

Committee on National Security Systems

**CNSS Instruction No. 4031
16 February 2012**



**Cryptographic High Value
Products**





NATIONAL MANAGER

FOREWORD

1. The Committee on National Security Systems Instruction (CNSSI) No. 4031, “Cryptographic High Value Products,” establishes the category of Cryptographic High Value Product (CHVP) as designated by NSA, to secure SECRET and Below National Security Systems. CHVPs require less administrative burden and control than the existing categories of Controlled Cryptographic Items (CCI) and classified products.
2. CNSSI No. 4031 is effective upon signature.
3. Additional copies of this instruction may be obtained from the Secretariat or the Committee on National Security Systems website – www.cnss.gov.

FOR THE NATIONAL MANAGER:

/s/
DEBORA A. PLUNKETT

Cryptographic High Value Products

SECTION I – BACKGROUND AND PURPOSE..... 1
 SECTION II – APPLICABILITY AND SCOPE 1
 SECTION III – AUTHORITY 2
 SECTION IV – RESPONSIBILITIES 2
 SECTION V – CONTROL REQUIREMENTS 1
 SECTION VI – EXCEPTIONS 5
 ANNEX A – SPONSORSHIP OF U.S. ENTITIES FOR USE OF CHVPs A-1
 ANNEX B - DEFINITIONS..... B-1
 ANNEX C - REFERENCES C-1

SECTION I – BACKGROUND AND PURPOSE

1. In order to meet the objectives of the U.S. Government, classified and sensitive information must be shared between and among federal government departments, agencies, and other U.S. and foreign entities. This information is transmitted over National Security Systems (NSSs). National Security Agency (NSA)-approved cryptography is required to protect NSSs and the information that resides therein. A Cryptographic High Value Product (CHVP) enables the use of public standards for cryptographic protocols and algorithm interoperability, per Committee on National Security Systems (CNSS) Policy No. 15 (reference a).

2. The category of CHVP is designated by NSA to secure certain NSSs, but with less administrative burden and control than required by the existing categories of Controlled Cryptographic Items (CCI) and classified products.

3. CHVPs may be approved to protect information up to the SECRET level when communicating with other NSA-approved devices. Each product must be used commensurate with its certification/approval letter signed by the NSA IA Director, acting on behalf of the National Manager, and its operational security doctrine.

4. This document defines CHVPs and specifies the requirements for their use, control, safeguarding, and disposition.

SECTION II – APPLICABILITY AND SCOPE

5. The requirements of this instruction apply to all departments and agencies of the U.S. Government using CHVPs. Use of a CHVP for SECRET and Below applications by entities outside the U.S. Government constitutes agreement by that entity to be bound by the applicable provisions of this instruction. TOP SECRET information must be protected by means approved by NSA for that level of classification, normally either by use of classified or Controlled Cryptographic Item (CCI) equipment.

6. Procurement and use of CHVPs to safeguard classified information by foreign governments and international organizations recognized by the U.S. Department of State may only occur subsequent to the completion of the National Security Telecommunications and Information System Security Policy (NSTISSP) No. 8 (reference b) release procedures. Contact the NSA Client Advocacy Office on 410-854-4790 to begin the NSTISSP No. 8 process.

7. When the requirements or terms of this instruction appear to conflict with the requirements or terms of any other national-level issuance, identify this conflict and request guidance through organizational channels from DIRNSA, ATTN: IA Policy and Doctrine Division, 9800 Savage Road, Suite 6749, Fort George G. Meade, MD 20755-6749.

SECTION III – AUTHORITY

8. This instruction is issued pursuant to National Security Directive No. 42, National Policy for the Security of National Security Telecommunications and Information Systems (reference c). It applies to all Federal Departments and Agencies, including their supporting contractors that operate, use, or manage NSS.

9. Nothing in this policy should be interpreted as altering or superseding the existing authorities of the Director of National Intelligence.

SECTION IV – RESPONSIBILITIES

10. The Director, National Security Agency (DIRNSA), is responsible for:

- a. Approving the products that meet the qualifications to be designated CHVPs and publishing a complete listing of products that have been designated CHVPs;
- b. Developing, coordinating, and distributing operational security doctrine applicable to CHVPs;
- c. Promulgating specific guidelines to be used during the development and manufacture or assembly of all CHVPs and ensuring these guidelines are provided to affected contractors and vendors;
- d. Providing management and oversight for cryptographic key and certificate management to include approval of key generation and management products, certificate management products, key management providers, and certificate management providers when used by CHVPs for the protection of National Security Systems.
- e. Providing keying material for CHVPs used to protect National Security Systems.

11. Heads of Federal Departments and Agencies are responsible for:
- a. Obtaining keying material from NSA or other NSA-approved sources, and managing such keying material in accordance with operational security doctrine;
 - b. Sponsoring U.S. entities for use of CHVPs and associated keying material (see ANNEX A);
 - c. Training users, including sponsored U.S. entities, in the proper procedures for use, control, and accounting of CHVPs and associated keying materials;
 - d. Subject to paragraph 6, obtaining approval for use of CHVPs for interoperability with foreign governments and international organizations;
 - e. Reporting incidents involving CHVPs and associated keying material as required by paragraph 22; and
 - f. Ensuring CHVPs are used according to the equipment operational security doctrine. This includes ensuring that CHVP devices only communicate with other NSA-approved devices.

SECTION V – CONTROL REQUIREMENTS

12. Keying Material.
- a. Keying material for NSSs must be obtained from NSA or from other NSA-approved sources. The rules for handling and accounting for COMSEC keying material found in CNSSI No. 4005 (reference d) must be followed.
 - b. Keying material for CHVPs may be classified up to SECRET. CHVPs are not approved to protect TOP SECRET information and must not be filled with TOP SECRET keying material. If TOP SECRET key is inadvertently loaded, the equipment must be zeroized immediately and a COMSEC incident report filed in accordance with NSTISSI No. 4003 (reference e).
 - c. For non-national security applications, procurement of keying material from NSA or NSA-approved sources is not required.
13. Unkeyed CHVPs are unclassified and must be controlled in a manner no less stringent than established by the individual departments, agencies, or organizations for high dollar value/sensitive material (e.g., computers or military radios). In addition, protective measures employed must reasonably protect against attempts by individuals to gain unauthorized access to CHVPs.

14. Keyed CHVPs must be protected at the same level as the keying material. In addition, protection must be consistent with the classification of the key contained in the equipment, its purpose, and/or the sensitivity of the information or function being protected by the key. If a keyed CHVP becomes inoperable and cannot be zeroized (zeroization has not been confirmed), the CHVP must be treated as keyed.

15. Security Clearances.

a. A security clearance or Limited Access Authorization (see DoD 5200.2-R section C3.4.3 (reference f)) or equivalent, to the classification level of the keying material and/or sensitivity of the protected information is required for access to CHVPs that contain classified keying material.

b. Provided appropriate security measures have been taken, and an individual has been granted access by a U.S. Government cognizant security authority to all the classified information being protected by a CHVP and its keying material, then that individual is considered to have the proper security clearance for access to the keyed CHVP.

16. Cryptographic Access Program (CAP). Only persons having an appropriate security clearance (to the level of the keying material) and need-to-know will handle and/or load RED (unencrypted) keying material into a CHVP. In addition, personnel routinely handling SECRET keying material designated CRYPTO must have a cryptographic access briefing. See CNSSP No. 3 (reference g) for details on the cryptographic access program. Keying material must be obtained from a formal COMSEC account as prescribed in CNSSI No. 4005 (reference d).

NOTE: Personnel handling only CONFIDENTIAL or UNCLASSIFIED keying material (e.g. CONFIDENTIAL CRYPTO or UNCLASSIFIED CRYPTO) are not required to have a cryptographic access briefing.

17. Access.

a. Notwithstanding paragraph 5.a. of CNSSP No. 14, “National Policy Governing the Release of Information Assurance (IA) Products and Services to Authorized U.S. Persons or Activities that are Not a Part of the Federal Government” (reference h), the cognizant security authority may only grant access to a keyed CHVP to U.S. persons in accordance with paragraph 15.b above. (For criteria on which organizations may obtain or use CHVPs, see paragraph 5 above.) As defined in the International Traffic in Arms Regulations (reference i), U.S. persons include U.S. citizens, whether by birth or naturalized; lawful permanent residents; and any business entity that is incorporated to do business in the U.S. (22 C.F.R. § 120.15 (reference j)).

b. Access to CHVPs by any non-U.S. person must be authorized in accordance with reference b and meet any applicable security requirements that would be imposed, in accordance with paragraph 15.b above, on a U.S. person.

c. The decision to grant access should be made in conjunction with the Authorizing Official (AO) (formerly called the Designated Approving Authority (DAA)) of the information system incorporating the CHVP.

18. Preparation for Unattended Shipment.

a. Unkeyed CHVPs should be packaged for shipment in any manner that is approved for the transport of similar high dollar value items (e.g., computers or military radios), and that provides evidence of tampering.

b. If the CHVP includes a split key process such as a cryptographic ignition key (CIK) or a Personal Identification Number (PIN) that activates the equipment, then the CHVP and CIK/PIN must be packaged and shipped separately.

NOTE: When a CIK is part of the equipment configuration and removed from the CHVP, the equipment is considered unkeyed. When a PIN is part of the equipment design and it is in a locked state, the equipment is considered unkeyed.

c. If it is necessary to ship a keyed CHVP (i.e., it contains keying material not protected by a CIK/PIN that has been shipped separately), the CHVP must be packaged and shipped in accordance with the classification of the keying material contained.

19. Transportation of CHVPs.

a. CHVPs must only be shipped to an organization/activity authorized to possess CHVP in accordance with the authorization criteria in paragraphs 5, and 6 above.

b. CHVPs must be prepared for shipment as set forth in paragraph 18, above.

NOTE: Paragraphs 18 and 19 deal with unattended shipment of products. Hand carrying of products, especially mobile products designed for portability, will be accomplished according to local security policy.

c. Transportation of CHVPs containing classified keying material must be in accordance with CNSSI No. 4005 (reference d).

20. Inventory/Control and Tracking Requirements for CHVPs.

a. Shipping and receipt of CHVP(s) may be performed by the authorized logistics or COMSEC asset management authority of an organization designated by the recipient.

b. Life Cycle Usage. The applicable logistics or COMSEC asset management authority should maintain records for actions, activities, and disposition of CHVPs.

c. Accounting. CHVPs may be inventoried, controlled, and tracked in agency or departmental Accountable Property Systems of Record or COMSEC asset management systems.

Keying material must be controlled and safeguarded in accordance with operational security doctrine. Accountable property or COMSEC asset management records shall be kept current and reflect the current status, location, and condition of the asset until authorized disposition of the property occurs. These records shall provide a complete trail of all transactions suitable for audit and are the authoritative source for validating the existence and completeness of an asset.

NOTE: All keying material used to secure NSSs must be handled and accounted for IAW CNSSI No. 4005 (reference d) as set forth in paragraph 12.a above.

21. Maintenance. Only qualified individuals may maintain CHVPs. Maintenance of CHVPs must be in accordance with NSTISSI No. 4000, Communications Security Equipment Maintenance and Maintenance Training (reference k), which is hereby expanded to apply to CHVPs.

22. Incidents. Incidents involving CHVPs must be handled as follows:

a. DIRNSA, the responsible key management authority, the appropriate cognizant security authority, and the Department/Agency COMSEC Incident Monitoring Activity must be notified of those incidents where:

(1) A keyed CHVP was shipped in a manner that did not meet the requirements of paragraphs 18 and 19 in accordance with the classification of its keying material.

(2) A keyed CHVP is lost.

(3) There is evidence or proof of theft, tampering, or sabotage of keyed CHVPs, or unauthorized access to keying material.

b. DIRNSA and the appropriate cognizant security authority must be notified of those incidents when there is evidence or proof of theft, tampering, or sabotage of unkeyed CHVPs.

c. The responsible security authority specified by Departments/Agencies shall be notified of the following CHVP Incidents that are not reportable to DIRNSA for appropriate administrative action:

(1) An unkeyed CHVP is lost.

(2) There is evidence of possible tampering with, or unauthorized access to or modification of an unkeyed CHVP.

(3) There are indications of known or suspected theft of an unkeyed CHVP.

23. Disposition and Destruction.

a. Routine destruction of unkeyed CHVPs should be accomplished as directed by the head of the department, agency, or organization or his/her designee.

b. CHVPs that are keyed must be zeroized (positively erased) prior to destruction.

c. CHVPs that are unusable and may contain keying material must be treated as a keyed device in accordance with paragraph 14 above. Such equipment must be forwarded for disposition through department, agency, or organization channels to the organizational point described in the approved operational security doctrine, or to a point specified by DIRNSA, IA Life Cycle Support 9800 Savage Road Suite 6718, Fort George G. Meade, MD 20755-6718.

SECTION VI – EXCEPTIONS

24. If any organization is unable to satisfy any of the requirements set forth in this instruction, that activity must request an exception, through Department/Agency channels, from the National Manager (DIRNSA, ATTN: IA Policy and Doctrine Division). Non-federal entities must request exceptions through the sponsoring U.S. department or agency.

ANNEX A – SPONSORSHIP OF U.S. ENTITIES FOR USE OF CHVPs

1. Applicability

a. This annex is applicable to U.S. Government departments and agencies with a requirement to use CHVPs to communicate national security information securely with U.S. entities.

b. The routine use of CHVPs by U.S. entities for operations outside of the United States and its territories must be vetted in accordance with national, departmental, Department of Defense, Joint Chiefs of Staff, or Department of State requirements.

c. The routine use of CHVPs by U.S. Government contractors must be in accordance with requirements of the National Industrial Security Program Operating Manual (NISPOM) (reference 1).

2. Process. For use of CHVPs by U.S. entities, as identified in paragraphs 1.b and 1.c above, the federal government sponsor will:

a. Obtain approved CHVP equipment from an NSA-approved source.

b. Order the keying material required from NSA or other approved source and control the keying material in accordance with CNSSI No. 4005 (reference d). The federal government sponsor will serve as the controlling authority for the keying material obtained for this requirement.

c. Execute an agreement with the U.S. entity wherein the U.S. entity acknowledges its responsibilities for the protection of national security information and for the CHVP and associated keying material.

d. Load keying material in electrical form into the CHVP used by the U.S. entity that does not have the access privilege to do it itself.

e. Manage the process of obtaining security clearances (when required), for the individuals requiring access to classified national security information.

f. Train the users in the use of the CHVP and associated control and reporting requirements.

ANNEX B - DEFINITIONS

The definitions contained in CNSSI No. 4009 (reference m) apply to this policy. Additional definitions of specialized terms unique to this policy are:

a. Cognizant Security Authority. That entity designated by the head of a U.S. Government department, agency or organization charged with responsibility for all physical, technical, personnel, and information security matters affecting a particular organization, who will oversee and manage CHVPs within their organization.

NOTE: Within an organization, there may be a hierarchy of cognizant security officers/authorities existing at a variety of echelons (e.g., a specific geographical area; a specific military base or activity, etc.) with each cognizant security official/ authority having sole jurisdiction within that area or activity. (Source: CNSSI No. 4005 (reference d).)

b. Composed Commercial Solution. Two or more commercial IA products layered together to address the security requirements of an operational use case according to NSA guidance. A composed solution, once approved by NSA, may take the place of a single certified Government-off-the-Shelf (GOTS) IA product to provide the confidentiality and/or other security services necessary to protect National Security Systems.

c. Controlled Cryptographic Item (CCI). Secure telecommunications or information system, or associated cryptographic component, that is unclassified and handled through the COMSEC Material Control System (CMCS), an equivalent material control system, or a combination of the two that provides accountability and visibility. Such items are marked “Controlled Cryptographic Item,” or, where space is limited, “CCI.” (Source: CNSSI No. 4009 (reference m).)

d. Cryptographic High Value Products (CHVPs). NSA-approved products incorporating only UNCLASSIFIED components and UNCLASSIFIED cryptographic algorithms. This does include commercial off-the-shelf (COTS) products approved by NSA, but does not include composed commercial solutions or their components, unless an individual component has been approved as a CHVP. Unkeyed CHVPs are not classified or designated as Controlled Cryptographic Items (CCIs). Examples of CHVPs include the IPS-250 and the RF-310M-HH.

e. Incident. Occurrence that potentially jeopardizes the security of COMSEC material or the secure electrical transmission of national security information or information governed by 10 U.S.C. Section 2315. (Source: CNSSI No. 4009 (reference m).) This includes CHVPs and supporting COMSEC materials.

f. Keyed CHVP. CHVP with operational keying material installed, and the ability to provide confidentiality or other security services.

g. Keying Material. Key, code, or authentication information in physical, electronic, or magnetic form. (Source: CNSSI No. 4009 (reference m).)

h. Unkeyed CHVP. CHVP that contains no keying material capable of being activated (i.e., an unkeyed CHVP could have no keying material loaded or it may have keying material loaded but the key activating device or information is not present).

i. U.S. Entity. U.S. persons or activities that are not part of the federal government (hereinafter referred to collectively as U.S. entities). "U.S. entity" includes:

(1) State, local, or tribal governments;

(2) State, local, and tribal law enforcement and firefighting entities;

(3) public health and medical entities;

(4) regional, state, local, and tribal emergency management entities, including State Adjutants General and other appropriate public safety entities; or

(5) private sector entities serving as part of the nation's Critical Infrastructure/Key Resources. (Executive Order 13526 (reference n). See also CNSSP No. 14 (reference h), paragraph 1.)

ANNEX C - REFERENCES

The requirements of the following publications apply to this instruction to the extent specified herein:

- a. CNSSP No. 15, "National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems," dated March 2010.
- b. NSTISSP No. 8, "National Policy Governing the Release of Information Systems Security (INFOSEC) Products or Associated INFOSEC Information to Foreign Governments," dated 13 February 1997.
- c. National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," dated 5 July 1990.
- d. CNSSI No. 4005, "Safeguarding Communications Security (COMSEC) Facilities and Materials," dated 22 August 2011.
- e. NSTISSI No. 4003, "Reporting and Evaluating COMSEC Incidents," dated December 1991.
- f. DoD 5200.2-R, "Personnel Security Program Regulation," dated January 1987.
- g. CNSSP No. 3, "National Policy on Granting Access to U.S. Classified Cryptographic Information," dated October 2007.
- h. CNSSP No. 14, "National Policy Governing the Release of Information Assurance (IA) Products and Services to Authorized U.S. Persons or Activities that are Not a Part of the Federal Government," dated November 2002.
- i. International Traffic in Arms Regulations (ITAR), dated April 2010.
- j. Title 22, U.S. Code of Federal Regulations (22 C.F.R).
- k. NSTISSI No. 4000, "Communications Security Equipment Maintenance and Maintenance Training," dated January 1998.
- l. National Industrial Security Program Operating Manual, dated 28 February 2006.
- m. CNSSI No. 4009, "National Information Assurance (IA) Glossary," dated April 2010.

n. Executive Order 13526, “Classified National Security Information,” dated 29 December 2009.

In addition, reference c above authorizes the Director, National Security Agency (DIRNSA), to be the National Manager for National Security Systems, and the following document sets forth DIRNSA’s role for setting standards for National Security Systems.

o. Executive Order 12333, “United States Intelligence Activities,” as amended 30 July 2008.