



CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6
DISTRIBUTION: A, B, C, J

CJCSI 6510.02B
27 November 2002

CRYPTOGRAPHIC MODERNIZATION PLAN

References:

- a. CJCS Notice 6510, 3 July 2002, "Communications Security (COMSEC) Modernization Plan"
- b. CJCSI 6510.06, 15 February 2001, "Communications Security Releases to Foreign Nations"

1. Purpose. This instruction sets policy for the modernization of cryptographic equipment held by all DOD components specified in paragraph 3, reference a.
2. Cancellation. CJCSI 6510.02A, 30 November 1999, is canceled.
3. Applicability. Unless specifically exempted, all DOD components specified in paragraph 3 of reference a must comply with the actions specified in Enclosure A. Additionally, the components must comply with the actions for each item of equipment identified in reference a, Enclosure A.
4. Policy. Selected allied and US military forces require interoperable secure communications to support joint, combined, and coalition operations. Although the responsibility for acquiring, installing, and maintaining secure communications lies primarily with the Services, the command and control responsibilities of the joint military command structure dictate that the Chairman of the Joint Chiefs of Staff (supported by the Joint Staff) and the unified combatant commanders exercise continuing oversight of Service cryptographic programs. Enclosure A contains detailed cryptographic policy guidance.

5. Responsibilities. All DOD components specified in paragraph 3 of reference a must:

a. Adhere to the specific policy guidance outlined in Enclosures A and B.

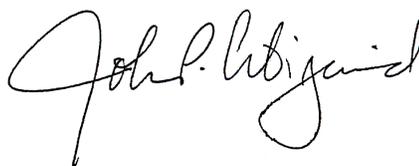
b. Initiate actions to replace and modernize cryptographic equipment in accordance with reference a, Enclosure A.

6. Summary of Changes. Enclosure A was refined to clearly define specific roles and responsibilities for the execution of cryptographic modernization. Enclosure B has been added to assist DOD components on the procedures of cryptographic modernization planning.

7. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other Federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page--<http://www.dtic.mil/doctrine>. Copies are also available through the Government Printing Office on the Joint Electronic Library CD-ROM.

8. Effective Date. This instruction is effective upon receipt.

For the Chairman of the Joint Chiefs of Staffs:



JOHN P. ABIZAID
Lieutenant General, USA
Director, Joint Staff

Enclosures:

A -- Cryptographic Modernization Responsibilities

B -- Cryptographic Modernization Planning Process

ENCLOSURE A

CRYPTOGRAPHIC MODERNIZATION RESPONSIBILITIES

1. The Military Communications-Electronics Board (MCEB) will:
 - a. Validate plans, through its Information Assurance Panel (IAP), for programmed modernization and replacement of cryptographic issues presented to it by the Joint Staff, NSA, Services, agencies, and combatant commanders through the DOD Cryptographic Modernization Working Group (CMWG).
 - b. Refer, as required, any new or modified cryptographic modernization requirements to the Joint Requirements Oversight Council for consideration.
2. Combatant Commanders will:
 - a. Identify to the affected Service, through the Joint Staff, any special and/or unique cryptographic compatibility requirements within their respective areas of responsibility pertaining to the modification and replacement of cryptographic equipment.
 - b. As appropriate, ensure actions such as submission of foreign release requests (reference b actions) are initiated in time to meet the equipment phase out dates identified in reference a, Enclosure A.
 - c. Monitor cryptographic equipment implementation, transition, and fielding to identify issues that impact compliance with reference a or interoperability in a joint or combined environment. Advise the appropriate Service(s) and the Joint Staff of the identified issues and coordinate with all relevant parties to resolve them.
 - d. The Commander, USSOCOM, under Title 10 acquisition authority, will fund for special operations forces unique cryptographic items only.
3. Services will:
 - a. Plan, program, and budget for replacement, modification or procurement of US cryptographic systems in accordance with (IAW) reference a, Enclosure A and allied interoperability requirements identified by the combatant commands.

b. Schedule cryptographic equipment replacement to continually improve and preserve joint and combined interoperability within each combatant command's AOR.

c. Replace or modify cryptographic equipment in the US DOD elements for which the Service is responsible IAW reference a, Enclosure A.

d. Monitor cryptographic equipment implementation, transition, and fielding to identify issues that impact compliance with reference a or interoperability in a joint or combined environment. Advise the Joint Staff and other Service(s) as appropriate of the issues identified and coordinate with all relevant parties to resolve them.

4. Director, NSA, will:

a. Plan, program, and budget for replacement or modification of NSA-owned cryptographic equipment IAW reference a, Enclosure A.

b. Coordinate cryptographic equipment replacement and modifications with services and agencies through the DOD CMWG IAW reference a, Enclosure A.

c. Prescribe standards, policies, and procedures governing installation, operation, use, modification, or removal of cryptographic systems used by or on behalf of the US DOD.

d. Provide instructions to US DOD elements for disposition of obsolete equipment.

e. Advise allies and civil agencies of the schedule for equipment replacement and modifications contained in reference a, Enclosure A.

f. Make available for sale or lease, via Foreign Military Sales or other US Government means, replacement, or modifications for, cryptographic equipment to ensure continued interoperability.

h. Ensure that design, engineering, and manufacture of cryptographic replacement devices are in compliance with current DOD policy regarding interoperability and are certified as interoperable in joint and coalition operations as required.

5. Defense Information Systems Agency (DISA) will:

a. Plan, program, and budget for replacement or modification of DISA cryptographic equipment IAW reference a, Enclosure A.

b. Ensure the coordinated replacement or modification of cryptographic equipment within the Defense Information Systems Network.

c. Support the identification and resolution of interoperability issues related to joint and combined applications of equipment listed in reference a, Enclosure A.

6. Command, Control, Communications, and Computer Systems Directorate, (J-6), Joint Staff will:

a. Adjudicate cryptographic issues that impact joint or combined interoperability.

b. Validate interoperability requirements and process foreign release requests for approval IAW reference b.

(INTENTIONALLY BLANK)

ENCLOSURE B

CRYPTOGRAPHIC MODERNIZATION PLANNING PROCESS

1. General

a. The NSA must certify cryptographic products for the protection of national security information. Annually, the NSA assesses the national cryptographic inventory and recommends to the MCEB the “no later than” replacement date for each cryptographic item. Reference a, Enclosure A identifies the determined replacement date.

b. Designated Approval Authorities (DAAs) can petition to the MCEB for continued employment of a cryptographic item beyond its MCEB-validated replacement date for a specific application. Each petition will be processed on a case-by-case basis and must be assessed by the NSA before review/validation by the MCEB.

2. Cryptographic Modernization Planning Process. A block diagram of the COMSEC modernization planning process is detailed in Figure B-1. Each numbered step is discussed in detail in the following paragraphs:

a. Step One -- The NSA identifies individual COMSEC replacement date(s). Annually, the NSA will identify COMSEC items requiring replacement and specify initial replacement dates IAW reference a. Replacement dates will be based upon NSA threat evaluations, available threat documentation, and established high-grade cryptography certification standards. Recommended changes to reference a will be provided with sufficient lead-time to ensure replacement cryptographic devices can be implemented across a reasonable programmatic timeline.

b. Step Two -- Coordination with the CMWG. NSA coordinates the product replacement dates with the Services, agencies, and combatant commanders through the DOD Cryptographic Modernization Working Group (CMWG). The CMWG provides staff-recommended dates to the IAP for review and direction.

c. Step Three -- IAP reviews and recommends. The IAP reviews product replacement dates and provides recommendations to the MCEB. Each recommendation will be made sufficiently in advance to facilitate the Service’s inclusion in future years defense program submissions.

- d. Step Four -- MCEB validates replacement date. The MCEB validates the dates that obsolete cryptographic items must be removed from the inventory.
- e. Step Five -- Date published in CJCSN 6510.02. The validated date will be coordinated at the Joint Staff level and published in annual CJCSN 6510.XX updates (reference a).
- f. Step Five ALPHA -- DAA identifies requirement for continued use. If a DAA identifies an operational need to continue use of a cryptographic equipment past its removal date, the DAA prepares the rationale/justification for keeping the equipment in operation and identifies tactics, techniques, and procedures that may be applicable to augment information protection actually being afforded by the obsolete cryptographic device.
- g. Step Five BRAVO -- DAA petitions for continued use. The DAA will submit a petition for continued use of a specific cryptographic item through the NSA.
- h. Step Five CHARLIE -- NSA Assesses and recommends. NSA will assess continued use of the obsolete cryptographic equipment to determine and describe the resulting risk, establish criteria for risk acceptance (when applicable), and identify steps that shall be taken to mitigate risk and minimize negative consequences. That assessment and its accompanying recommendations will be provided to the MCEB for direction and action.
- i. Step Five DELTA -- MCEB decision point. Based upon NSA's recommendation, the MCEB will decide to approve or deny the DAA's request for continued use of obsolete equipment.
- j. Step Five ECHO -- DAA identifies alternative capabilities. If the MCEB does not approve the DAA's petition, the DAA will have to discontinue use of the cryptographic and identify alternative and/or additional capabilities to protect the national security information in the affected communications system under his control.
- k. Step Five FOXTROT -- Continued use IAW MCEB direction. If the petition is approved, the DAA will be able to operate within the established parameters that have been validated by the MCEB.
- l. Step Six -- NSA discontinues key production. After a cryptographic item passes its removal date, NSA will stop key production for that equipment in conjunction with its removal from the inventory and/or

Enclosure B

regrade the classification of keying material and product control commensurate with the actual information protection being provided.

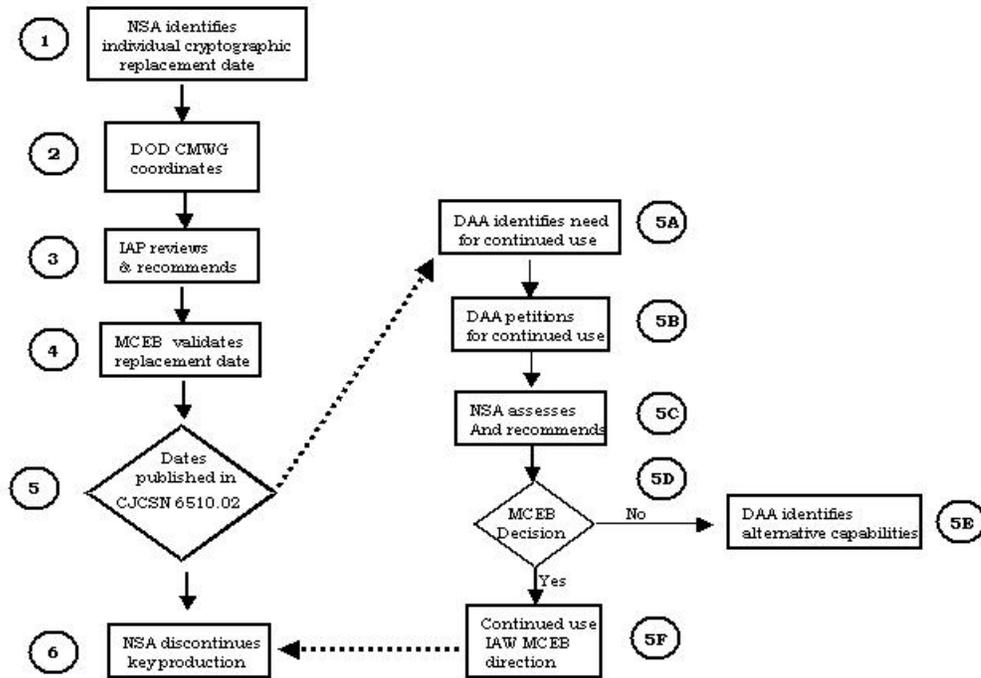


Figure B-1. Cryptographic Modernization Planning Process

(INTENTIONALLY BLANK)