Committee on National Security Systems

CNSS Policy No. 19
February 2007

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

This document prescribes minimum standards. Your department or agency may require further implementation.

Committee on National Security Systems

CNSS Policy No. 19

CHAIR

FOREWORD

1. The U.S. Government's communication infrastructure is becoming more reliant upon network communications. Legacy government owned and operated circuit switched communication channels are being replaced with packet switched infrastructures. National Security Systems (NSS) users are also starting to leverage commercial and foreign public Internet Protocol (IP) infrastructures. These networks will provide a converged transport infrastructure for data applications, as well as real-time services. Communication channels that were often implemented to support a single application over a link will now rely on a shared infrastructure that supports multiple applications operating over a mesh network. As this transition occurs, legacy link encryptors must be incrementally replaced with network encryption products. 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 (HAIPE) Interoperability Specification (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.

2. This policy is being issued to provide governance for the procurement of IP encryption products for Fiscal Year (FY) 2009 and beyond. The intent of this policy is to ensure that all IP products procured after FY 2008 are compliant with the appropriate version of the HAIPE IS.

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. The first report for the attached policy is due six months following its issuance.

4. This policy can be located in the library on the CNSS website: www.cnss.gov.

/s/
John G. Grimes

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

SECTION I – SCOPE

1. This Policy is applicable to all U.S. Government Departments and Agencies that are considering the acquisition or use of HAIPE compliant products associated with the protection of National Security Systems (NSS) and/or National Security Information (NSI).

2. This policy is being issued per 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."

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

SECTION II – REFERENCES

4. CNSSI No. 4009, "National Information Assurance (IA) Glossary," dated June 2006.

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

6. For further guidance contact NSA Commercial Solution Center (NCSC), C41 at haipe_po@missi.ncsc.mil.

SECTION III – DEFINITIONS

7. Definitions in CNSS Instruction No. 4009 (Reference b) apply to this policy. Additional terms are defined in ANNEX A.

SECTION IV – POLICY

8. All Internet Protocol Version 4 (IPv4) or IPv6 standalone encryptors, or systems containing IPv4 or IPv6 encryptor capabilities, protecting NSS and/or NSI that

are procured or acquired after September 30, 2008, shall comply with core requirements in the HAIPE IS Version 3. If the device supports additional capabilities associated with a HAIPE IS Version 3 Extension(s), these features must be implemented in a manner compliant with all associated extension requirements.

9. HAIPE IS 3.0 compliant devices support HAIPIS 1.3.5 modes; therefore, operational secure networks can be upgraded one node at a time.

10. Future enhancements such as HAIPE-to-HAIPE Key Transfer, Ethernet Encapsulation, and Plaintext Header Compression will require HAIPE 3.0 operating modes and transforms. Devices compliant with 1.3.5 must be upgraded to 3.0 to take advantage of these future features.

SECTION V – RESPONSIBILITIES

11. U.S. Government Departments and Agencies employing network encryption products to protect NSI, or other mission critical information related to national security shall purchase HAIPE IS 3.0 compliant products by the date set forth in the policy section of this document. These organizations are also responsible for upgrading existing HAIPIS 1.3.5 devices with HAIPE 3.0 devices, as appropriate. It is also recommended that organizations purchasing HAIPE compliant devices work with commercial HAIPE vendors to exchange implementation, environmental, or performance requirements, as the HAIPE IS does not specify them.

12. The National Security Agency (NSA) will establish programs and sponsor development (e.g., Commercial COMSEC Endorsement Program [CCEP] or the User Partnership Program) of HAIPE IS 3.0 compatible devices. NSA is also responsible for certifying the security and interoperability of new HAIPE devices and software upgrades to previously certified devices.

13. This policy, along with its compliance dates, will be revised upon the release of any updates to HAIPE IS Version 3

Encls:
ANNEX A – Definitions
ANNEX B – Background

ANNEX A

DEFINITIONS

Terms used in this policy have the following meanings:

a. Ethernet Encapsulation - Used to describe HAIPE traffic and protection and networking capabilities related to encapsulating of Ethernet traffic.

b. Plaintext Header Compression - Compressing Plain Text IP headers during HAIPE traffic processing to reduce the overhead associated with encapsulating plaintext IP packets.

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

d. High Assurance Internet Protocol Encryptor Interoperability Specification (HAIPE IS) - Suite of documents containing the traffic protection, networking, and interoperability functional requirement necessary to ensure the interoperability of HAIPE compliant devices. This policy applies to HAIPE IS Version 3.0 or any subsequent errata version (e.g., 3.0.1, 3.0.2, etc…). (Also referred to in earlier versions as HAIPIS.)

e. HAIPE-to-HAIPE Key Transfer - Refers to the transfer of key material using a central HAIPE crypto-net controller to distribute keys to client HAIPE devices over a pre-established Security Association (SA).

f. Legacy - Feature or capability that has been superseded but is still used due to operational necessity.

ANNEX B

BACKGROUND

The U.S. Government's communication infrastructure is becoming more reliant upon network communications. Legacy government owned and operated circuit switched communication channels are being replaced with packet switched infrastructures such as Defense Information Services Agency's (DISA's) Global Information Grid – Bandwidth Expansion (GIG-BE). National Security Systems users are also starting to leverage commercial and foreign public Internet Protocol (IP) infrastructures. These networks will provide a converged transport infrastructure for data applications, as well as real-time services. Communication channels that were often implemented to support a single application over a link will now rely on a shared infrastructure that supports multiple applications operating over a mesh network. As this transition occurs, legacy link encryptors must be incrementally replaced with network encryption products. The interoperability of network-layer encryption devices is vital in enabling net-centric capabilities, while maintaining end-to-end protection of National Security System traffic. The HAIPE Interoperability Specification 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.

The Department of Defense (DoD) and the Intelligence Community (IC) have been the primary users of encryption products. However, packet switched network infrastructures are now being deployed to enable assured information sharing among homeland defense, first responders, second and third parties, and other U.S. Government (USG) stakeholders. All of these user communities require interoperable security solutions.

Interoperability standards enable the transition from single vendor stovepipe Information Assurance (IA) solutions to competitive products offered by multiple vendors. HAIPE IS version 1.x introduced basic signaling interoperability between various products and was primarily intended for enclave gateway implementations. HAIPE IS version 3.0 supports Internet Protocol Version 6 (IPv6), standardized over-the-network management and bandwidth efficient modes and transforms. HAIPE 3.0 complaint products can be implemented in hosts and terminals, in addition to enclave gateway solutions.

HAIPE compliant products are certified against a host of requirements detailed in the HAIPE IS. The purpose of the HAIPE IS is to capture the traffic protection, networking, and management functional requirements necessary to ensure the interoperability of HAIPE compliant devices. The HAIPE IS does not contain any implementation, environmental, or performance requirements. The HAIPE IS defines a set of core and extension features for network-layer encryption implementations. The core features define minimum essential capabilities for:

- HAIPE to HAIPE Interoperability
- HAIPE to Network Infrastructure Interoperability
- HAIPE to Management Infrastructure Interoperability
- HAIPE to Key Management Infrastructure Interoperability

The extension features define additional control and management plane capabilities, as well as legacy traffic protection capabilities to support interoperability with legacy HAIPE implementations. Extension features are appropriate for some, but not all, implementations.

HAIPE IS 3.0 offers many critical enhancements from previous versions including:

- Bandwidth efficient transforms that reduce the overhead associated with packet encapsulation
- Transport encapsulation mode that provides additional reduction in overhead
- Suite B cryptography that leverages publicly available cryptographic algorithms
- Enhanced QoS field bypass for differential service, congestion notification, and flow labels
- Improved multicast proxy support
- Independent support for IPv4 and IPv6 traffic
- Support for IPv6 features such as Flow Label bypass, address auto-configuration, and neighbor discovery among others
- Scalable Peer discovery, which allow for HAIPEs to dynamically locate and establish security associations with peer HAIPEs in large networks
- Standardized secure network management for all compliant HAIPE devices

HAIPE uses Internet Engineering Task Force (IETF) protocols to provide its traffic protection, networking, and management capabilities. The HAIPE IS specifies the use of the IETF Encapsulating Security Payload version 3 (ESPv3) to encapsulate plaintext IPv4 or IPv6 traffic. HAIPE uses the IETF's Simple Network Management Protocol version 3 (SNMPv3) to support over-the-network management and the IETF's Routing Information

Protocol version 2 (RIPv2) and Routing Information Protocol Next Generation (RIPng) to provide the HAIPE local discovery capability. The IETF has defined a cryptographic transform based upon Advanced Encryption Standard (AES) and Galois Counter Mode (GCM). The Suite B Cryptographic Mode specified in HAIPE IS 3.0 is also based upon AES and GCM. NSA will engage with the IETF to align HAIPE specifications and the emerging standards for GCM.