be allowed to accomplish maintenance functions unless approved in a Letter of Offer and Acceptance (LOA) or a Technical Assistance Agreement (TAA).
- h) **Discrepancy Reporting:** Unauthorized destruction, loss, theft, or unauthorized access to ATIRCM hardware, technology or software as well as any allegation, report, or evidence of unauthorized attempts to collect information on the ATIRCM system will be reported to the U.S. Embassy's Security Cooperation Organization (SCO).
 - 1. **Pre-delivery Planning:** Prior to delivery of ATIRCM, representatives from PM ASE, DASA (DE&C) and Purchasing country will meet to develop a mutually agreed ATIRCM Security Plan with provisions for a site survey. Prior to this meeting, PM ASE will coordinate to provide the Purchaser a security checklist. The checklist is used to assure the integrity of security measures in place for the ATIRCM system. Deficiencies identified during ATIRCM component storage site certification must be corrected prior to ATIRCM deliveries. The scope of the initial meeting will be to determine if the Purchaser has met the intent of the ATIRCM system security requirements described in the security note.
- i) **ATIRCM System Maintenance and Upgrade:** Select ATIRCM components will be returned to the USG or U.S. contractor, as directed by PM ASE, for maintenance and operational upgrade (return will be on a rotational basis). PM ASE regularly updates the threat library based on operational requirements and will provide the Purchaser the latest available software.
- j) **System Decommission:** At system decommission, the Purchaser shall obtain U.S. Department of State consent for disposal. PM ASE must be contacted for disposition instructions prior to any demilitarization/disposal effort.