CNSS Advisory Memorandum
INFORMATION ASSURANCE/1-04
July 2004

Advisory Memorandum for Information Assurance (IA) - Security Through Product Diversity

CNSS Advisory Memorandum
INFORMATION ASSURANCE/1-04
July 2004

Committee on National Security Systems

National Manager

FOREWORD

1. This memorandum advises U.S. Government departments and agencies to implement a multi-layered, multi-vendor approach to security such as a defense-in-depth solution.

2. Representatives of the Committee on National Security Systems (CNSS) may obtain additional copies of this memorandum from the Secretariat at the address listed below.

3. I encourage dissemination of the contents of this memorandum to all Government entities, vendors, or contractors engaged in IA activities associated with national security systems.

/s/
MICHAEL V. HAYDEN
Lieutenant General, USAF

CNSS Advisory Memorandum
INFORMATION ASSURANCE/1-04
July 2004

Advisory Memorandum
Information Assurance (IA) - Security Through Product Diversity

1. Purpose and Scope - This memorandum advises U.S. Government departments and agencies to emphasize a multi-layered and multi-vendor approach to security when architecting information systems.

2. Guidance - National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products (NSTISSP No. 11) limits the selection of IA products to those that have been evaluated or validated by criteria specified in the policy. NSTISSP No. 11 does not provide guidance on how to compose compliant products into secure systems. Further, satisfying NSTISSP No. 11 criteria does not necessarily imply that a product is free of vulnerabilities. For instance, products evaluated against basic National Information Assurance (NIAP) protection profiles, levels 4 and below, do not include robust vulnerability testing as part of their validation. In most cases, certification of these products simply implies that the product functions as advertised.

Protecting systems encompasses more than just acquiring compliant products. Security of information systems is best achieved through a multi-layered security approach that employs sound information system security engineering, integrated security solutions, and good IA practices.

From a technology perspective, combining a multi-layered security approach with NSTISSP No. 11 compliant products offers the best protection from attackers because it requires the attacker to breach multiple layers of security before successfully gaining access to critical system resources. Examples of compliant products that may be layered include firewalls, virus protection, access controls (e.g., smart cards, passwords, and biometrics), encryption, intrusion detection, digital certificates, and virtual private networks (VPNs).

3. Recommendation - When developing and deploying security solutions, Government agencies and departments should employ a multi-layer approach to security such as using a defense-in-depth solution. When possible, compliant products should also be acquired from a diverse group of vendors since inadvertent or deliberate vulnerabilities present in one vendor’s products may be offset by security afforded by products acquired from other vendors. The combination of product layers and diversity for both software and hardware will enhance overall systems security.