Department of the Army
Pamphlet 25–2–16

Information Management: Army Cybersecurity

Communications Security (COMSEC)

Headquarters
Department of the Army
Washington, DC
8 April 2019

UNCLASSIFIED

SUMMARY

DA PAM 25–2–16
Communications Security (COMSEC)

This new Department of the Army pamphlet, dated 8 April 2019—

- Provides Army communications security guidance for all information technology capabilities used in and by the Army (chap 2).
- Describes the Key and Certificate Management Plan process (app C).
- Establishes the process related to the Army Capability Support Plan and its function to implement the Department of the Army mandate to review and validate the Army programs' requests for technical services and support from the National Security Agency (app D).
- Adds process for submitting a key extension request in accordance with the Chairman of the Joint Chiefs of Staff Instruction 6510.02E (app E).
- Addresses implementation of DODI 8523.01, DODI 8500.01, and DODI 8510.01, as they relate to communications security (throughout).

Headquarters
Department of the Army
Washington, DC
8 April 2019

Department of the Army Pamphlet 25–2–16

Information Management : Army Cybersecurity

Communications Security (COMSEC)

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army

History. This publication is a new Department of the Army pamphlet.

Summary. This pamphlet implements DODI 8523.01, DODI 8500.01, and DODI 8510.01 as they relate to communications security. It provides Army communications security guidance for all information technology capabilities used in and by the Army. Guidance is also provided regarding national security systems that utilize commercial products and/or architectures for protecting information, both designated as data-at-rest and/or data-in-transit. This document provides procedural guidance that relates to the policies established in AR 25–2. It contains instructions, processes, formats, reporting requirements, and guidelines necessary to register and track all Army deployments and use of commercial solutions and equipment.

Applicability. This pamphlet applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. Also, it applies to Department of the Army civilian personnel, including civilian contractors.

Proponent and exception authority. The proponent of this pamphlet is the Chief Information Officer/G–6. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Office of the Chief Information Officer/G–6 (SAIS–PRG), 107 Army Pentagon, Washington, DC 20310–0107.

Distribution. This pamphlet is available in electronic media only and is intended for the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

Contents—Continued

Appendixes

Figure List

Glossary

Chapter 1
Introduction

1–1. Purpose
This Department of the Army pamphlet (DA Pam) issues the Army communications security (COMSEC) procedures for all information technology (IT) capabilities used in and by the Army. COMSEC is a component of cybersecurity concerned with the measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptographic security, transmission security, emissions security, and physical security of COMSEC material. Guidance is also provided about national security systems (NSS) that utilize commercial products and/or architectures for protecting classified information, both designated as data-at-rest and/or data-in-transit. This DA Pam expands on the instructions, processes, formats, reporting requirements, and guidelines for all COMSEC procedures for all IT capabilities used in and by the Army.

1–2. References and forms
See appendix A.

1–3. Explanation of abbreviations and terms
See the glossary.

1–4. Scope
This DA Pam applies to all Headquarters, Department of the Army (HQDA) staff, Army commands (ACOMs), Army service component commands (ASCCs), direct reporting units (DRUs), program executive officers (PEOs), Army agency directors, program managers (PMs) and product directors (PDs), cybersecurity personnel, engineering personnel, acquisition personnel, and capability developers, designers, testers, and general users responsible for achieving acceptable levels of cybersecurity in acquisition, operation, and maintenance for all IT and network systems used in/by the Army. It is applicable to information systems (ISs) used for teleworking, ISs owned or operated by contractors ISs, ISs acquired with non-appropriated funds, automated tactical systems, automated weapons systems (AWSs), and distributed computing environments as directed by proper authority. Department of Defense (DOD) and Army information include Special Access Program (SAP) IT, other than SAP IS handling sensitive compartmented information (SCI). This document does not alter or supersede existing authorities and policies of the Director of National Intelligence regarding the protection of SCI and SAP for intelligence as directed by Executive Order 12333, and for national security information (NSI) systems as directed by Executive Order 13231, and other applicable laws and regulations.

1–5. Overview
a. This DA Pam aligns with DODI 8523.01, DODI 8500.01, and DODI 8510.01, as they relate to COMSEC. Army COMSEC programs will incorporate all Army, National Institute of Standards and Technology (NIST), DOD, Joint, and Committee on National Security Systems (CNSS) policies and procedures when addressing cybersecurity, as directed by proper authority.

b. All Army IT will be assigned to, and governed by, an ACOM or agency cybersecurity program that manages risk commensurate with the importance of supported missions and the value of potentially affected information or assets.

c. Army organizations must ensure individual accountability and responsibility for assigned personnel. Commanders, directors, information system owners (SOs), authorizing officials (AOs), information systems security managers (ISSMs), information systems security officers (ISSOs), PMs, PDs, supervisors, and users in positions with privileged access are responsible and accountable for the implementation of Army security requirements in accordance with AR 25–2 and this DA Pam.

Chapter 2
Communications Security
This chapter provides Army standards and procedures for the acquisition, implementation, and life cycle management of cryptographic systems, products, and services used to protect Army controlled unclassified information (CUI) and classified NSI, systems, and networks.

2–1. Protection of national security information and national security systems
a. Security requirements.

(1) NSS are any telecommunications system or IS operated by the U.S. Government, the function, operation, or use of which—

(a) Involves intelligence activities.

(b) Involves cryptologic activities related to national security.

(c) Involves command and control of military forces.

(d) Involves equipment that is an integral part of a weapon or weapon system.

(e) Is critical to the direct fulfillment of military or intelligence missions, and does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

(2) Protect transmission of Army information through the COMSEC measures and cybersecurity procedures set forth in this document.

(3) Only NSA/Central Security Services-approved COMSEC products and services (to include Commercial Solutions for Classified (CSfC) and cryptographic high value property (CHVP)) will be used to secure NSI and systems.

(4) Only NSA-approved cryptographic products and solutions that have been endorsed by the Chief Information Officer (CIO)/G–6, Cybersecurity Directorate (SAIS–CB) and listed in the Army Information Systems Security Program Application (ISSPA) will be used for the protection of classified information.

(5) Do not use foreign cryptographic systems or products to protect U.S. classified NSI. Further, do not use a NIST or National Information Assurance Partnership (NIAP) Common Criteria testing laboratory-evaluated product that is not part of an NSA-approved cryptographic solution (for example, CSfC), and endorsed by the CIO/G–6, Cybersecurity Directorate (SAIS–CB).

(6) Use of any product not endorsed by CIO/G–6, Cybersecurity Directorate (SAID–CB) to protect classified NSI will be removed from the Army network. Any questions should be directed to CIO/G–6, Cybersecurity Directorate (SAIS–CB).

(7) SOs and commanders will develop and maintain a continuity of support plan/IT contingency plan to ensure operational availability of commonly used COMSEC equipment during crisis or contingencies.

(8) COMSEC equipment will be compatible and interoperable with DOD and NSA-approved key management systems.

(9) Classified cryptographic devices and unencrypted keying material will be accounted for by entry of this information into the COMSEC materiel control system. Encrypted keying material is considered UNCLASSIFIED//FOUO and will be accounted for and tracked. Refer to AR 380–40 and TB 380–41 for additional guidance on encrypted key.

(10) Account for and track unclassified controlled cryptographic items (CCI) and CHVP as organizational equipment using the property book. Refer to AR 710–2 for additional guidance.

(11) Only keying material produced by NSA or generated by NSA-certified key generation sources will be used to key cryptographic systems that protect NSI and systems.

b. Cryptographic system solutions deployed in high risk areas.

(1) High risk areas are areas or situations where capture or exploitation is possible or almost certain.

(2) Tactical environments are commensurate with being deployed on the battlefield or other hostile areas, which are deemed as a high-risk area.

(3) For the purposes of this DA Pam, all tactical ISs (excluding single purpose devices that process/transmit/store non-tactical information internal to the platform) are considered critical to the direct fulfillment of military or intelligence missions, and therefore are regarded as NSS. Requests for exception to a tactical IS being an NSS must be submitted to the CIO/G–6, Cybersecurity Directorate (SAIS–CB) for evaluation and approval.

(4) All tactical ISs (systems employed in a tactical environment) will be protected by NSA-approved or NSA-certified cryptography. NSA-approved cryptography includes those NSA-approved public standards covered under Committee on National Security Systems Policy (CNSSP) 15.

(5) PEOs/PMs/SOs will perform a risk assessment to determine appropriate security levels for their system and environment.

(6) All cryptographic systems employed in the tactical force structure must be compatible with public key infrastructure and/or the electronic key management system/key management infrastructure (KMI).

c. Protect national security systems using National Security Agency-approved public standards.

(1) Depending on the mission and requirement for interoperability, the use of NSA-approved public standards cryptography may be used to protect NSS and NSI per CNSSP 15. The implementation of these NSA-approved public standards and algorithms must be reviewed and approved by the CIO/G–6, Cybersecurity Directorate (SAIS–CB), prior to acquisition and implementation.

(2) CSfC.

(a) CSfC is a process that allows the use of commercial components (selected from the NSA-approved CSfC components list) to be used in a layered solution in accordance with NSA-approved capability packages (CPs) to protect classified

NSS and NSI. This can enable the development and fielding of secure communication systems with richer features and lower costs in a shorter time than custom government-developed solutions.

(b) Army organizations pursuing CSfC solutions will coordinate with the Communications Electronics, Research and Development Engineering Center (CERDEC) CSfC trusted integrator team prior to NSA registration to identify possible technical issues. CERDEC can provide guidance and technical assistance to resolve issues and support the organization in obtaining NSA registration and AO authorization of the CSfC solution.

(c) CERDEC will maintain a repository of CSfC information that will be made available to Army organizations. This repository will include DOD CSfC implementations for different CPs, lists of components for each CP implementation, and lessons learned. Component lists will include NSA CSfC component lists and Army-recommended hardware lists, software releases, and standard configuration information.

(d) Any Army program or activity requesting to implement a CSfC solution must include planning to fully fund rapid replacement of all systems planned for fielding.

2–2. Protection of controlled unclassified information

Protect information not approved for public release and processed on DOD ISs with NIST-approved products for the protection of controlled unclassified/sensitive but unclassified U.S. Government or commercial information. Cryptographic systems or products intended for the protection of unclassified or sensitive information and systems must comply with the following--

a. Use cryptographic modules validated under the NIST Cryptographic Module Validation Program as meeting, at minimum, level 2 security requirements of Federal Information Processing Standard (FIPS) 140–2.

b. Systems and products must be evaluated by a NIAP-certified or common criteria evaluation and validation scheme-certified common criteria testing laboratory and, at minimum, meet all requirements of evaluation assurance level 3 and the common criteria controlled access protection profile. This requirement is not applicable to enterprise security management, general purpose operating systems, and database management systems.

c. Use of invalidated cryptographic modules for the protection of sensitive information is prohibited. All cryptographic solutions for the protection of sensitive information must comply with subparagraphs *a* and *b*, above.

d. Products that exceed minimum FIPS 140–2 security requirements and common criteria evaluation assurance levels will be given preference when considered for procurement.

e. Requirements for NIST–NIAP-approved cryptographic systems intended to protect CUI will be identified and validated by the CIO/G–6, Cybersecurity Directorate (SAIS–CB). Funding for these systems will be the responsibility of the organization or activity identifying the requirement.

f. Implementation of triple DES utilizing appropriate key material constructs that do not support DES or DES interoperability are valid with lifecycles indicated in NIST SP 800–57.

g. Advanced encryption standard (AES) can be used to protect sensitive and unclassified information. The implementation of AES in products intended to protect classified NSI and NSS must be reviewed and approved by NSA, and approved by the CIO/G–6, Cybersecurity Directorate (SAIS–CB) prior to their acquisition. Acquire all COMSEC products and services via the ISSPA that serves as the centralized COMSEC acquisition authority.

2–3. Acquisition of Commercial Communications Security Endorsement Program security solutions

a. The Commercial COMSEC Endorsement Program (CCEP) is an NSA development program for cybersecurity products. Under the CCEP, NSA enters into a business relationship with a vendor to develop and produce products that are of direct and obvious benefit to improving the cybersecurity posture for DOD customers. The Army treats CCEP devices as non-developmental products.

b. Non-developmental cryptographic material using an algorithm approved by NSA under the CCEP (CCI/CHVP) will use the CERDEC evaluation process. The CERDEC evaluation report from the CERDEC Cryptographic Modernization Laboratory is a requirement for type classification. Prior to equipment use, PEO/PMs will coordinate with project leader network enablers (PL NET Es).

c. PEOs/PMs, in accordance with 10 USC 2366b, are required to provide a plan to mitigate and account for any costs in connection with anticipated modernization and de-certification of cryptographic systems and components during the production and procurement of the major defense acquisition program. This plan will be coordinated with the CIO/G–6, Cybersecurity Directorate (SAIS–CB).

d. Procurement of cryptographic products directly from a vendor is prohibited. All cryptographic products will be requested through the Army ISSPA, approved by HQDA staff (Assistant Secretary of the Army (Acquisition, Logistics and Technology) (ASA (ALT)); CIO/G–6, Cybersecurity Directorate (SAIS–CB); and Deputy Chiefs of Staff, G–3/5/7, G–4, and G–8), and procured through Communications Security Logistics Activity (CSLA) to be valid for use. Exceptions will be considered on a case-by-case basis by the CIO/G6, Cybersecurity Directorate (SAIS–CB).

e. COMSEC products will be developed, acquired, operated, maintained, and disposed of through the approved methods set forth in this DA Pam, as well as in AR 700–142, AR 710–2, AR 380–40, and associated security doctrine.

f. Army organizations must go through the Army Information Systems Security Program (ISSP) process to acquire COMSEC products and services.

Note. Some requests through ISSPA requires a supporting Communications Security Account to be identified.

g. Army PEOs/PMs/cybersecurity program managers, and special operations program managers are responsible for requesting and locally validating their organization's requests for cryptographic equipment, as authorized by modified table of organization and equipment (MTOE)/table of distribution and allowances (TDA) (see app B).

h. The ISSPA facilitates the procurement of standalone cryptographic solutions. It does not provide a means to procure acquisition program developed products.

i. Organizations may submit a request for expedited delivery (RED) via the ISSPA to meet urgent requirements needed within 60 days. An RED will be addressed by HQDA ahead of routine requests. The process is available online at https://issp.army.mil.

j. Request commands validate requirements (in accordance with AR 710–2 and AR 71–32) for cryptographic equipment and ensure alignment with organizational MTOE and TDA authorizations. Detailed instructions and procedures on how to enter and track your requirements in the Army ISSPA are available online at https://issp.army.mil.

k. Basis of issue plan (BOIP) feeder data developed by Army PMs for new weapons/computing environment (CE) systems, IT systems and NSS, will separately identify end item Class II and Class VII radios and other cryptographic equipment as "separately authorized" associated support items of equipment, to ensure all such devices are added to The Army Authorization Documents System (MTOE/TDA) in accordance with AR 71–32, and accounted for on unit property books for reporting to the CCI Serialization Program via Global Combat Support System-Army, as mandated by CNSSI 4001 and AR 710–3.

2–4. Funding requirements

a. The ISSPA is the Army's single, authoritative, requirements repository for recording, validating, and approval of requests for cryptographic equipment. It is the HQDA management tool to centrally record requests for cryptographic equipment and serves as an acquisition support tool. The information collected in the ISSPA is used to develop funding requirements for the annual program objective memorandum (POM) cycle. Additionally, in accordance with AR 25–2, the ISSPA is the required resource for Army commands to input their projected requirements for cryptographic and key management equipment to meet mission needs and to comply with modernization initiatives.

b. Army components/ACOMs/ASCCs/DRUs will identify and program for cybersecurity funding requirements for ISs they manage and control. Materiel developers will identify and program for cybersecurity funding requirements for strategic and tactical ISs they own as a part of the ISs' program costs, and follow AR 700–127 policy to ensure cybersecurity compliance for all fielded, PM-developed systems throughout the life cycle of the system. The CIO/G–6, Cybersecurity Directorate (SAIS–CB) will develop and publish annual cybersecurity funding guidance for Army components/ACOMs/ASCCs/DRUs cybersecurity requirements managed in management decision packages (MDEPs) as appropriate.

c. ACOM/ASCC/DRU ISSOs and ISSMs will use the Army ISSPA, managed by the Communications Security Logistics Activity at Fort Huachuca, Arizona, to submit their cybersecurity and COMSEC funding requirements for MDEPs MS4X and FPMC for review and validation. To establish an account and receive training for the Army ISSPA input, ISSOs and ISSMs must contact the ISSPA help desk at csla.issp@us.army.mil or call commercial at (520) 538–1829.

d. Resourcing for cryptographic equipment is provided in two ways—

(1) Central Army procurement is through "FPMC" fund source for cryptographic capability resourced from HQDA managed assets. The FPMC equipment requests are managed against Army priorities, authorization levels and command plan requirements submitted by Army organizations.

(2) Units and acquisition programs transfer organizational funds to the organizational purchase communications security fund source for cryptographic equipment being procured using unit or program funds for valid/documented authorizations.

e. Enhancements or modifications to the ISSPA should be directed to the CIO/G–6, Cybersecurity Directorate (SAIS–CB) for review.

2–5. Key and certificate management planning for cryptographic components and solutions

a. Key and certificate management plans (KCMPs) are vital to the implementation of COMSEC products and services into the Army infrastructure. All approved cryptographic systems protecting NSS, NSI or CUI (to include CSfC) will have a KCMP that describes in detail all activities involved in the design and handling of cryptographic keying material for the

system. Keying material includes other related security parameters (such as IDs, PINS, and passwords). In addition, Army programs will have a key and certificate specification, when needed. The KCMP will describe accountability/tracking of the keying material over the entire life cycle of the system from generation, distribution, storage, accounting, and entry of key into the system through use, deletion, and final destruction.

b. The CIO/G–6, Cybersecurity Directorate (SAIS–CB) must ensure that cryptographic solutions being developed by Army programs are supportable, sustainable, and conform to the enterprise architecture consistent with KMI capabilities.

c. The KCMP document describes the use and control of all key management products and services (including other related security parameters such as IDs, PINs, and passwords) used by a cryptographic application (cryptographic engine, end cryptographic unit, system of systems) throughout its life cycle. Refer to the NSA KCMP Data Item Description and the NSA technical security requirements document for the document template and content guidance (see app C).

d. All Army programs developing cryptographic solutions protecting NSS, NSI or CUI, to include those that do not require NSA infrastructure or production support (for example, CSfC), are required by AR 25–2 to have a CIO/G–6, Cybersecurity Directorate (SAIS–CB)-approved KCMP.

e. The process for Army programs to follow for drafting and submitting a KCMP to the CIO/G–6, Cybersecurity Directorate (SAIS–CB) for HQDA staffing and approval is defined in appendix C.

f. Key management requirements.

(1) All Army programs that develop, acquire, or use a cryptographic application, module, or system will—

(a) Use KMI standards, specifications, and protocol, including provisions for secure electronic delivery of key management products and services to the cryptographic application.

(b) Use encrypted key distribution and encrypted fill methods for distributing key management products and services. Key encryption allows the Warfighter to distribute keys securely over various networks.

(c) Implement protection techniques for classified software, algorithms and data. Comply with NSA requirements to protect classified software, algorithm and data in end solutions. Army programs can use algorithm encryption such as JOSEKI and WATARI. A JOSEKI or WATARI implementation must meet NSA specification and requirements.

(2) Exceptions to the requirements listed in (1) above must be documented in the KCMP and approved by the CIO/G–6, Cybersecurity Directorate (SAIS–CB).

(3) PMs, with test key requirement issues, must contact the CIO/G–6, Cybersecurity Directorate (SAIS–CB) for assistance.

2–6. Protected distribution systems

a. Protected distribution systems (PDSs) must be constructed per criteria contained in National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 7003, AR 380–27, and supplemented with the cybersecurity procedures in AR 25–2.

b. Any IS that includes a PDS to transmit data will not be operationally accredited until the PDS has been approved by AO.

2–7. Radio-frequency wireless systems

This applies to securing radio-frequency (RF) wireless solutions on tactical networking infrastructure. However, this section does not apply to secret collateral classified and unclassified cellular and wireless local area network solutions employed by Army organizations.

a. Protect all voice-, data-, or network-defined military radio systems and commercial off-the-shelf implemented wireless communications devices and services to the level of sensitivity of the information contained or transmitted.

b. Use electronic, auto-manual, or manual crypto-systems to provide the required security for existing radio systems that do not have embedded or electronic crypto-systems. However, all future procurements must comply with paragraph 2–3 above. All radio systems that pass NSS information must follow paragraphs 2–1 and 2–2, above.

c. The use of commercial non-encrypted radio systems in support of command and control functions is strictly prohibited.

d. Radios used for public safety communications with civil agencies or to communicate on civil aviation channels are excluded from the requirements of subparagraphs *a* and *b*, above. However, this exclusion does not apply to communications dealing with aviation combat operations.

2–8. National Security Agency support service request

a. The CIO/G–6, Cybersecurity Directorate (SAIS–CB) will validate requests for NSA security services. Any Army organization seeking NSA services to support mission requirements must submit a request by means of a client questionnaire. Request must be submitted to CIO/G–6, Cybersecurity Directorate (SAIS–CB). The CIO/G–6, Cybersecurity Directorate (SAIS–CB) facilitates the request process by providing support in developing and refining the NSA requirements

questionnaire and by submitting the request to the appropriate authorities for approval. Requests submitted directly to NSA will be accepted, however, will be rerouted back to the CIO/G–6, Cybersecurity Directorate (SAIS–CB) for action. Requests submitted directly to NSA will experience a delay in processing due to required rerouting. Requests to NSA are submitted via the NSA Client Advocate in the NSA IAD (see app D).

b. If the requirement does not have approval from the Deputy Chief of Staff (DCS), G–3/5/7 or TRADOC capability manager (TCM), it will not receive NSA support.

c. The initial request must be submitted by the first colonel in the chain of command or the PM.

d. NSA Army Client Advocate forwards completed client questionnaire to CIO/G–6, Cybersecurity Directorate (SAIS–CB) for staffing. CIO/G–6, Cybersecurity Directorate (SAIS–CB) will coordinate program product requirements with appropriate authorities and approval by the DCS, G–3/5/7 and/or the appropriate TCM prior to soliciting NSA support. (Note: If the requirement does not meet Army validation requirements then it will not receive NSA support). The CIO/G–6, Cybersecurity Directorate (SAIS–CB) will validate the program product requirements and coordinate submission to the NSA Client Advocate to receive NSA support. The validated request will be prioritized and approved by DCS, G–3/5/7 and returned to the CIO/G–6, Cybersecurity Directorate (SAIS–CB) for submission to the NSA. NSA will triage requests and identify resourcing requirements to support the program/initiative. Requests that are not approved will be returned to the requestor.

e. CIO/G–6, Cybersecurity Directorate (SAIS–CB) will conduct bi-annual staffing and quarterly reviews of those programs/initiatives receiving or requesting NSA support with the DCS, G–3/5/7 Mission Command LWN Director and the NSA Army Senior Account Manager to ensure all efforts continue to be aligned with Army priorities.

2–9. Key extension requests

The NSA identifies cryptographic products requiring replacement and specifies the last year of use for the legacy device. Key is terminated for devices based on Chairman Joint Chiefs of Staff Notice (CJCSN) 6510. AOs with a compelling operational need (in conjunction with other Services), may request, through the CIO/G–6, Cybersecurity Directorate (SAIS–CB), extended use of keys for operational systems that contain cryptographic products that have passed their last year of use. Requests are on a case-by-case basis, until such systems can be transformed, modernized, or otherwise replaced. The approval will be added as an artifact to the accreditation and authorization (A&A) package. Additional instructions can be found in the current CJCSI 6510.02 series and the Army key extension request (KER) (see app E).

2–10. Use of cryptographic devices

The CIO/G–6, Cybersecurity Directorate (SAIS–CB) will determine what COMSEC/CCI/CHVP devices are approved for use on Army networks. Use of COMSEC/CCI/CHVP not approved by the CIO/G–6, Cybersecurity Directorate (SAIS–CB) on Army networks is prohibited. Army units will identify the need for COMSEC/CCI/CHVP devices via the ISSPA.

Appendix A

References

Section I

Required Publications

AR 25–2
Army Cybersecurity (Cited on title page.)

AR 71–32
Force Development and Documentation (Cited in para 2–3*j*.)

AR 380–40
Safeguarding and Controlling Communications Security Material (Cited in para 2–1*a*(9).)

AR 700–127
Integrated Product Support (Cited in para 2–4*b*.)

AR 700–142
Type Classification, Materiel Release, Fielding, and Transfer (Cited in para 2–3*e*.)

AR 710–2
Supply Policy Below the National Level (Cited in para 2–1*a*(10).)

CJCSI 6510.02 series
Cryptographic Modernization Planning (Cited in para E–1*c*.) (Limited Distribution, available at https://ca.dtic.mil/cjcs_directives/cjcs/instructions.htm.)

CNSSI 4001
Controlled Cryptographic Items (Cited in para 2–3*k*.) (Available at https://www.cnss.gov.)

CNSSP 15
Use of Public Standards for Secure Information Sharing (Cited in para 2–1*b*(4).) (Available at https://www.cnss.gov.)

DODI 8500.01
Cybersecurity (Cited on title page.)

DODI 8510.01
Risk Management Framework (RMF) for DOD Information Technology (IT) (Cited on title page.)

DODI 8523.01
Communications Security (COMSEC) (Cited on title page.)

FIPS 140–2
Security Requirements for Cryptographic Modules (Cited in para 2–2*a*.) (Available at http://csrc.nist.gov.)

NIST SP 800–57
Recommendation for Key Management (Cited in para 2–2*f*.) (Available at http://nvlpubs.nist.gov.)

TB 380–41
Security: Procedures for Safeguarding, Accounting, and Supply Control of COMSEC Materiel (Cited in para 2–1*a*(9).)

10 USC 2366b
Major Defense Acquisition Programs: Certification Required Before Milestone B Approval (Cited in para 2–3*c*.) (Available at http://uscode.house.gov/.)

Section II

Related Publications

A related publication is a source of additional information. The user does not have to read it to understand this publication.

AR 25–30
Army Publishing Program

AR 70–77
Program Protection

AR 380–5
Department of the Army Information Security Program

AR 380–10
Foreign Disclosure and Contacts with Foreign Representatives

AR 380–27
Control of Compromising Emanations

AR 380–67
Personnel Security Program

AR 380–381
Special Access Programs (SAPS) and Sensitive Activities

AR 530–1
Operations Security

AR 710–3
Inventory Management Asset and Transaction Reporting System

CJCSI 5116.05
Military Command, Control, Communications, and Computers Executive Board

CJCSI 6211.02D
Defense Information Systems Network (DISN) Responsibilities

CJCSI 6510.02E
Cryptographic Modernization Planning (U//FOUO)

CJCSN 6510
Information Assurance Cryptographic Equipment Modernization Requirements (S//REL)

CNSSI 1010
Cyber Incident Response

CNSSI 1253
Security Categorization and Control Selection for National Security Systems

CNSSI 4009
Committee on National Security Systems (CNSS) Glossary

CNSSP 11
Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products

CNSSP 12
National IA Policy for Space Systems Used to Support National Security Missions

CNSSP 300
National Policy on Control of Compromising Emanations

DOD 5220.22–M
National Industrial Security Program Operating Manual

DOD 5220.22–R
Industrial Security Regulation

DOD 5400.11–R
Department of Defense Privacy Program

DOD 8570.01–M
Information Assurance Workforce Improvement Program

DODD 5230.09
Clearance of DOD Information for Public Release

DODD 5230.11
Disclosure of Classified Military Information to Foreign Governments and International Organizations

DODD 5230.25
Withholding of Unclassified Technical Data from Public Disclosure

DODD 5500.07
Standards of Conduct

DODD 8000.01
Management of the Department of Defense Information Enterprise (DOD IE)

DODD 8140.01
Cyberspace Workforce Management

DODI 1400.25
DOD Civilian Personnel Management System

DODI 5000.02
Operation of the Defense Acquisition System

DODI 5134.16
Deputy Assistant Secretary of Defense for Systems Engineering (DASD SE))

DODI 5134.17
Deputy Assistant Secretary of Defense for Developmental Test and Evaluation (DASD (DT&E))

DODI 5200.39
Critical Program Information (CPI) Identification and Protection within Research, Development, Test, and Evaluation (RDT&E)

DODI 5200.44
Protection of Mission Critical Functions to Achieve Trusted Systems & Networks

DODI 8520.03
Identity Authentication for Information Systems

DODI 8530.01
Cybersecurity Activities Support to DOD Information Network Operations

DODI 8540.01
Cross Domain (CD) Policy

DODM 5200.01, Volume 3
DOD Information Security Program: Protection of Classified Information

DODM 5200.01, Volume 4
DOD Information Security Program: Controlled Unclassified Information (CUI)

DISN Connection Process Guide
Defense Information Systems Network (DISN) Connection Process Guide

JIE SA
Joint Information Environment Security Architecture

NSTISSP No. 101
National Policy on Securing Voice Communications

NIST SP 800–53 Rev. 4 IR–4
Security and Privacy Controls for Federal Information Systems and Organizations

NSA Data Item Description (DID) DI–MISC–81688A
Key and Certificate Management Plan (KCMP)

NSA Technical Security Requirements Document (TSRD)
Key and Certificate Management Planning

National Security Agency (NSA) Memorandum
Cryptographic Equipment Decertification (CED) (S//REL)

10 USC 2222
Defense business systems: business process reengineering; enterprise architecture; management

29 USC 791
Employment of Individuals with Disabilities

29 USC 794
Nondiscrimination under Federal grants and programs

29 USC 794d
Electronic and Information Technology

Section III

Prescribed Forms

This section contains no entries.

Section IV

Referenced Forms

Unless otherwise indicated, DA forms are available on the APD website (httpw://armypubs.army.mil).

DA Form 2028
Recommended Changes to Publications and Blank Forms

Appendix B

Army Information Systems Security Program Request Process

B–1. Overview

a. This appendix establishes the processes related to the Army Information Systems Security Program (AISSP). The AISSP is the Army's implementation of the Department of Defense (DOD) mandated Information Systems Security Program used to manage and control information assets (Cybersecurity, Information Assurance (IA), and Communications Security (COMSEC) that protect classified, sensitive, and unclassified information stored, processed, accessed, or transmitted by information systems. The ISSPA is the Army's single, authoritative, requirements repository for recording, validating, and approval of requests for cryptographic equipment.

b. The ISSPA is a web-based tool that automates the processes supporting the AISSP. The ISSPA provides centralized records maintenance and validation for IA, Cyber, and COMSEC requirements for the Army. The application provides a means for organizations to plan, program, fund, implement, manage, and provide logistics support to the integration of IA, Cyber, and COMSEC requirements which support the Army Network Campaign Plan (ANCP) to secure command networks and operational IT systems. This application also assists the ISSM, formerly known as Information Assurance Program Managers (IAPM), in implementing their organizational command plans and CS capabilities needed to protect Army systems, networks, and sensitive information per AR 25–2.

c. This appendix applies to the procurement of standalone cryptographic devices using the ISSPA. This appendix does not apply to embedded cryptographic devices or secure mobility solutions. IAPMs/IAMs (ISSMs/ISSOs) are responsible for creating five year command COMSEC modernization command plans. These plans will project future cryptographic requirements for each command. The command plans will be submitted to CIO/G–6, Cybersecurity Directorate (SAIS–CB) for validation. The five year command plans will be used to create an evolutionary acquisition strategy, allowing the commands to maintain effective, modern, secure capabilities.

d. This appendix addresses instructions for the ISSPA validation and approval process.

e. Organizations may have immediate cryptographic requirements (required receipt in less than 60 days). In this case, organizations should follow the operational needs statements playbook guidance and submit their urgent requirement request for COMSEC items into the ISSPA.

f. Additionally, the unit will need to submit a RED outlining the immediate need, and an architectural diagram (AD) reflecting the intent. Samples of these documents can be obtained from the ISSPA.

B–2. Army Information System Security Program Application

This appendix provides guidance on the use of the ISSPA within the DA for all ISSMs/ISSOs/Established Users and leverages applicable DODDs and DA memorandums and regulations as referenced.

B–3. Administrative requirements

Principle HQDA Staff representatives, consisting of DCS, G–3/5/7; CIO/G–6; and DCS G–8, will review and validate Army requests for cryptographic and key management.

a. CIO/G–6, Cybersecurity Directorate (SAIS–CB) will—

(1) Serve as the functional proponent for CS/IA/COMSEC.

(2) Provide program oversight for Army CS/IA/COMSEC equipment and associated ancillary devices.

(3) Request and execute resources for the ISSPA; represent the AISSO resource requirements to support and sustain the AISSP to Army's governance and program execution group (PEG) forum(s) as required.

(4) Fund ISSPA PM and staff per the functional support agreement.

(5) Provide projected Temporary Duty (TDY) scheduled for ISSPA staff.

(6) Establish and maintain ISSPA SOP for the collection, validation, screening, and approval of Army CS/IA/COMSEC requirements supporting the AIAP.

(7) Provide IA/CS/COMSEC guidance to Army elements consistent with the network strategy and in coordination with Army Staff (ARSTAF) via the ISSPA.

(8) Develop, review, and coordinate Army input into DOD CS/IA/COMSEC policy documents.

(9) Conduct annual ISSPA approval and commitment process for projection and DI requirements.

(10) Document concurrence/non-concurrence for the approval/disapproval of ISSPA requirements.

(11) Identify requirements which did not receive unanimous stakeholder concurrence/non-concurrence.

(12) Establish a system that will collect all Army CS/IA/COMSEC requirements for devices needed to protect telecommunications and information systems that process classified, sensitive, and unclassified information systems.

(13) Host weekly ISSPA approval and commitment process.

(14) In coordination with G–3/5/7, validate urgent operational ISSPA requirements.

(15) Document, develop, coordinate, present, prioritize and defend Army CS resource requirements in the planning, programming, and budgeting process as related to forecast data captured in the ISSPA. Based on validated ISSPA requirements, present validated CS requirements into the appropriate PEG.

(16) Evaluate technological trends in Army CS/IA/COMSEC and establish methodologies to integrate advancements based on validated ISSPA requirements.

(17) Use the ISSPA to collect Army CS/IA/COMSEC requirements.

(18) Approve change proposals/requests to the ISSPA to support the software and hardware configuration management process, technology upgrade and modernization, and meet cybersecurity requirements.

(19) Approve and establish software baseline for approved cryptographic and key management solutions.

(20) Provide guidance, including timeline, for ISSPA users to submit COMSEC equipment and IA/CS tools and products projection into the ISSPA database.

(21) Maintain ISSP data within the Army Portfolio Management Solution.

(22) Ensure information assurance requirements are fulfilled regarding the ISSPA accreditation per AR 25–2 and other strategic guidance.

b. DCS, G–3/5/7 will—

(1) Approve and prioritize urgent requirements based on operational needs.

(2) Review network ADs.

(3) Provide guidance and oversight for Army Strategic Planning Board (ASPB) requirements.

(4) Participate in the CIO/G–6, Cybersecurity Directorate (SAIS–CB)-scheduled ISSPA ARSTAF teleconference.

c. DCS G–8 will—

(1) Assist in development of policies and budget criteria.

(2) Provide guidance for funding of Army CS/IA/COMSEC equipment used in support of all Army missions.

(3) Approve funding for urgent AISSP requirements.

(4) Prescribe and supervise the implementation of procedures for management decision package (MDEP) FPMC budget.

(5) Coordinate with CIO/G6, Cybersecurity Directorate (SAIS–CB) regarding validity of network ADs.

(6) Participate in the ISSPA approval and commitment process for projection and data interchange requirements as it applies to asset availability and resource guidance.

(7) Participate in the CIO/G6, Cybersecurity Directorate (SAIS–CB) scheduled ISSPA ARSTAF teleconference.

(8) Approve funding for the ISSPA operation, modernization, cybersecurity and accreditation requirements, life cycle replacement of both hardware and software, and sustainment.

d. CECOM/CSLA staff will—

(1) Provide day to day management of the ISSPA and all functions supporting the application to include—

(a) Development.

(b) Maintenance.

(c) Documentation.

(d) Training.

(e) Help desk support.

(f) Configuration management.

(2) Certification and accreditation.

(a) At direction/approval of HQDA, make system modifications and changes as required.

(b) Interface with HQDA and user-community on required data entry.

(c) Provide initial review of out-of-cycle and urgent ISSPA requests based on authorization documents and on-hand levels.

(d) Provide guidance to CSLA item managers and the ISSP program manager.

(e) Review operational needs statements and AD accompanying ISSPA requests.

e. PL Net E will—

(1) Utilize the ISSPA to collect Army CS/IA/COMSEC requirements for devices needed to protect telecommunications and information systems that process classified or national security related information.

(2) Document all budget and execution data within the ISSPA.

(3) Develop, document, coordinate, prioritize, present, and defend CS/IA/COMSEC resource requirements with direction from the ARSTAF in the planning, programming, and budgeting process as related to forecasted data captured in the ISSPA.

(4) Present validated requirements in coordination with CIO/G–6 to the appropriate PEG.

(5) Provide all pertinent documentation for new CCEP products for inclusion into the ISSPA.

(6) Broadcast and implement replacement initiatives and integration strategies.
(7) Provide resourcing guidance as coordinated with DCS, G–8.
(8) Participate in CIO/G6, Cybersecurity Directorate (SAIS–CB)-scheduled ISSPA ARSTAF teleconference.
(9) Take appropriate resourcing actions on approved REDs.
(10) Identify contingency stock levels to CSLA Information Assurance Division.

f. ISSM will—

(1) Implement a process to execute the duties and responsibilities for the ISSP program.
(2) Use the ISSPA to—

(a) Validate organizational hierarchy as it exists in the ISSPA.
(b) Perform account management by validating subordinate users and maintaining accuracy.
(c) Generate requirements for organization/subordinate organization in the ISSPA.
(d) Validate requirements and forward to CIO/G–6 for approval.
(e) Generate impact statement prior to the approval and commitment process each year. This impact statement informs HQDA on the impact to operations if the units are not fully committed the requested equipment.
(f) Distribute committed assets to themselves and subordinate organizations after HQDA approval.
(g) Ensure requirement dispositions are submitted for their organization and subordinate organizations.

g. ISSO will—

(1) Perform account management by validating subordinate users and maintaining accuracy.
(2) Generate requirements for organization/subordinate organizations in the ISSPA.
(3) Validate requirements and forward to CIO/G–6 for approval.
(4) Ensure requirement dispositions are submitted for their organization and subordinate organizations.

h. CSLA item managers will process requirement dispositions with the following data elements:

(1) Estimated delivery date.
(2) Quantity processed.
(3) Item source (inventory or vendor).
(4) Actual delivery date.
(5) Total package fielding number (if applicable).
(6) Transportation tracking number.
(7) Any notes relevant to the transaction.
(8) Any additional fields required.

i. Other users will—

(1) Generate requirements for their organization in the ISSPA.
(2) Submit requirement dispositions for their organization.

Appendix C

Army Key and Certificate Management Plan Process

C–1. Overview

This appendix provides the process and standard practices for all Army PEOs/PMs/SOs/IAPMs for operationally required systems for Army programs to follow for developing and submitting their KCMP to the CIO/G–6, Cybersecurity Directorate (SAIS–CB) for HQDA support and approval to obtain key support, to include review and approval by the NSA if required. This process allows the CIO/G–6, Cybersecurity Directorate (SAIS–CB) office to staff the appropriate offices to evaluate the proposed KCM approach and ensure the program aligns with the current and future Army KCM architecture, capabilities, processes, and operations. This will ensure usability of critical COMSEC assets, as well as compliance with established policy. It will also prevent possible duplication of effort while ensuring common migration, modernization and interoperability consistent with Army transformation and modernization initiatives.

C–2. Army key and certificate management process applicability

All Army programs developing cryptographic solutions protecting NSS, NSI, or CUI, to include those that do not require NSA infrastructure or production support (for example, CSfC), are required by AR 25–2 to have an approved KCMP. Current programs with a KCMP support agreement with NSA will not be required to follow the procedures documented in this process. Programs that have not submitted a KCMP to CIO/G–6 or NSA, or are currently in the KCMP process with CIO/G–6 or NSA, will be required to follow the procedures as documented. Programs will update their KCMPs at their earliest convenience and coordinate with the CIO/G–6, Cybersecurity Directorate (SAIS–CB) office and CERDEC for review.

C–3. Process duties

In support of execution of this process, these organizations will participate as stakeholders with the following duties:

a. PEOs/PMs/SOs, along with other COMSEC related staff members, are responsible for reviewing and complying with the process described in this document, and guidance provided by the CIO/G–6 in developing a KCMP.

b. CERDEC is responsible for assisting programs in developing KCMPs, providing technical review of KCMPs for Army KCM Stakeholders, as well as reviewing any generated KCM documents and providing technical input regarding the security and other technical and operational aspects of the approach on behalf of the CIO/G–6, Cybersecurity Directorate (SAIS–CB).

c. CIO/G–6, Cybersecurity Directorate (SAIS–CB) will serve as the Army principal organization for the PEO/PMs/SOs with respect to Army network security compliance, Army acceptance/approval, and KCMP documentation staffing within the Army.

d. CSLA key management team is responsible for reviewing and providing comments against all KCMPs to ensure the KCMPs meet Army life-cycle and logistics mission needs for the key and certificate products and services identified in the KCMPs.

e. PL NET E is responsible for COMSEC applications, implementation, and platform integration and will provide review and comments regarding the development, procurement, deployment, and sustainment implications of the KCMP as documented.

f. ARSTAF is responsible for assessing the KCMP documentation and providing its comments and recommendation for approval or disapproval and justification for use within the Army key management system from a strategic planning, prioritization, and guidance perspective for the development and implementation of solutions that satisfy operational and generating force requirements across the full spectrum of Joint operations.

g. DCS, G–3/5/7, as a member of the ARSTAF, will provide review and comments regarding the operational and generating force impact of the KCMP documentation.

h. NSA, as the national manager for protection of NSS and NSI, is the developer and operator of the key management capability used to protect all NSS and NSI. NSA is the determining authority for conformance of KCMPs and key specifications that will require keys from their infrastructures, and must explicitly approve all KCMPs and key specifications via a support agreement prior to supplying any keys for supported systems.

i. Key and certificate management stakeholders community of interest (COI) is responsible for validating 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 and Services, and will provide review and comments from that perspective on the KCMP.

C–4. Process

a. PEOs, programs or SOs inform CERDEC of the need for keys, certificates, or other security products (for example, PINs, passwords, and so forth) for a particular product, solution, or system.

b. CERDEC performs an initial assessment of the product or solution's key and certificate management (KCM) concept and approach. CERDEC notifies CIO/G–6, Cybersecurity Directorate (SAIS–CB) of the KCM approach and the need for technical support and an initial Stakeholder meeting (optional—if the initial assessment indicates a sufficiently complete and supportable approach, an initial meeting may not be required of all programs or solutions). CIO/G–6, Cybersecurity Directorate (SAIS–CB) assigns an Army KCM resource to serve as an internal Army technical KCM subject matter expert (SME) resource to assist the solution's team in their KCMP development.

c. After notification and assessment of initial meeting need, CIO/G–6, Cybersecurity Directorate (SAIS–CB) coordinates any needed meeting within 30 days with Army KCM stakeholders, to include Army key production, operations, sustainment, supporting, and engineering organizations (for example, CIO/G–6, Cybersecurity Directorate (SAIS–CB); DCS, G–2; CERDEC; PL Net E; CSLA key management team; the Program/solution office; and other key organizations as needed (for example, load device or MPMSS PMO(s))). The purpose of the initial meeting or teleconference is to gain an early understanding and awareness of the cryptographic solution being developed and give the solution team and Stakeholders the opportunity to ensure that the solution approach is compliant and supportable by the Army, and if required NSA, infrastructures and operations.

d. Program develops their KCMP with support from the CIO/G–6, Cybersecurity Directorate (SAIS–CB)-identified technical KCM SME.

e. Program submits their developed KCMP to CIO/G–6, Cybersecurity Directorate (SAIS–CB) for review and acceptance. CIO/G–6 will coordinate the Army review by KCMP stakeholders, and if required the NSA. The technical KCM SME works with the Program office to adjudicate and incorporate comments received from the Army stakeholders and the NSA, iterating the review/adjudicating cycle as needed to produce a KCMP that is accepted and approved by CIO/G–6, Cybersecurity Directorate (SAIS–CB), and the NSA if required.

f. After approval, the program office provides CIO/G–6, Cybersecurity Directorate (SAIS–CB) a copy of the final approved version to place in its repository of accepted and approved Army KCMPs.

Note. See figure C–1 for depiction of steps.

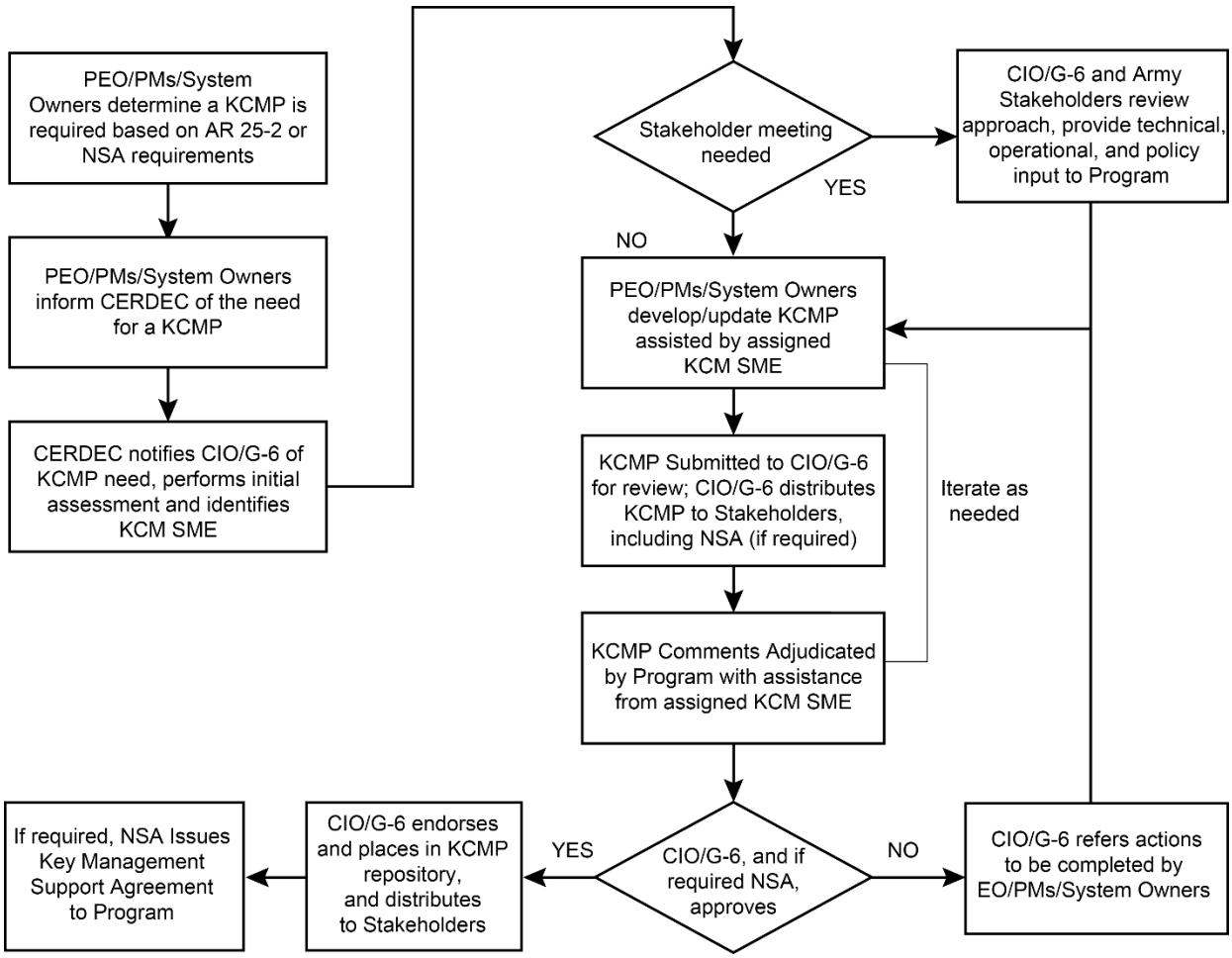

Figure C–1. Army key and certificate management diagram

Appendix D

Army Capability Support Plan Request Process

D–1. Overview

a. This appendix establishes the processes related to the Army Capability Support Plan (ACSP) (see fig D–1). The ACSP is the Army's implementation of the DA mandate to review and validate Army requests for technical services and support from the National Security Agency.

b. This appendix addresses instructions for the ACSP validation and prioritization process.

D–2. Army Information System Security Program Application

This appendix provides guidance on the use of the ISSPA within the DA for all ISSMs/ISSOs/established users and leverages applicable DODDs and DA memorandums and regulations as referenced.

D–3. Administrative requirements

Principal HQDA Officials and Staff, consisting of DCS, G–3/5/7; CIO/G–6; and other appropriate ARSTAF members within their respective areas of function or process will develop, coordinate, manage, and execute action in support of the ACSP.

a. CIO/G–6, Cybersecurity Directorate (SAIS–CB)—

(1) Serves as the functional proponent for ACSP.
(2) Provides program oversight for Army program submissions.
(3) Reviews, and coordinates Army input into support documents (for example, questionnaires).
(4) Establishes a system that will collect all supporting documentation.
(5) Conducts the ACSP validation process.
(6) Validates and submits urgent ACSP requests for support.
(7) Documents, develops, coordinates, and presents validated submissions.
(8) Provides cryptographic guidance to Army elements consistent with national policy.
(9) Uses the ACSP request to collect all Army NSA support requirements.

b. DCS, G–3/5/7—

(1) Prioritizes and approves request based on operational needs.
(2) Provides guidance and oversight of Army program submissions.
(3) Participates in the CIO/G–6, Cybersecurity Directorate (SAIS–CB) scheduled ACSP ARSTAF teleconference.

c. ARSTAF—

(1) Assists in validation and prioritization process.
(2) Participates in the CIO/G–6, Cybersecurity Directorate (SAIS–CB) scheduled ACSP ARSTAF teleconference.

d. PEOs/PMs/SOs—

(1) Provides all pertinent documentation for new CCEP products being submitted for NSA support.
(2) Performs account management by validating requirements for support.
(3) Validates requirements and forward to CIO/G–6 for approval.

D–4. Army Capability Support Plan process diagram

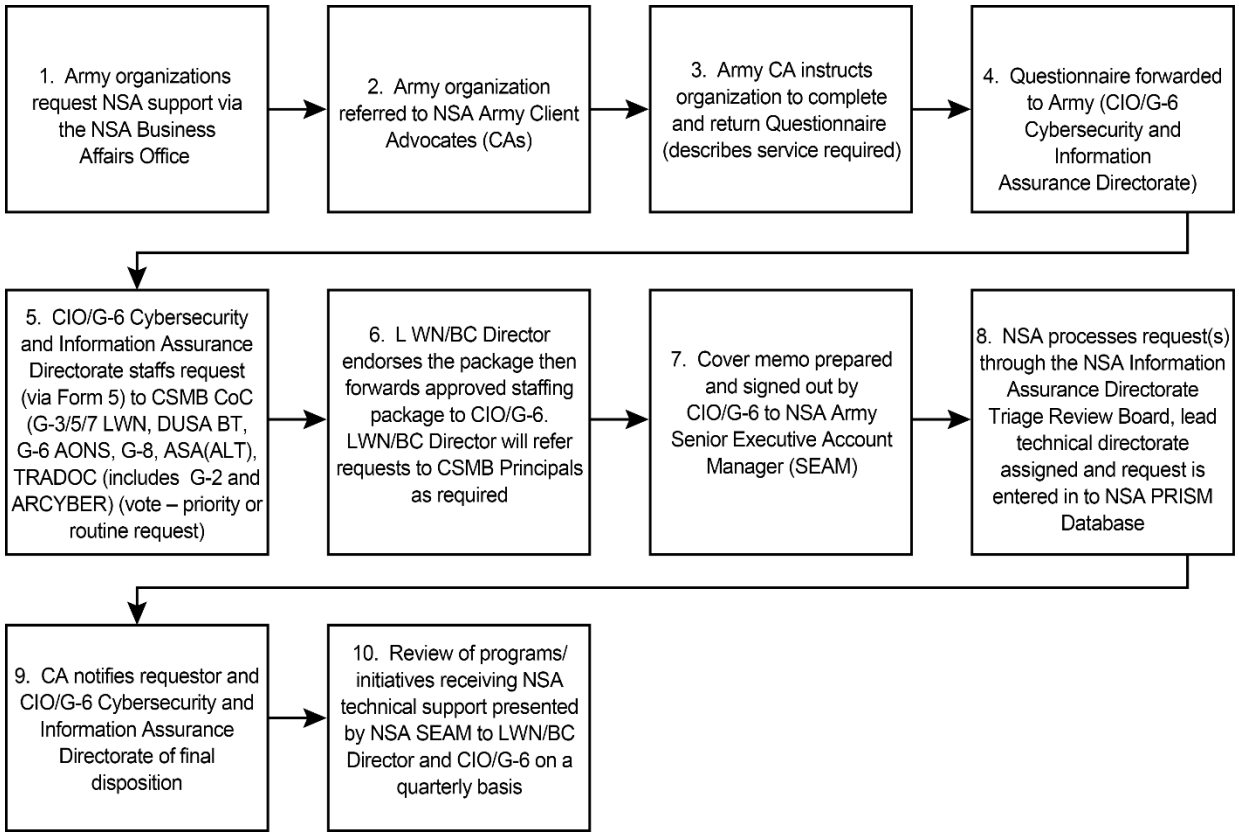

Figure D–1. Army Capability Support Plan process diagram

Appendix E

Army Key Extension Request

E–1. Overview

a. This document establishes the Army's process for submitting a KER in accordance with the CJCSI 6510.02E. This appendix clarifies the process that Army PEOs/Program Managers (PMs)/SOs/Information Assurance Program Managers (IAPMs) or ISSMs and designated approval authorities (DAAs) or authorizing officials (AOs) must adhere to when requesting continued key support for systems that contain an operationally required cryptographic product beyond its last year of use (LYOU), as defined in appendix A, or beyond the cessation of keying material support (cease key date), as outlined in the device specific cryptographic equipment decertification memorandums published by the NSA. Use of key beyond the cease key date is a reportable COMSEC incident.

b. In certain situations, it may not be possible for the Army to implement a replacement or modernization strategy consistent with the guidance and timelines. In these cases, the cognizant DAA/AO can petition the Military Command, Control, Communications, and Computers (C4) Executive Board (MC4EB) by sending a KER to the CIO/G–6, Cybersecurity Directorate (SAIS–CB). Each KER will be processed on a case-by-case basis and must be assessed by the NSA, which will recommend a course of disposition for final review/approval by the MC4EB.

c. Before engaging in the key extension process, Army PEOs/PMs/SOs/IAPMs or ISSMs and DAAs or AOs must recognize degradation of security based on information presented in CJCSN 6510 Series (see app A), or increasing difficulties in providing logistic support to a cryptographic product or system. An analysis of alternatives must be initiated by the appropriate offices, 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 existing system is required. All alternative approaches (including material and non-material solutions; nonmaterial meaning; tactics, techniques and procedures (TTP); and procedural changes) must be fully considered to eliminate or mitigate information security risk to the warfighter system.

d. At a minimum, KERs must be initiated at least one year prior to the LYOU or cease key date.

E–2. Army key extension request

This appendix provides standard practices for all Army PEOs/PMs/SOs/IAPMs or ISSMs and DAAs or AOs to obtain key support for operationally required systems before the cryptographic product arrives at LYOU or cease key date. This will ensure continued use of critical COMSEC assets, as well as compliance with established procedures. It will also prevent possible duplication of effort while ensuring common migration, modernization and interoperability consistent with Army transformation and modernization initiatives. This appendix augments guidelines established in CJCSI 6510.02E. This appendix will be reviewed at least annually and in conjunction with future revisions to CJCSI 6510.02E.

a. Administrative roles and duties requirements.

(1) PEOs/PMs/SOs, along with other COMSEC-related staff members, are responsible for identifying critical replacement and modernization needs and reviewing the guidance provided in the CJCSN 6510 , CJCSI 6510.02E and cryptographic equipment decertification memorandum. PEOs/PMs/SOs will notify the IAPM/ISSM, who will inform the cognizant DAA/AO as soon as he or she identifies equipment that will not be out of the field prior to its LYOU or cease key date. PEOs/PMs/SOs are responsible for developing the KER and forwarding it through the IAPM/ISSM to the cognizant DAA/AO. PEOs/PMs/SOs must also notify the controlling authority (CONAUTH) that provides key material for the system and have the CONAUTH review and sign off on the completed KER. It is recommended that KERs be initiated as soon as a potential need is identified for continued use beyond LYOU or cease key date, to allow time for all parties to collaborate on this effort. At a minimum, KERs must be initiated at least one year prior to the LYOU or cease key date.

(2) DAA/AOs are responsible for reviewing the generated KER, accepting, and mitigating risks associated with the analysis of alternatives and risk analysis processes. NSA will provide a technical risk assessment, Defense Intelligence Agency will provide an assessment of current threats, and the results of these analyses will be provided to allow the DAA/AO to make an informed risk decision. The DAA/AO must understand that accepting risks is recognizing degradation of security based upon CJCSN 6510 requirements. The DAA/AO will sign the KER and forward it to the CIO/G–6, Cybersecurity Directorate (SAIS–CB).

(3) CIO/G–6, Cybersecurity Directorate (SAIS–CB) will serve as the principal advisor to the DAA/AO with respect to Army responsibilities, network security compliance, risk acceptance/approval and KER processing. Furthermore, CIO/G–6, Cybersecurity Directorate (SAIS–CB) will facilitate the formal staffing of the DAA/AO's KER to ARSTAF and forward the approved package to MC4EB via the Joint Staff J6.

(4) ARSTAF is responsible for assessing the KER and providing its recommendation for approval or disapproval and justification to the DAA/AO. It provides strategic planning, prioritization, and guidance for the development and implementation of solutions that satisfy operational and generating force requirements across the full spectrum of Joint operations.

(5) DCS, G–3/5/7, as a member of the ARSTAF, will determine the operational and generating force impact if the system does not receive a key extension, and possible workarounds to reduce this impact.

(6) CIO/G–6, Cybersecurity Directorate (SAIS–CB) will support the Army's KER as submitted and briefed by the SO at the Cryptographic Security Panel (CSP) prior to the package moving forward to the MC4EB for approval.

(7) MC4EB serves as the principal military advisory forum for assessing the Information Technology (IT) aspects of C4 matters, to include Warfighting Mission Area IT Portfolio Management. It informs the Joint Capability Integration Development System; Planning, Programming, Budgeting and Execution Systems; and Defense Acquisition System processes through military advice, assessments, and recommendations regarding the implementation of IT (communication and electronics) solutions. The MC4EB, as defined in CJCSIs 5116.05 and 6510.02E, will approve or deny a DAA/AO's request for continued use on a system of cryptographic products past their published LYOU or cease key date.

b. Memorandum requirements. The KER memorandum must include (see fig E–1)—

(1) The time duration of use of decertified equipment requiring continued key support.

(2) List devices that require continued key support.

(3) List of organizations affected.

(4) Short title, classification, and controlling authority of the keying material required.

(5) List all cryptographic devices by nomenclature or short title affected by this KER.

(6) Intelligence life of data (how long does the information need to be protected, expressed in specific timeframe (hours, days, months, and/or years).

(7) The hardware and/or software issues are preventing the modernization.

(8) Additional information that is pertinent to assisting in assessing the risk of the KER.

(9) The plan of action and milestones (POA&M) that includes an architecture overview of the systems and networks, a fielding plan, schedule, and programmatic funding profile.

(10) Certification 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.

Note. KERs are classified SECRET and must be handled and distributed via the secure internet protocol router network (SIPRNET).

Note. This is a sample format. Once filled in, the memorandum will be classified SECRET//NOFORN and must only be stored, accessed, and distributed via the SIPRNET.

DEPARTMENT OF THE ARMY
ORGANIZATION
STREET ADDRESS
CITY STATE ZIP

(*Organization Office Symbol*)
(*Date*)

MEMORANDUM THRU:

CIO/G-6 Cybersecurity Directorate, Attn. COMSEC Division, 5850 23rd Street, Room 317, Ft. Belvoir, VA 22060-5832
Assistant Deputy Chief of Staff, G-3/5/7, 400 Army Pentagon, Washington, DC 20310-0400

For: Military Communications-Electronics Board (MC4EB), Joint Staff J-6 Office,
6000 Joint Staff, Pentagon, Washington, DC 20318-6000

SUBJECT: Key Extension Request (KER) for National Security System (NSS) and Continued Key Management Support.

1. The (Program Office) requests continued key management support from NSA until (month year) for (cryptographic device). 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) (i.e., Designated Approving Authority (DAA)) and Operational Mission Data Owner) acknowledges receipt and review of (CED memoranda) and that the NSA will not waive stated decertification commitments. DAA/AO willingly accepts all risk associated with the continued operations of the system(s) listed in line item number two below.

2. List and 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, COCOMs, and Allied/Coalition partners affected by this KER.

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. How long does the data owner require the data to be protected from compromise once it has been transmitted over the network (i.e., hours, days, months, and years)?

b. What is the speed that information is transmitted over the network (i.e., 2.4Kbps, 16Kbps, 1Mbps, 5Mbps, etc.)?

Figure E–1. Army key extension request memorandum

(*Organization Office Symbol*)
SUBJECT: Key Extension Request (KER) for National Security System (NSS) and Continued Key Management Support.

c. What RF spectrum is the information transmitted over the network (i.e., LF, VLF, HF, UHF, EHF, etc.)?

d. How often is the cryptographic device and system setting in a ready state connected with the distant end waiting to exchange data (i.e., 24/7, 12/7, 1 day a week, 5 days a week, etc.)?

e. How often is the information actually being transmitted from the system across the network (i.e., constant broadcast, 10 minute-bursts, 2-hour transmissions, 3-times a day, etc.?

7. What hardware and/or software issues are preventing the modernization of these systems listed above in line item number 2, in accordance with the timelines published in (CED memoranda)? Include summary of your Analysis of Alternatives (AoA).

8. Provide any additional information that is pertinent to assisting in assessing the risk of the KER (e.g., new replacement equipment for this decertified device is not releasable to Allied/Coalition Partners). Also consider factors that mitigate the risk.

9. Provide the Program Office Plan of Action and Milestones (POA&M) for achieving compliance with cryptographic modernization in accordance with NSA/CSS 3-9 policy. 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.

10. 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)?

11. The following information must be completed for the listed individuals. They are Program Manager / System Owner, Information Assurance Program Manager, Controlling Authority,

Program Manager / System Owner

a. Rank/Grade:
b. Name (Last, First MI):
c. Command/Agency:
d. City, State, Zip Code:
e. Country:
f. Telephone:
g. Unclassified Email:
h. Classified Email:

Figure E–1. Army key extension request memorandum—Continued

(*Organization Office Symbol*)
SUBJECT: Key Extension Request (KER) for National Security System (NSS) and Continued Key Management Support.

Information Assurance Program Manager

a. Rank/Grade:
b. Name (Last, First MI):
c. Command/Agency:
d. City, State, Zip Code:
e. Country:
f. Telephone:
g. Unclassified Email:
h. Classified Email:

Controlling Authority

a. Rank/Grade:
b. Name (Last, First MI):
c. Command/Agency:
d. City, State, Zip Code:
e. Country:
f. Telephone:
g. Unclassified Email:
h. Classified Email:

(*Signature Block of Designated Approving Authority*)

Figure E–1. Army key extension request memorandum—Continued

c. Key extension request process. The process for KERs is diagrammed in figure E–2. The following paragraphs describe each step in detail:

(1) Decertification letter conflicts with operational requirement. PEOs/PMs/SOs, along with other COMSEC related staff members, are responsible for identifying critical replacement and modernization needs and for reviewing the guidance provided in the CJCSN 6510, CJCSI 6510.02E, and cryptographic equipment decertification memorandum. If it is determined that no replacement or effective workaround is readily available, PEOs/PMs/SOs must prepare a KER and coordinate with the CONAUTH and IAPM/ISSM to inform the DAA/AO.

(2) DAA/AO. If a DAA/AO, in conjunction with the combatant command (COCOM) and/or program of record (POR), identifies a compelling operational need to continue use of a cryptographic system past its LYOU or cease key date, the DAA/AO must decide to accept the risk and submit a KER in order to continue to receive key support for the decertified system. The DAA/AO will submit the KER through CIO/G–6, Cybersecurity Directorate (SAIS–CB). This request will include the rationale/justification for keeping the affected system in operation. The DAA/AO will also identify any TTPs that may be applicable to augment Information Assurance (IA) protection and mitigation. The DAA/AO's analysis of

alternatives will be used to determine and describe the resulting risk, establish criteria for risk acceptance (when applicable), and identify steps taken to mitigate risk and minimize negative consequences.

(3) CIO/G–6, Cybersecurity Directorate (SAIS–CB). The CIO/G–6, Cybersecurity Directorate (SAIS–CB) will serve as the principal advisor to the DAA/AO with respect to Army network security compliance, risk acceptance/approval and KER processing. If the KER is technically compliant, CIO/G–6, Cybersecurity Directorate (SAIS–CB) will facilitate its staffing to appropriate members of the ARSTAF for comments and recommendations.

(4) ARSTAF decision point. ARSTAF members, overseeing synchronization activities that strategically inform, enable and direct force generation processes supporting the development and delivery of integrated capabilities over time, will assess the KER and provide their approval or disapproval recommendation and justification to the DAA/AO for continued use on a system of cryptographic products past their LYOU or cease key date. As a member of the ARSTAF, DCS, G–3/5/7 will determine the operational and generating force impact if the system does not receive a key extension, and possible workarounds to reduce this impact.

(a) ARSTAF request denied. If the ARSTAF does not recommend approval of the KER, the request will be returned to the DAA/AO for termination of request or with actions to be completed. The DAA/AO will adjudicate and modify the KER based upon the ARSTAF comments and identify additional alternatives and/or capabilities to protect the information in the affected communications system. The updated KER will be resubmitted to the CIO/G–6, Cybersecurity Directorate (SAIS–CB) for recommendations/analysis and re-staffing. Cryptographic system use will terminate by the end-of-use date until resolution of the KER, unless NSA formally agrees to provide continued key support pending outcome of the KER.

(b) ARSTAF request approved. If ARSTAF recommends approval of the KER, the CIO/G–6, Cybersecurity Directorate (SAIS–CB) will forward the request to the CIO/G–6 for endorsement. The endorsed package will be sent to the MC4EB for approval via Joint Staff J6, and the request will be processed per CJCSI 6510.02E. NSA will review the KER, 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. The NSA assessment and its accompanying recommendations will be provided to the MC4EB and DAA/AO for direction and action. The CIO/G–6, Cybersecurity Directorate (SAIS–CB) will support the SO in obtaining approval from the CSP. After approval by the CSP, the KER will be forward to the MC4EB.

(5) MC4EB approval/disapproval. If the MC4EB approves the request, the CIO/G–6, Cybersecurity Directorate (SAIS–CB) will inform the DAA/AO of any required mitigating actions to implement the solution. CIO/G–6, Cybersecurity Directorate (SAIS–CB) will send approval to the following COMSEC stakeholders, for their continued support: CONAUTH, CSLA, PL NET Es. If the MC4EB disapproves the request, key support and the cryptographic system's use will be terminated by the end-of-use date.

(a) DAA/AO follow-up reporting. This report will address mitigating actions and any significant issue that could impact the POA&M. The CIO/G–6, Cybersecurity Directorate (SAIS–CB) will review and forward the report to the appropriate offices. The report must use the KER Memorandum template as the basis for the information being sought.

(b) Frequency of follow-up reporting. The MC4EB direct the time frame for the report.

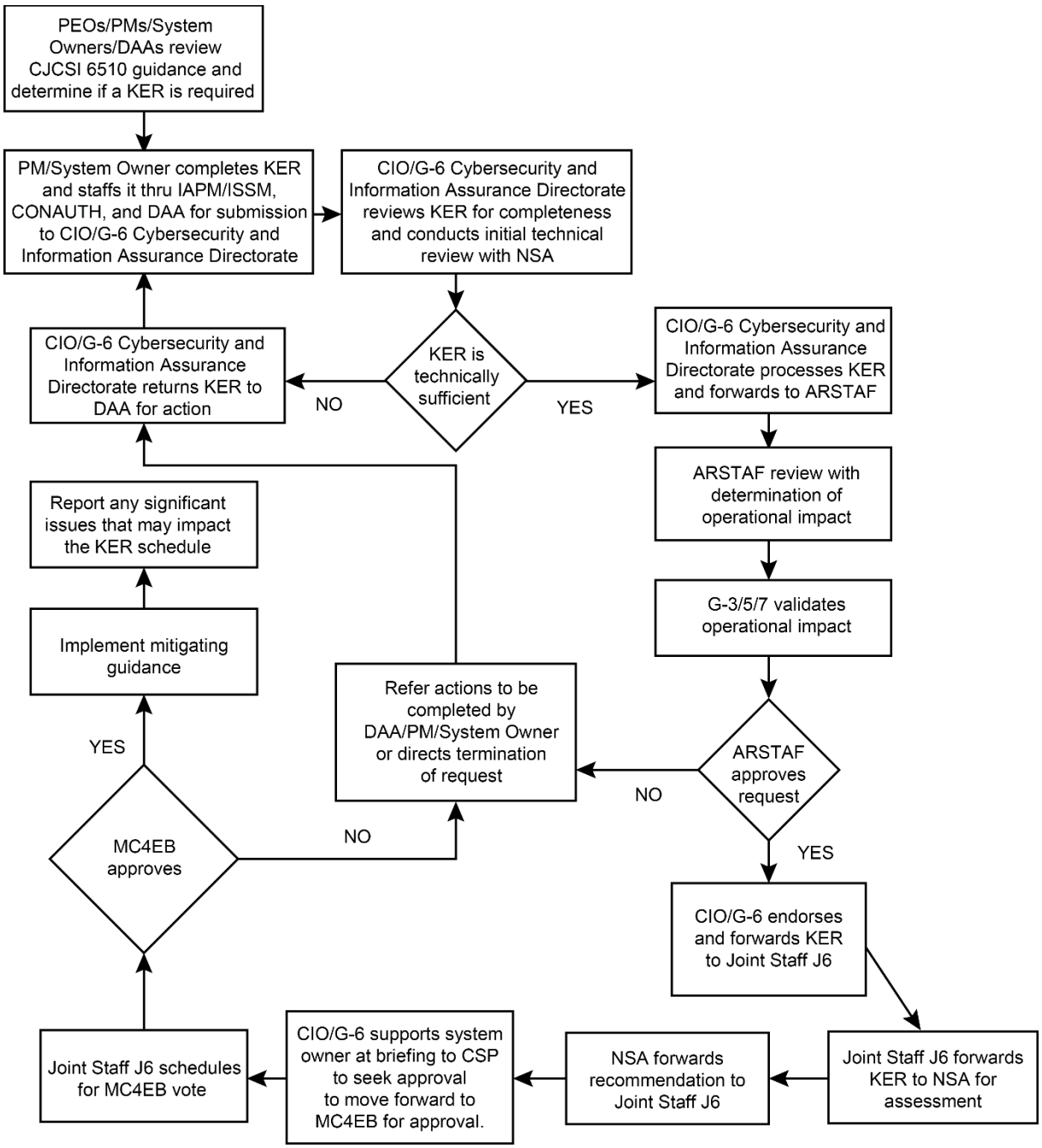

Figure E–2. Army key extension request process diagram

Glossary

Section I

Abbreviations

ACOM
Army command

ACSP
Army Capability Support Plan

AD
architectural diagram

AES
advanced encryption standard

AISSP
Army Information Systems Security Program

AO
authorizing official

AoA
Analysis of Alternatives

AR
Army regulation

ARSTAF
Army Staff

ASA (ALT)
Assistant Secretary of the Army (Acquisition, Logistics and Technology)

ASCC
Army service component command

CCEP
Commercial COMSEC Endorsement Program

CCI
controlled cryptographic item

CE
Computing Environment

CERDEC
Communications Electronics, Research and Development Engineering Center

CHVP
cryptographic high value property

CIO
Chief Information Officer

CJCSI
Chairman of the Joint Chief of Staff Instruction

CMVP
Cryptographic Module Validation Program

CNSS
Committee on National Security Systems

CNSSI
Committee on National Security Systems Instruction

CNSSP
Committee on National Security Systems Policy

COMSEC
communications security

CONAUTH
controlling authority

CS
Cybersecurity

CSfC
Commercial Solutions for Classified

CSLA
Communications Security Logistics Activity

CUI
controlled unclassified information

DA Pam
Department of the Army pamphlet

DAA
designated approval authority

DCS
Deputy Chief of Staff

DES
Data Encryption Standard

DISA
Defense Information Systems Agency

DOD
Department of Defense

DODD
Department of Defense Directive

DODI
Department of Defense Instruction

DODM
Department of Defense Manual

DRU
direct reporting unit

FIPS
Federal Information Processing Standard

HQDA
Headquarters, Department of the Army

IAD
Information Assurance Directorate

IS
Information System

ISSM
information systems security manager

ISSO
information systems security officer

ISSPA
Information Systems Security Program Application

IT
Information Technology

KCM
key and certificate management

KCMP
key and certificate management plan

KER
key extension request

KMI
key management infrastructure

LWN
Land Warfighter Network

LYOU
last year of use

MC4EB
Military Command, Control, Communications, and Computers (C4) Executive Board

MDEP
management decision package

MTOE
modified table of organization and equipment

NIAP
National Information Assurance Partnership

NIST
National Institute of Standards and Technology

NSA
National Security Agency

NSI
national security information

NSS
national security systems

PEG
program evaluation group

PEO
program executive officer

PL NET E
project lead network enablers

PM
program manager

POA&M
plan of action and milestones

RED
request for expedited delivery

SAP
Special Access Program

SCI
sensitive compartmented information

SIPRNet
secure internet protocol router network

SO
system owner

TCM
TRADOC capability manager

TDA
table of distribution and allowances

TTPs
Tactics, Techniques and Procedures

USC
United States Code

Section II

Terms
This section contains no entries.