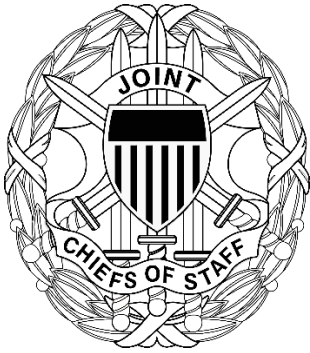


UNCLASSIFIED

CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION



J-6

DISTRIBUTION: A, B, C

CJCSI 6510.02G

20 March 2025

CRYPTOGRAPHIC MODERNIZATION PLANNING

References:

See Enclosure E

1. Purpose. In accordance with (IAW) the authority in reference (a), this instruction provides policy and guidance for planning, programming, and implementing the modernization of High Assurance cryptographic products certified by the National Security Agency (NSA) and held by Department of Defense (DoD) Components. Cryptographic products approved through the Commercial Solutions for Classified (CSfC) program are not included in this instruction. All CSfC modernization questions should be referred to the CSfC Program Office (PO) in the NSA Cybersecurity Directorate. Cryptographic products approved through the Cryptographic High Value Product (CHVP) program are not included in this instruction. All CHVP modernization questions should be referred to the CHVP PO in the NSA Cybersecurity Directorate. Upon request, assistance with implementing this instruction can be made available by contacting the Joint Staff Directorate for Command, Control, Communications, and Computers/Cyber, J-6 or the NSA Cybersecurity Directorate.

2. Superseded/Cancellation. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.02F, "Cryptographic Modernization Planning," 4 August 2022 is hereby superseded.

3. Applicability. This instruction applies to the Combatant Commands (CCMDs) and their subordinate commands, joint task forces, Services, Defense Agencies, and DoD Field Activities. The organizations to which this instruction applies must act IAW its policy objectives and in compliance with 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

UNCLASSIFIED

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

command and control responsibilities of the joint military command structure dictate that the CJCS (supported by the Joint Staff) and the Combatant Commanders (CCDRs) exercise continuing oversight of assigned forces' cybersecurity 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 processed and transmitted over National Security Systems (NSS).

b. The NSA, as the national manager for cryptographic products will, through its Cryptographic Evaluation (CE) office, identify only NSA approved cryptographic products requiring replacement, pursuant to reference (b). The CE office will collaborate with data owners to determine the specific last year of use (LYOU) for aging devices and algorithms. Urgency associated with modernization planning will be reported IAW reference (b), using color codes as follows:

(1) RED – obsolete cryptographic devices still in the inventory, and in operation beyond LYOU. 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.

(2) YELLOW – cryptographic product modernization planning and/or execution must ensure product removal from mission areas within 10 years of the date listed in the LYOU table in reference (b).

(3) GREEN – devices are fully compliant with national cryptographic standards and LYOU is greater than 10 years away.

c. Services and Defense Agencies must comply with reference (b).

(1) POs (Service Selected Entity), in conjunction with their Authorizing Official (AO) or AO equivalent and Service Principal and/or Chief Information Officer (CIO), should request a continued use of decertified products not later than (NLT) 1 year prior to the published LYOU in reference (b). This request should be directly coordinated by the PO, the NSA CM office, and reviewed by the Joint Staff J-6. In the event a decertified product would be required to be used beyond the published cease key dates, then a key extension request (KER) for decertified product must be submitted. Requests should be submitted as soon as a deficiency and/or limitation is noted that could impact the reported transition date, but NLT 1 year prior to the published cease key dates.

UNCLASSIFIED

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

Requests shall be processed on a case-by-case basis until such systems can be transformed, modernized, or otherwise replaced. Enclosure B defines key extension procedures for decertified cryptographic products. POs must develop a briefing using the provided Military Command, Control, Communications, and Computers Executive Board (MC4EB) slide templates and brief their programs at the MC4EB boards. Slide templates can be located at the MC4EB SharePoint on SIPRNET: <<https://intelshare.intelink.sgov.gov/sites/mc4eb/SitePages/Home.aspx>>.

(2) In cases where a key extension for decertified products affects multiple Services across DoD and there is no specified Service AO, the petition for a key extension will be initiated by the Service with the greatest operational impact, as determined by the MC4EB Cryptographic Security Panel (CSP). The process will be as follows:

(a) That Service will act as the lead organization (LO) to facilitate the petition for a key extension.

(b) 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.

(c) 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.

(d) When the culmination of supporting documentation from the Services is complete, the request will be passed through their chain for staffing and final endorsement before sending the request to the Joint Staff.

(e) Once the endorsement has been received, the petition request will be forwarded to the Joint Staff J-6 for formal staffing and processing.

(f) From that point, the process follows the directions given in this instruction in Enclosure B, Figure 1.

(g) During Joint Staff processing, the request will be forwarded to the NSA for analysis and recommendations.

(h) NSA will forward the results of their analysis with specific recommendations to the MC4EB via the Joint Staff J-6.

UNCLASSIFIED

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

(i) The request will continue to follow the procedures as outlined in Enclosure B, Figure 1.

(j) In the submission of the request, the petitioning Service will address the same requirements outlined in the PO responsibilities as described in Enclosure A of this instruction.

(3) Upon the completion of modernization efforts and the need for a KER no longer exists, the Service acting as LO will submit a Close Out memo IAW the template found in Enclosure D.

5. Definitions. See Glossary.

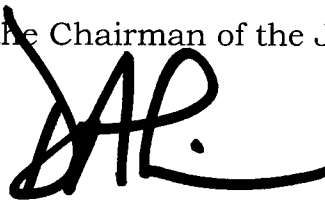
6. Responsibilities. All DoD Components must adhere to the specific guidance contained in Enclosures A, B, C, and D of this instruction.

7. Summary of Changes. Updates to CJCSI 6510.02G include clarifying authority, roles, responsibilities, and procedures for the Services and CCMDs for submission of a KER for continued use of communication security devices whose cryptographic algorithms have reached the LYOU or have been decertified. Added KER close out template to references (reference (d)). References dates have also been updated.

8. Releasability. UNRESTRICTED. This directive is approved for public release; distribution is unlimited on the Non-classified Internet Protocol Router Network (NIPRNET). DoD Components (to include the CCMDs), other Federal agencies, and the public may obtain copies of this directive through the Internet from the CJCS Directives Electronic Library at <<http://www.jcs.mil/library>>. Joint Staff activities may also obtain access via the SECRET internet Protocol Router Network (SIPRNET) directives Electronic Library web sites.

9. Effective Date. This INSTRUCTION is effective upon signature.

For the Chairman of the Joint Chiefs of Staff:



DOUGLAS A. SIMS, II, LTG, USA
Director, Joint Staff

UNCLASSIFIED

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

Enclosures

- A – Cryptographic Modernization Responsibilities
- B – Cryptographic Modernization Planning Process for Requesting Key
Extension for a Decertified Product
- C – Key Extension Request Template
- D – KER Close out Template
- E – References

UNCLASSIFIED

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

(INTENTIONALLY BLANK)

UNCLASSIFIED

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

ENCLOSURE A

CRYPTOGRAPHIC MODERNIZATION RESPONSIBILITIES

1. The PO, in conjunction with Service Principal/CIO and AO will:

a. Address the operational readiness of cybersecurity 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 entering the YELLOW category, pursuant to implementing the direction, objectives, timelines, and requirements of reference (b).

c. Develop a POA&M, to include an architecture overview of the systems and networks, a fielding plan, schedule, and programmatic funding profile for cryptographic products entering the YELLOW category.

d. Identify critical replacement needs and modernization requirements (to include space and Nuclear Command, Control, and Communications applications) IAW references (d) and (e). Additional clarifying information for space and nuclear command and control (NC2) applications can be obtained from the NSA Cryptographic Modernization (CM) office at <NSACryptoMod@nsa.smil.mil> (SIPRNET).

e. Address capability requirements for modernized, cryptographic cybersecurity solutions for C4ISR, IT, and weapons systems developments that are intended to replace operational systems that employ at-risk or obsolescent cryptographic products IAW reference (g).

f. Identify, evaluate, and approve/disapprove development of cryptographic cybersecurity solutions for C4ISR, IT, and weapons systems capability requirements in compliance with reference (b).

g. Consult and act IAW reference (e) when releases to foreign nations are considered, or when a key extension is operationally necessary.

UNCLASSIFIED

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

2. The MC4EB will:

a. Validate and monitor plans for programmed transformation, modernization, and replacement of cryptographic items presented by the Joint Staff, NSA, Services, Agencies, and CCMDs, through the MC4EB Cryptographic Security Panel, IAW reference (f).

b. Refer, as necessary, any new or modified cryptographic modernization capabilities requirements to the Joint Requirements Oversight Council IAW reference (g).

3. CCDRs 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 (AOR) 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, IAW 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 requests for a key extension for decertified products are processed as specified in Enclosure B on behalf of foreign partners within their respective AORs.

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.

e. Advise the appropriate Service(s) and the Joint Staff of cryptographic modernization deficiencies, and coordinate their resolution.

f. In addition to the responsibilities identified above, Commander, U.S. Special Operations Command, under title 10 acquisition authority, will fund for special operations forces' unique cryptographic items, pursuant to cryptographic product replacement objectives identified in reference (b).

UNCLASSIFIED

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

4. Services and Agencies will:

a. Plan, program, and budget for the transformation, modernization, replacement, sustainment, and disposition of U.S. cryptographic products and systems pursuant to reference (b), as well as for joint, allied, interagency, and combined interoperability requirements identified by CCDRs, their CIOs, and their AOs.

b. Develop a POA&M, to include an architecture overview of the systems and networks, a fielding plan, schedule, and programmatic funding profile.

c. Schedule and synchronize cryptographic product and system transformation, modernization, or replacement to continually improve and preserve joint, allied, interagency, and combined interoperability within each CCMD AOR.

d. Transform, modernize, or replace cryptographic products and systems in U.S. DoD elements for which it is responsible, pursuant to reference (b).

e. 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.

f. Advise the Joint Staff, via the MC4EB CSP, and other Service(s) of cryptographic modernization deficiencies to coordinate a resolution. Services and agencies shall also assess and identify instances of encryption not in compliance with NSA-approved quantum resistant algorithms or Commercial National Security Algorithms, and report their results to the NSS National Manager via the DoD CIO IAW section 1 (b).(iv).(D) of reference (k). Points of contact for the MC4EB can be found at the MC4EB Sharepoint on SIPRNET: <<https://intelshare.intelink.sgov.gov/sites/mc4eb/SitePages/Home.aspx>>.

g. Present and brief the MC4EB annually, or as prescribed by the MC4EB, on all planning for cryptographic modernization, for all YELLOW and RED statuses in reference (b), and for all key extensions granted previously by the MC4EB.

h. Report to the Joint Staff, via the MC4EB CSP, the implementation of reference (b), and compliance with references (b) and (e) by program managers and AOs.

UNCLASSIFIED

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

i. Deliver a cryptographic modernization plan, updated annually, to the DoD CIO to ensure synchronization of efforts meet current and emerging threats to NSS.

5. Director, NSA (DIRNSA) will:

a. Plan, program, and budget for the cybersecurity 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 CCMDs, Services, and agencies, via the MC4EB CSP, 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 DoD.

d. Advise allies and coalition partners 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, replacements or modifications for cryptographic products to ensure continued utility and interoperability.

f. Ensure 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. Advise the MC4EB on risk posture, to include probability of an event occurrence, in order to enable Services/POs to assess risk and the MC4EB in making a decision to approve or deny a KER 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 AOs.

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

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

k. Provide communications security (COMSEC) keying materials for cryptographic products, so long as they are approved for use. Once cryptographic 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, the direction would be via MC4EB approval of a KER.

l. In conjunction with the Joint Staff J-6 and the Defense Information Systems Agency (DISA), determine the applicable PO for decertified cryptographic products identified in 5.g. and ensure timetable and LYOU from 5.i. is issued to the identified PO.

m. Provide instructions, guidance, and a template for completing a KER package.

6. DISA will:

a. Plan, program, and budget for the transformation, modernization, or replacement of cryptographic products under its cognizance, IAW CJCSN 6510 (reference b).

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

c. Support identification and resolution of interoperability deficiencies related to joint, allied, and combined applications of products and systems listed in CJCSN 6510 (reference b).

d. Assist DIRNSA in determining applicable PO and/or AO for decertified cryptographic products.

7. Joint Staff J-6, 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, IAW reference (e).

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

c. Process KERs 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 identifying applicable PO and/or AO for decertified cryptographic products.

UNCLASSIFIED

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

ENCLOSURE B

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

1. General. POs, in conjunction with their AOs and Service Principals/CIO, can petition the MC4EB, through the Joint Staff J-6, for key extension for systems that require continued operations of an NSA cryptographic product beyond the product's published LYOU. MC4EB will review and validate petitions for continued employment of cryptographic devices for a specific system beyond the dates directed by reference (b).
2. Definition. Key extension for a decertified product is the authorization for continued operation of an NSS beyond the NSA-prescribed decertification dates for cryptographic products used within that system. KERs shall be approved by the MC4EB.
3. Prior to Submitting a KER for a Decertified Product. Before engaging in the key extension process, a PO 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 PO should contact their Operational Mission Executive Agent, who 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, if alternative approaches are available, or if continued use of the existing system is required. All alternative approaches (including material and non-material solutions; non-material meaning; tactics, techniques, and procedures (TTPs); policy changes) must be fully considered to eliminate or mitigate information security risk to the Service/Agency's system.
4. Process to Request Key Extension for a Decertified Cryptographic 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 – Determine Requirement for a KER. If a PO, their AO, and their Service Principal/CIO identify a compelling operational need to continue using a cryptographic system employing products past published cease key dates, a rationale/justification for keeping the affected system in operation must be prepared, and TTPs that may be applicable to augment cybersecurity protection must be identified. The PO will notify the Service Principal/CIO in order to inform the MC4EB CSP that the system affected requires a key

UNCLASSIFIED

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

extension and to have an LO appointed as necessary. See Enclosure C for the memorandum template.

b. Step Two – Petition the MC4EB for Key Extension. The Service Principal/CIO will submit a petition to the Joint Staff J-6 to request continued use of a system containing specific cryptographic equipment that has surpassed its published cease key dates. The petition is in the format of a KER (see format in Enclosure C). The KER may be sent either by scanned soft copy via SIPRNET (points of contact for the MC4EB can be found at the MC4EB Sharepoint on SIPRNET: <<https://intelshare.intelink.sgov.gov/sites/mc4eb/SitePages/Home.aspx>>) or by mail to the address listed below:

Joint Staff/J-6 Office
6000 Joint Staff Pentagon
Washington, DC 20318-6000
Service Executive Agent CryptoMod Office

c. Step Three – Joint Staff J-6 will Process the KER. The Joint Staff J-6 will process the request and have it prepared for the MC4EB. The J-6 will also forward the KER and AoA to the NSA for review and assessment.

d. Step Four – NSA Assesses and Recommends. NSA will review the KER and 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. NSA's assessment and recommendations will be provided to the MC4EB for direction and action.

e. Step Five – MC4EB Decision. The MC4EB will decide through its governance structure outlined in reference (f) to approve or deny a request for continued use of systems utilizing cryptographic products past their published cease key dates.

f. Step Six – Identify Alternative Capabilities and Implement Corrective Measures. If the MC4EB disapproves the petition, the PO, in conjunction with their AO and Service Principal/CIO, will identify alternatives and/or additional capabilities to protect the information in the at-risk communications system and implement corrective measures.

g. Step Seven – Approval of Key Extension According to MC4EB Direction. If the petition is approved, the PO will be able to operate within the established parameters recommended by the NSA and approved by the MC4EB. The Service PO shall provide notification of key extension to the appropriate user community, including allies.

UNCLASSIFIED

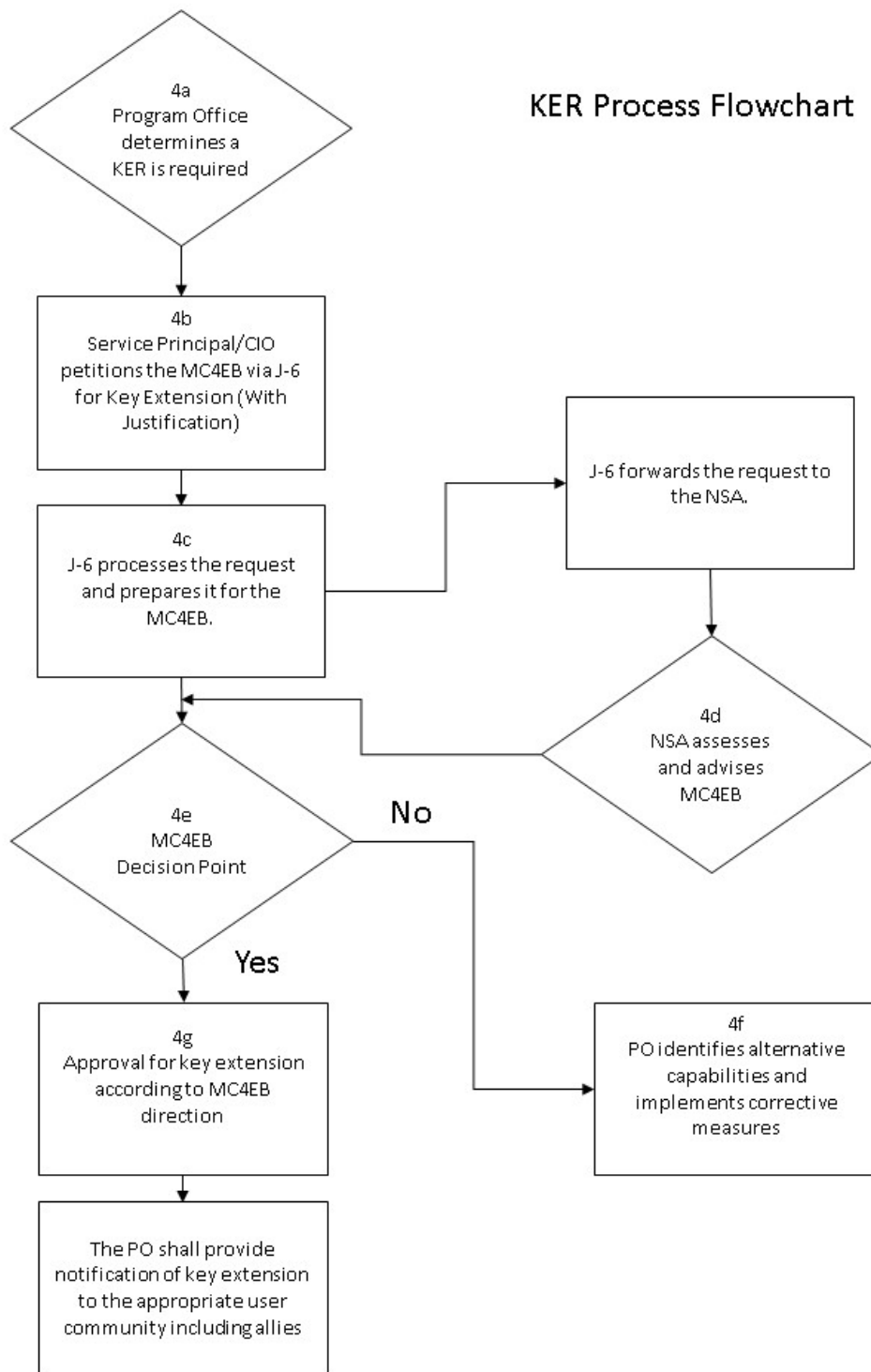


Figure 1. KER Process Flowchart

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

(INTENTIONALLY BLANK)

UNCLASSIFIED

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

ENCLOSURE C

KEY EXTENSION REQUEST TEMPLATE

Before submitting your KER, remember to classify your documents IAW the Classification Guide For Cryptographic Modernization 3-9 (obtained through the NSA CM office) in relation to the enclosed information.

Reply to:

MEMORANDUM FOR: MILITARY COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS EXECUTIVE BOARD (MC4EB)

THRU: Service Principal/CIO

Joint Staff/J-6 Office
6000 Joint Staff Pentagon
Washington, DC 20318-6000
Service Executive Agent CryptoMod Office

SUBJECT: REQUEST FOR CONTINUED KEY MANAGEMENT SUPPORT FOR NSA DECERTIFIED CRYPTOGRAPHIC EQUIPMENT

1. The (Program Office) requests continued key management support from NSA until (month year) for (cryptographic device) using the (cryptographic algorithm name) algorithm. The program office and system owner acknowledge reviewing NSA's Cryptographic Equipment Decertification (CED) memoranda specifically decertifying cryptographic devices used in systems affected by this KER. The (Authorizing Official (AO) and Operational Mission Data Owner) acknowledges receipt and review of (CED memoranda) and that the NSA will not waive stated decertification commitments. AO willingly accepts all risk associated with the continued operations of the system(s) listed in line item number two below.
2. List all operational systems and networks by names that are affected by this KER. Provide a detailed description of each to include whether the network supports a NC2, Joint, allied/coalition partner, and/or Service-specific mission.
3. List all U.S. Military Services, Agencies, CCMDs, and allied/coalition partners affected by this KER.

UNCLASSIFIED

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

4. List all key short titles affected by this KER, including classification of key, frequency of key change (i.e., daily, weekly, monthly, or yearly), and controlling authorities.
5. List all cryptographic devices by nomenclature or short title affected by this KER.
6. Provide the following information for a more detailed understanding of how the cryptographic device, system, and network function together:
 - a. State how long the data owner requires the data to be protected from compromise once it has been transmitted over the network (e.g., 1 hour, 1 day, 1 year, 5 years, 10 years, 20 years).
 - b. State at what speed information is transmitted over the network (e.g., 2.4Kbps, 16Kbps, 1Mbps, 5Mbps).
 - c. State what RF spectrum the information is transmitted over the network (e.g., LF, VLF, HF, UHF, EHF).
 - d. State how often is the cryptographic device and system setting in a ready state connected with the distant end waiting to exchange data (e.g., 24/7, 12/7, 1 day per week, 5 days per week).
 - e. State how often the information is actively transmitted from the system across the network (e.g., constant broadcast, 10-minute bursts, 2-hour transmissions, 3 times per day).
7. List the hardware and/or software issues that are preventing the modernization of these systems listed above in line item number 2, IAW the timelines published in (CED memoranda).
8. Categorize the operational risk IAW the Joint Risk Analysis Methodology (reference (j)). Use the entire expected modernization timeline to define the time horizon. A complete operational risk assessment will be conducted by the supporting Service and NSA after initial request submission. The supporting Service will be responsible for assessing consequence, and NSA will be responsible for assessing probability.
9. Provide any additional information that is pertinent to assisting in assessing the risk of the KER.

UNCLASSIFIED

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

10. Provide the PO a POA&M for achieving discontinued use of obsolete cryptographic equipment and replacing with modernized equipment. Include a detailed solution description of each system and network listed in line item 2. The POA&M needs to include an architecture overview of the systems and networks, a fielding plan, schedule, and programmatic funding profile.

11. Do you certify that the network **does not** contain any members that would continue to operate at an information sharing level other than that for which the keying material will be extended (members requiring information sharing at a higher classification level must be moved to another, approved network to operate at the intended level of classification)?

12. The following requestor information and signatures must be completed within the DoD Memoranda signature block before submitting this request to the MC4EB and the Joint Staff (J-6).

Requestor: Combatant Command/Service/Program Office Information:

Rank / Grade Last, First MI: _____

Command / Agency: _____

City / State / Zip Code: _____

Country: _____

Telephone: _____

Unclassified E-mail: _____

Classified E-mail: _____

(Program Office Signature)

(Name and Date)

.....

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

Requestor: Data Owner:

Rank / Grade Last, First MI: _____

Command / Agency: _____

City / State / Zipcode: _____

Country: _____

Telephone: _____

Unclassified E-mail: _____

Classified E-mail: _____

(Data Owner Signature)

(Name and Date)

.....
Requestor: Agency AO (i.e., DAA) Information:

Rank / Grade Last, First MI: _____

Command / Agency: _____

City / State / Zipcode: _____

Country: _____

Telephone: _____

Unclassified E-mail: _____

Classified E-mail: _____

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

(DAA Signature)

(Name and Date)

.....
Requestor: Service Principal/CIO:

Rank / Grade Last, First MI: _____

Command / Agency: _____

City / State / Zipcode: _____

Country: _____

Telephone: _____

Unclassified E-mail: _____

Classified E-mail: _____

(Service CIO Signature)

(Name and Date)

Before submitting your KER remember to classify your documents IAW the Classification Guide For Cryptographic Modernization 3-9 (obtained through the NSA CM office) in relation to the enclosed information.

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

(INTENTIONALLY BLANK)

UNCLASSIFIED

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

ENCLOSURE D

KEY EXTENSION REQUEST CLOSE OUT TEMPLATE

Reply to:

MEMORANDUM FOR: MILITARY COMMAND, CONTROL, COMMUNICATIONS,
AND COMPUTERS EXECUTIVE BOARD (MC4EB)

THRU: Service Principal/CIO

Joint Staff/J-6 Office
6000 Joint Staff Pentagon
Washington, DC 20318-6000
Service Executive Agent CryptoMod Office

SUBJECT: FINAL CLOSE OUT OF (SYSTEM) KEY EXTENSION REQUEST

1. The (Program Office) requests discontinuation of the (system) Key Extension Request (KER).
2. The algorithm associated with the (system) KER is (algorithm). The current KER is in effect until (day, month, year).
3. The short titles associated with the (system) KER are:
 - a. (short title)
4. The COMSEC Manager, (first name, last name), acknowledged the cancellation of key support for (system) in accordance with current policy and procedures.
5. Per this memorandum, I declare key support for (system) is no longer required. My point of contact for this matter is (first name, last name) who can be reached at (phone number) or (classified email).

NAME, RANK, SERVICE
Position/Title

Attachments:
As stated

D-1

Enclosure D

UNCLASSIFIED

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

(INTENTIONALLY BLANK)

UNCLASSIFIED

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

ENCLOSURE E

REFERENCES

- a. DoDI 8523.01, 6 January 2021, "Communications Security (COMSEC)"
- b. CJCSN 6510, 31 August 2019, "Information Assurance Cryptographic Device Modernization Requirements"
- c. DoDI 8330.01, 27 September 2022, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)"
- d. CJCSI 6510.01F, 16 August 2022, "Information Assurance and Computer Network Defense"
- e. CJCSI 6510.06D, 31 July 2024, "Communications Security Releases to Foreign Partners"
- f. CJCSI 5116.05A, 22 January 2024, "Military Command, Control, Communications, and Computers Executive Board"
- g. CJCSI 5123.01I, 30 October 2021, "Charter of the Joint Requirements Oversight Council and Implementation of the Joint Capabilities Integration and Development System"
- h. CJCSM 6510.01B, 20 July 2012, "Cyber Incident Handling Program"
- i. NSA/CSS Classification Guide For Cryptographic Modernization (Cryptomod) 3-9, 1 March 2022
- j. CJCSM 3105.01B, 22 December 2023, "Joint Risk Analysis Methodology"
- k. National Security Memorandum-8, 19 January 2022, "Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems"

UNCLASSIFIED

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

(INTENTIONALLY BLANK)

UNCLASSIFIED

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

GLOSSARY

ACRONYMS

AO	Authorizing Official
AoA	Analysis of Alternatives
C4ISR	command, control, communications, computers, intelligence, surveillance, and reconnaissance
CCMD	Combatant Command
CED	Cryptographic Equipment Decertification
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chief of Staff
CJCSI	Chairman of the Joint Chief of Staff Instruction
CJCSN	Chairman of the Joint Chief of Staff Notice
CND	Computer Network Defense
COMSEC	communications security
CM	cryptographic modernization
CSfC	Commercial Solutions for Classified
CSP	Cryptographic Security Panel
DIRNSA	Director, NSA
DISA	Defense Information Systems Agency
DoD	Department of Defense
IC	Intelligence Community
IT	information technology
JROC	Joint Requirements Oversight Council
KER	Key Extension Request
LO	lead organization
LYOU	last year of use
MC4EB	Military Command, Control, Communications and Computers Executive Board
NC2	nuclear command and control
NIPRNET	Non-Classified Internet Protocol Router Network
NSA/CSS	National Security Agency/Central Security Service
NSS	National Security Systems

UNCLASSIFIED

CJCSI 6510.02G
20 March 2025

PO	program office
POA&M	Plan of Action and Milestones
SIPRNET	Secret Internet Protocol Router Network
TTP	tactics, techniques, and procedures