CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6 CJCSI 6510.02D
DISTRIBUTION: A, B, C, JS-LAN 15 October 2010

CRYPTOGRAPHIC MODERNIZATION PLANNING

References: See Enclosure C

1. Purpose. Given the authority by reference a, this instruction provides policy and guidance for planning, programming, and implementing the modernization of cryptographic products certified by the National Security Agency (NSA) and held by Department of Defense (DOD) components. (Upon request, assistance with implementing this instruction can be made available by contacting the Joint Staff J65C or the NSA Information Assurance Directorate.)

2. Cancellation. CJCSI 6510.02C, 21 July 2006, is canceled.

3. Applicability. This instruction applies to the combatant commands and their subordinate commands, joint task forces, Services, Defense Agencies, and Defense Activities. The organizations to which this instruction applies must act in accordance with its policy objectives and in compliance with direction provided by reference b.

4. Policy. Pursuant to reference c, U.S. military forces require interoperable secure communications to support joint, allied, combined, interagency, 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 combatant commanders, exercise continuing oversight of assigned forces' IA solutions and cryptographic programs, as well as their implementations. Therefore;

a. DOD components will use only NSA approved cryptographic products to protect classified and/or sensitive national security information that is processed and transmitted over National Security Systems (NSS).

b. The NSA, as the national manager for cryptographic products will, through the National Cryptographic Solutions Management Office (NCSMO), identify cryptographic products requiring replacement, pursuant to reference b. The NCSMO will collaborate with data owners in determining the specific last year of use (LYOU) for aging devices and algorithms. Urgency associated with modernization planning will be reported in reference b, using color codes as follows: RED -- cryptographic product modernization planning and/or execution is not sufficient to avoid risk to the intelligence life of information encrypted by those products. Immediate removal from operational mission areas is required. YELLOW -- cryptographic product modernization planning and/or execution must ensure product removal from mission areas before the year listed in reference b table as LYOU. GREEN -- devices are fully compliant with national cryptographic standards. This is the case for devices with LYOU beyond 2025.

c. Services must comply with reference b.

(1) Designated Approving Authorities (DAAs) or system owners, when no DAA has been identified, in conjunction with other Services, should request a risk assessment for continued use of decertified products no later than one year prior to published LYOU. This request should be directly coordinated with the NSA NCSMO. In the event it would be required to use a decertified product beyond the published cease key dates then the DAA or system owner must submit a key extension for decertified product request. Requests should be submitted as soon as a deficiency and/or limitation is noted, but no later than one year prior to the published Cease key dates. Requests shall be submitted on a case-by-case basis until such systems can be transformed, modernized, or otherwise replaced. Enclosure B defines this process.

(2) In cases where a key extension for decertified products affects multiple Services across the DOD and there is no specified service DAA; the petition for a key extension will be initiated by the Service with the greatest operational impact, as determined by the Cryptographic Solutions Technical Advisory Group (CSTAG). That Service will act as the Lead Organization (LO) to facilitate the petition for a key extension. The LO will provide supporting documentation pursuant to Enclosure A, paragraphs 1-a thru 1-e, (i.e., impact statements, and requirements) from the user communities affected by the decertification. All other Services that are affected to a lesser degree will gather information and provide supporting documentation pursuant to Enclosure B, paragraphs 4-a and 4-e. Once this action is completed, with the culmination of supporting documentation from the Services, the request will then be passed up through their chain for staffing and final endorsement before being sent to the Joint Staff. Once the endorsement has been received, the petition request

will then be forwarded to the Joint Staff (J65C) for formal staffing and processing. From that point, the process follows the directions given in this instruction in Enclosure B, Figure B-1. During Joint Staff processing, the request will be forwarded to the NSA for analysis and recommendations. NSA will forward the results of their analysis with specific recommendations to the Military Communications-Electronics Board (MCEB) via Joint Staff (J65C). The request will continue to follow the procedures as outlined in Figure B-1. In the submission of the request, the petitioning Service will address the same requirements outlined in the responsibilities of the DAA, as outlined in Enclosure A of this instruction.

5. Background. As a direct result of increases in computational power and improvements in adversary cryptanalytic techniques and attacks, Information Assurance (IA) solutions composed of cryptographic products (to include equipment, items, offline aids, and systems that utilize communication security (COMSEC) and transmission security capabilities) eventually lose their ability to protect information. The degradation is particularly insidious when dealing with sensitive information that must be protected for years, if not decades, after transmission. In addition, IA solutions and cryptographic products become logistically unsupportable and must be replaced to ensure sustainment of critical mission operations and communications. For these reasons, planning, executing, and implementing replacement of cryptographic products must proceed in a timely and deliberate manner. The time period information requires to be protected from adversary exploitation after transmission intelligence life helps determine the last year of use (LYOU) for the specific cryptographic device and algorithm used in its original transmission. The intelligence life of information is generally determined by the data owner or original data creator.

6. Responsibilities. All DOD components must adhere to the specific guidance, contained in Enclosures A, B, and C of this instruction.

7. Action or Procedure. Entities to which this instruction applies shall act in accordance with the objectives that it establishes and with the procedures that it describes.

8. Summary of Changes. Enclosure B has been modified to assist DOD components in understanding of procedures for submitting a request for a key extension for decertified products determined necessary to support specific operational missions. Enclosure C, described the process for determining LYOU for cryptographic products, has been removed and replaced with the reference page.

9. Releasability. This instruction is approved for limited release. DOD components (to include the combatant commands) and other federal agencies may obtain copies of this instruction through controlled internet access only (limited to .mil and .gov users) from the CJCS Directives Home Page--http://www.dtic.mil/cjcs_directives/. Also on the SIPRNet Cryptographic Modernization Initiative Home Page--http://www.iad.nsa.smil.mil/resources/library/cryptomod_section/index.cfm. Joint Staff activities may access or obtain copies of this instruction from the Joint Staff Local Area Network.

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

FOR
B. E. GROOMS
RADM, USN
Vice Director, Joint Staff

Enclosures:
- A -- Cryptographic Modernization Responsibilities
- B -- Cryptographic Modernization Planning Process for Requesting Key Extension for a Decertified Product
- C -- References

ENCLOSURE A

CRYPTOGRAPHIC MODERNIZATION RESPONSIBILITIES

1. DAAs or system owners, when no DAA has been identified, in conjunction with other Services will:

a. Address the operational readiness of IA solutions and cryptographic products employed to provide continuous protection to national security information transmitted via command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR); information technology (IT); and weapons systems.

b. Initiate materiel and fiscal planning to replace and modernize cryptographic products, pursuant to implementing the direction, objectives, and requirements of reference b.

c. Identify critical replacement needs and modernization requirements (to include space and nuclear command and control (NC2) applications) in accordance with reference b, d, and e. Additional clarifying information for space and NC2 applications can be obtained from the NSA NCSMO at 410-854-8577

d. Address capabilities requirements for modernized cryptographically based IA solutions for C4ISR, IT, and weapons systems developments that are intended to replace operational systems that employ at-risk or obsolescent cryptographic products in accordance with reference f.

e. Identify, evaluate, and approve/disapprove development of cryptographically based IA solutions for C4ISR, IT, and weapons systems capabilities requirements, in compliance with reference b.

f. Consult and act in accordance with reference e when releases to foreign nations are considered or when a key extension is operationally necessary.

2. The MCEB will:

a. Validate plans through the IA Steering Group (IASG) for programmed transformation, modernization, and replacement of cryptographic items presented to it by the Joint Staff, the NSA, the Services, Agencies, and combatant commanders, through the CSTAG.

b. Refer, as necessary, any new or modified cryptographic modernization capabilities requirements, in accordance with reference f.

3. Combatant commanders will:

a. Identify to the affected Services, through the Joint Staff, any special and/or unique cryptographic capabilities required within their respective areas of responsibility that pertain to the transformation, modernization, or replacement of cryptographic products and systems.

b. As appropriate, ensure that requests for the release of cryptographic products to foreign governments, interagency and international organizations, in accordance with reference e, consider the phase-out indicators specified in reference b and that replacement of cryptographic products that are approaching obsolescence are addressed in the release action.

c. As appropriate, ensure DAA or system owner's requests for a key extension for decertified products, in accordance with reference g, are processed as specified in Enclosure B.

d. Monitor cryptographic product implementations, transitions, and fielding to identify deficiencies that restrict compliance with reference b or restrict operationally required joint, allied, interagency, or combined interoperability. Advise the appropriate Service(s) and the Joint Staff of cryptographic modernization deficiencies and coordinate their resolution.

e. In addition to the responsibilities identified above, the Commander, USSOCOM, under Title 10 acquisition authority, will fund for special operations forces' unique cryptographic items, pursuant to cryptographic product replacement objectives identified in reference b.

4. Services and Agencies will:

a. Plan, program, and budget for the transformation, modernization, or replacement of U.S. cryptographic products and systems pursuant to reference b, as well as for Joint, Allied, Interagency, and Combined interoperability requirements identified by combatant commanders, their chief information officers, and their DAAs.

b. Schedule and synchronize cryptographic product and system transformation, modernization, or replacement to continually improve and preserve joint, allied, interagency, and combined interoperability within each combatant command area of responsibility.

c. Transform, modernize, or replace cryptographic products and systems in U.S. DOD elements for which it is responsible, pursuant to reference b.

d. Monitor cryptographic products and systems implementations, transitions, and fielding to identify deficiencies that restrict compliance with reference b or diminish interoperability in Joint, Allied, Interagency, Coalition or Combined environments. Advise Joint Staff, via the CSTAG, and other Service(s) of cryptographic modernization deficiencies in order to coordinate a resolution.

e. Present and brief the MCEB annually on all planning for cryptographic modernization, quarterly for all RED statuses in reference b and, for all key extensions granted previously by the MCEB

f. Report to the Joint Staff, via the CSTAG, implementation of reference b and compliance with references b and e by program managers and DAAs.

5. Director, NSA (DIRNSA) will:

a. Plan, program, and budget for IA research, development, testing, and engineering necessary to transform, modernize, and replace NSA-certified cryptographic products, pursuant to reference b.

b. Coordinate program schedules for cryptographic product transformation, modernization, and replacement with combatant commands, Services, and Agencies, via the CSTAG, as it pertains to implementing reference b.

c. Prescribe standards, policies, and procedures governing installation, operation, handling, transformation, modernization, replacement, maintenance, modification, configuration control, and disposition of NSA certified cryptographic products or systems, on behalf of, the DOD.

d. Advise allies, coalition partners, and civil agencies of the schedule for cryptographic product transformation, modernization, and replacement, as contained in reference b.

e. Make available for sale or lease, via foreign military sales or other U.S. Government means, replacement or modifications for cryptographic products to ensure continued utility and interoperability.

f. Ensure that the design, engineering, and manufacture of cryptographic replacement products are in compliance with current DOD policy regarding interoperability and are certified as interoperable for joint, allied, interagency, and coalition operations, as required.

g. Decertify cryptographic products and discontinue associated keying material pursuant to implementing objectives identified in reference b.

h. Recommend or non-concur in DAA key extension requests for cryptographic products identified in reference b, pursuant to Enclosure B of this instruction.

i. Establish a product obsolescence timetable for each cryptographic product and the LYOU for those products to be used by system certifiers, system accreditors, and DAAs.

j. In coordination with the Joint Staff, ensure adjudication of cryptographic issues that impact joint or combined secure interoperability.

k. Provide COMSEC keying materials for cryptographic products so long as they are approved for use. Once products have reached the date(s) identified for discontinued use, NSA will discontinue keying material distribution for those systems/devices, unless directed otherwise by higher authority. For the purpose of this instruction, this would be via MCEB approval of a DAA/LO petition for a key extension.

l. In conjunction with JS/J6 and Defense Information Systems Agency (DISA), determine applicable DAA or system owner for decertified cryptographic products from 5.g. and ensure timetable and LYOU from 5.i. is issued to identified DAA and/or system owner.

m. Provide instructions, guidance, and a template for completing a key extension request package.

6. Defense Information Systems Agency (DISA) will:

a. Plan, program, and budget for the transformation, modernization, or replacement of cryptographic products under its cognizance, in accordance with reference b.

b. Ensure the coordinated transformation, modernization, or replacement of cryptographic products within the Defense Information Systems Network (DISN).

c. Support identification and resolution of interoperability deficiencies related to Joint, Allied, and Combined applications of products and systems listed in reference b.

d. Assist DIRNSA in determining applicable DAA or system owner for decertified cryptographic products.

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

a. In coordination with the NSA, ensure adjudication of cryptographic issues that impact joint, allied, or combined interoperability.

b. Validate interoperability requirements and process foreign release requests for approval, in accordance with reference e.

c. Process DAA requests for key extension for decertified products under DISA's purview using cryptographic products identified in reference b pursuant to Enclosure B of this instruction.

d. Assist DIRNSA in determining applicable DAA or system owner for decertified cryptographic products.

(INTENTIONALLY BLANK)

ENCLOSURE B

CRYPTOGRAPHIC MODERNIZATION PLANNING PROCESS FOR REQUESTING A KEY EXTENSION FOR A DECERTIFIED PRODUCT

1. General. DAAs, or system owners, when no DAA has been identified, in conjunction with their Service components can petition the MCEB, through the J6, for key extension for decertified products that contain a cryptographic product beyond the product's published cease key dates. Each system key extension request will be processed on a case-by-case basis and must be assessed by the NSA, which will recommend a course of disposition for review/approval by the MCEB. All system continued use dates will be coordinated at the Joint Staff level.

2. Definition. Key extension for a decertified product is the authorization for continued operation of a NSS beyond the NSA-prescribed decertification dates for cryptographic products used within that system. Key extension requests shall be approved by the MCEB.

3. Prior to submitting a key extension request for a decertified product. Before engaging in the key extension process, a DAA must recognize degradation of security based on information presented in reference b, or increasing difficulties in providing logistic support to a cryptographic product or system. The DAA will then conduct an Analysis of Alternatives (AoA), to include a security risk analysis of the processed information, to determine if a new system is appropriate, alternative approaches are available, or if continued use of the old system is required. All alternative approaches (including material and non-material solutions, non-material meaning, tactics, techniques & procedures (TTP's), policy changes) must be fully considered to eliminate or mitigate information security risk to the system warfighter.

4. Process to request key extension for a decertified product. A block diagram of the cryptographic modernization process for key extension is detailed in Figure 1. Each numbered step is discussed in detail in the following paragraphs.

a. Step One – DAA, or system owner, in conjunction with other Services determines requirement for continued use. If a DAA, or system owner, identifies a compelling operational need to continue use of a cryptographic system employing products past their published cease key dates, the DAA must prepare the rationale/justification for keeping the affected system in operation and identify the TTP's that may be applicable to augment IA protection. The DAA will notify the Service Principal in order to inform the

CSTAG the system affected requires a key extension and to have an LO appointed as necessary.

b. Step Two – DAA petitions the MCEB for key extension, coordinated through the Joint Staff. The DAA will submit a petition to request continued use of a system containing specific cryptographic equipment that has surpassed its published cease key dates to the Joint Staff (J65C). The Joint Staff (J65C) will process the request and have it prepared for the MCEB. The information may be sent either scanned soft copy via SIPRNet (contact J65C directly to get the current email address to forward petition) or mail it directly to the address listed below:

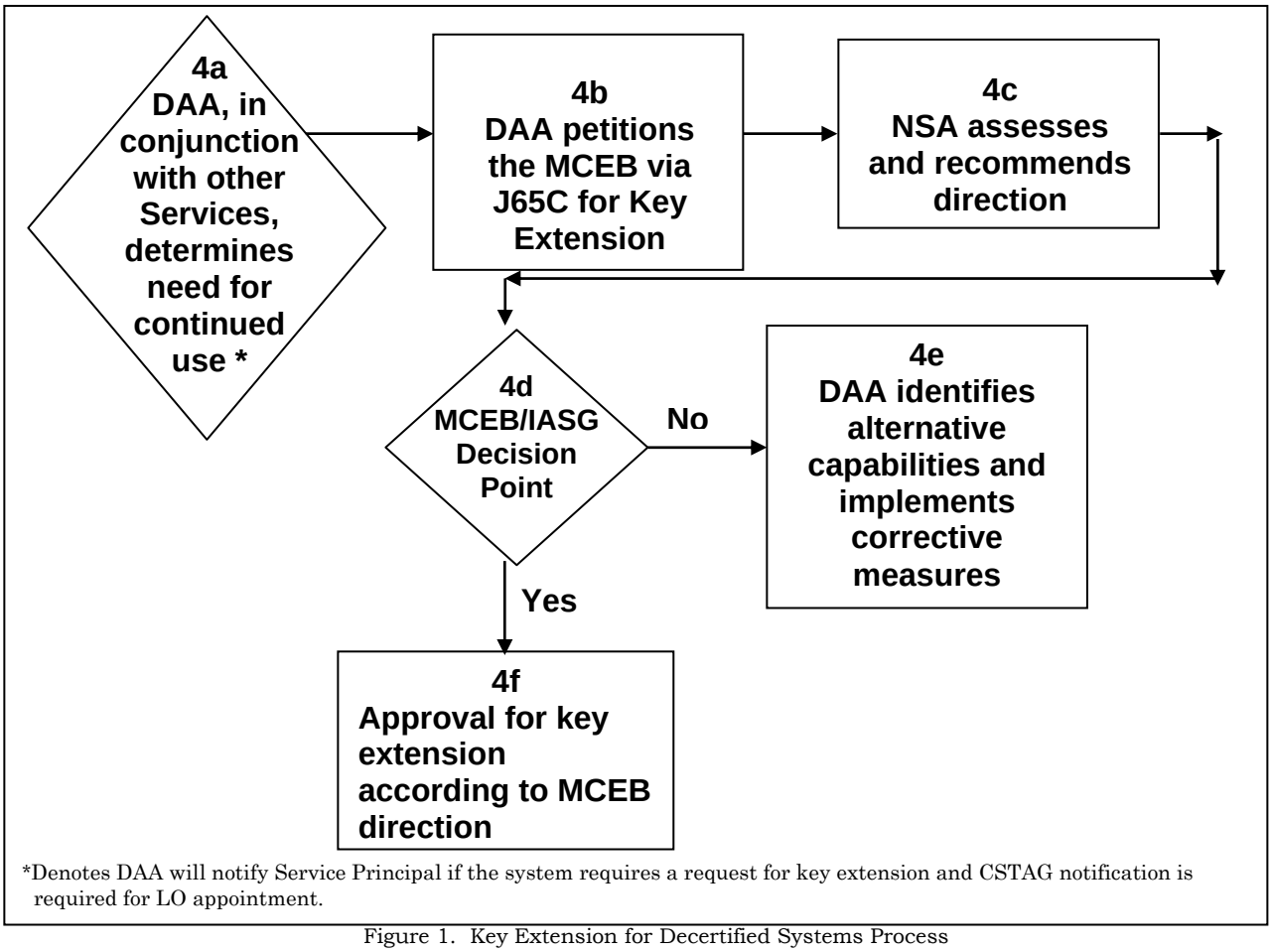
J65C
DOD J6
6000 Joint Staff
Pentagon
Washington, DC 20318-6000

c. Step Three – The NSA assesses and recommends. The J6 will forward the request to the NSA, which will review the DAA's AoA, determine and describe the resulting risk, establish criteria for risk acceptance (when applicable), and identify steps to be taken to mitigate risk and minimize negative consequences. That assessment and its accompanying recommendations will be provided to the MCEB/IASG and DAA for direction and action.

d. Step Four – MCEB decision point. The MCEB will decide to approve or deny a DAA's request for continued use of systems utilizing cryptographic products past their published cease key dates.

e. Step Five – DAA identifies alternative capabilities. If the MCEB disapproves the petition, the DAA will identify alternatives and/or additional capabilities to protect the information in the effected communications system and implement corrective measures.

f. Step Six – Approval of key extension according to MCEB direction. If the petition is approved, the DAA will be able to operate within the established parameters recommended by the NSA and approved by the MCEB. The DAA shall provide notification of key extension to the appropriate user community including allies.



*Denotes DAA will notify Service Principal if the system requires a request for key extension and CSTAG notification is required for LO appointment.

Figure 1. Key Extension for Decertified Systems Process

(INTENTIONALLY BLANK)

ENCLOSURE C

REFERENCES

a. DODI 8523.01, 22 April 2008, "Communications Security (COMSEC)"

b. CJCSN 6510 Series, "Information Assurance Cryptographic Equipment Modernization Requirements"

c. DODI 4630.8, 30 June 2004, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"

d. CJCSI 6510.01 Series, "Information Assurance and Computer Network Defense"

e. CJCSI 6510.06 Series, "Communications Security Releases to Foreign Nations"

f. CJCSI 3170.01G Series, "Joint Capabilities Integration and Development System"

g. CJCSM 6510.01 Series, "Defense-In-Depth: Information Assurance (IA) and Computer Network Defense (CND)"

SUPPORTING DOCUMENTS

CJCSI 6212.01 Series, "Interoperability and Supportability of Information Technology and National Security Systems "

CJCSI 6211.02 Series, "Defense Information Systems Network (DISN): Policy and Responsibilities"

(INTENTIONALLY BLANK)