

CNSSP No. 19 10 June 2013

Governing the Use of **High Assurance Internet Protocol Encryptor (HAIPE) Products**



CHAIR

FOREWORD

1. The communication infrastructure of the U.S. Government and its partners are heavily reliant upon network communications. Legacy government-owned and operated circuit switched communication channels are being replaced with packet switched infrastructures. National Security System (NSS) users now leverage commercial and foreign public Internet Protocol (IP) infrastructures, which provide real-time services and a converged transport infrastructure for data applications. The interoperability of network-layer encryption devices is vital to enabling net-centric capabilities, while maintaining end-to-end protection of NSS traffic. The High Assurance Internet Protocol Encryptor Interoperability Specification (HAIPE-IS) defines requirements for a modular suite of traffic protection, networking, and management features that provide secure interoperability between users, content repositories, and net-centric enterprise services. This policy supersedes CNSS Policy 19, "National Policy Governing the Use of High Assurance Internet Protocol Encryptor (HAIPE) Products," dated February 2007.

2. This policy provides guidance for the procurement of IP encryption products for Fiscal Year 2013 and beyond.

3. In accordance with the Federal Information Security Management Act (FISMA) of 2002, the Committee on National Security Systems (CNSS) Secretariat has initiated an Issuance Compliance Process for reporting annual status of Department and Agency implementation of new/revised CNSS Issuances.

4. Additional copies of this policy may be obtained from the Secretariat or at the CNSS website: <u>www.cnss.gov</u>.

/s/ Teresa M. Takai

NATIONAL POLICY GOVERNING THE USE OF HIGH ASSURANCE INTERNET PROTOCOL ENCRYPTOR (HAIPE) PRODUCTS

SECTION I – PURPOSE

1. This Policy establishes the criteria for the acquisition and use of HAIPE products to protect National Security Systems (NSS) and the information therein. Such products must adhere to certain standards and requirements to ensure the appropriate level of functionality, interoperability, and security among such devices.

2. The purchase of all HAIPE devices shall be in accordance with National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products* (Reference a) and CNSS Directive No. 505, "Supply Chain Risk Management (SCRM)," dated 7 March 2012 (Reference b).

SECTION II – AUTHORITY

3. The authority to issue this policy derives from National Security Directive 42 (Reference c), which outlines the roles and responsibilities for securing national security systems, consistent with applicable law, E.O. 12333 (Reference d), as amended, and other Presidential directives. Nothing in this policy shall alter or supersede the authorities of the Director of National Intelligence.

SECTION III – SCOPE

4. This policy applies to all U.S. Government Federal Departments and Agencies (D/A), including their supporting contractors and agents that operate, use or manage NSS.

SECTION IV – POLICY

5. HAIPE-IS 3.0.2 is the HAIPE baseline version of the HAIPE interoperability specification. Newly procured HAIPE network architectures containing Internet Protocol Version 4 (IPv4) or Internet Protocol Version 6 (IPv6) capabilities that protect NSS and the information therein shall comply with the requirements in the HAIPE-IS Version 3.0.2 or later. HAIPE-IS versions will be updated as needed to achieve interoperability and ensure compliance with the previous versions of HAIPE.

6. Operational networks currently secured by HAIPE 1.3.5 products can be upgraded one node at a time and still maintain interoperability by installation of HAIPE-IS 3.0.2 or later compliant products that include support for the HAIPE-IS legacy extension.

7. National Security Agency (NSA)-Approved Commercial Solutions, when properly implemented according to requirements and standards approved by NSA, are not required to comply with the HAIPE-IS.

8. It is recommended that organizations purchasing HAIPE compliant devices work with HAIPE vendors to exchange implementation, environmental, or performance requirements, as the HAIPE-IS does not specify them.

9. This policy shall be revised upon the release of any updates to HAIPE-IS.

SECTION V – RESPONSIBILITIES

10. A U.S. Government D/A employing network encryption products to protect national security information, or other mission critical information related to national security in accordance with CNSS Policy No. 15, "*National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems*" (Reference e) shall:

a. Acquire HAIPE-IS Version 3.0.2 compliant devices or later HAIPEs, or other NSA-certified, interoperable IP encryption products, according to the policy outlined in this document;

b. Upgrade older versions of HAIPE-IS compliant devices with newer versions of HAIPE devices, as appropriate; and

c. Ensure that the D/A's Authorizing Official (AO) accredits that the device is implemented in accordance with this policy and NSA-approved guidance.

11. NSA shall:

a. Support the development of HAIPE-IS compatible devices through a User Partnership Program. (additional information is available at http://www.nsa.gov/ia/business research/ia bao/user partnership program.shtml); and

b. Certify the security and verify the interoperability of new HAIPE devices and software upgrades to previously certified devices.

SECTION VI – DEFINITIONS

12. The following definitions are provided to clarify the use of specific terms contained in this policy. All other terms used in this issuance are defined in CNSS Instruction No. 4009, National IA Glossary (Reference f):

a. <u>High Assurance Internet Protocol Encryptor (HAIPE)</u>: Device that provides networking, traffic protection, and management features that provide information assurance (IA) services in an IPv4/IPv6 network.

b. <u>High Assurance Internet Protocol Encryptor Interoperability Specification</u> (<u>HAIPE-IS</u>): Suite of documents containing the traffic protection, networking, and interoperability functional requirements necessary to ensure the interoperability of HAIPE compliant devices. This policy applies to HAIPE-IS Version 3.0.2 and all subsequent HAIPE-IS versions.

c. <u>Legacy</u>: Feature or capability that has been superseded but is still used due to operational necessity. HAIPE-IS version 1.3.5 is a legacy version that has been superseded by HAIPE-IS version 3.0.2.

d. <u>NSA-Approved Commercial Solution</u>: The combination of multiple Commercial-Offthe-Shelf (COTS) IA products in a layered configuration that satisfies the security requirements of an operational use case, when properly implemented in accordance with NSA-approved requirements and standards.

SECTION VII – REFERENCES

13. The following references apply:

a. NSTISSP No. 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products, dated July 2003.

b. CNSS Directive No. 505, Supply Chain Risk Management (SCRM), dated 7 March 2012.

c. National Security Directive No. 42, National Policy for the Security of National Security Telecommunications and Information Systems, dated 5 July 1990.

d. Executive Order 12333 (EO 12333), United States Intelligence Activities, as amended, dated 30 July 2008.

e. CNSS Policy No. 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Secure Systems, dated 1 October 2012.

f. CNSSI No. 4009, National Information Assurance (IA) Glossary, dated April 2010.