NIST Special Publication 800-23

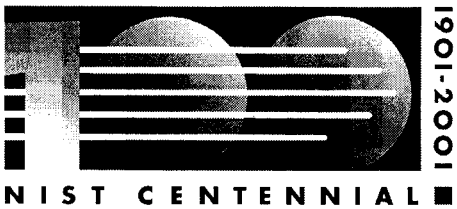
U.S. DEPARTMENT OF
COMMERCE
Technology Administration
National Institute of Standards
and Technology

Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products

Recommendations of the National Institute of Standards and Technology

Edward A. Roback

C O M P U T E R S E C U R I T Y



NIST National Institute of Standards and Technology • Technology Administration • U.S. Department of Commerce

NIST Special Publication 800-23

Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products

Recommendations of the National Institute of Standards and Technology

Edward A. Roback

C O M P U T E R S E C U R I T Y

Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

August 2000

U.S. Department of Commerce
Norman Y. Mineta, Secretary

Technology Administration
Dr. Cheryl L. Shavers, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
Raymond G. Kammer, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800 series reports on ITL's research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-23
Natl. Inst. Stand. Technol. Spec. Publ. 800-23, xx pages (Aug. 1999)
CODEN: NSPUE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 2000

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402-9325

Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products

Recommendations of the National Institute of Standards and Technology

Purpose

This document provides guidelines for Federal organizations' acquisition and use of security-related Information Technology (IT) products. NIST's advice is provided in the context of larger recommendations regarding security assurance.

Authority

This document has been developed by NIST in furtherance of its statutory responsibilities (under the Computer Security Act of 1987 and the Information Technology Management Reform Act of 1996, specifically 15 U.S.C. 278 g-3(a)(5)). This is not a guideline within the meaning of (15 U.S.C. 278 g-3 (a)(3)).

These guidelines are for use by Federal organizations which process sensitive information.[1] They are consistent with the requirements of OMB Circular A-130, Appendix III.

The guidelines herein are not mandatory and binding standards. This document may be used by non-governmental organizations on a voluntary basis. It is not subject to copyright.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding upon Federal agencies by the Secretary of Commerce under his statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, the Director of the Office of Management and Budget, or any other Federal official.

Background

These guidelines provide advice to agencies *for sensitive (i.e., non-national security) unclassified systems*. This advice regarding sensitive unclassified systems complements

[1] Many people think that sensitive information only requires protection from unauthorized disclosure. However, the Computer Security Act provides a much broader definition of the term "sensitive information:" *any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.*

the guidance recently issued for the *national security* community for the use and acquisition of "information assurance" products.

In January 2000, the National Security Telecommunications and Information Systems Security Committee (NSTISSC) issued National Security Telecommunications and Information Systems Security Policy (NSTISSP) Number 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products." NSTISSP Number *11 applies to national security systems* as defined in National Security Directive 42. A summary of NSTISSP Number 11 appears in Appendix I for reference purposes. The complete document is available to Government organizations through the NSTSSC Secretariat (I42), National Security Agency, 9800 Savage Road, Ft. Meade, MD, 20755-6716.

Guidelines

1. **Federal departments and agencies should understand the concept of computer security assurance.**

Broadly speaking, computer security assurance provides a basis for one to have confidence that security measures, both technical and operational, work as intended. Varying degrees of assurance[2] are supported through methods such as conformance testing, security evaluation, and trusted development methodologies. Assurance is not, however, a guarantee that the measures work as intended; it is closely related to areas of reliability and quality.[3]

2. **Federal departments and agencies should be aware of how assurance in the acquired products supports security.**

In general, the higher the assurance, the greater the confidence a manager has that the IT products, systems, networks being used work as intended and are being sufficiently protected.[4] Assurance in individual product components contributes to overall system security assurance – but it neither provides a guarantee of system assurance nor, in and of itself, secures a system. Use of products with an appropriate degree of assurance contributes to security and assurance of the system as a whole and thus should be an important factor in IT procurement decisions. For a security product, system or software a combination of measures for such areas as security functionality, sound development and operational practices, and periodic inspection and review, needs to be addressed as well. In other words, complementary and interdependent controls are needed, such as sound operating procedures, adequate training, comprehensive policies, sound security architectures, and a comprehensive risk management program.

---

[2] The term "assurance" is used throughout as shorthand for "security assurance."

[3] Details regarding the definition of assurance and examples of how it can be obtained can be found in NIST Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook" available at http://csrc.nist.gov/nistpubs/.

[4] Sufficient protection refers to the level of security deemed so by the management official who authorizes a system to process information, (some agencies refer to this authorization as accreditation). See Appendix III to OMB Circular A-130.

3. **Federal departments and agencies should be knowledgeable of the many approaches to obtaining security assurance in the products they procure.**

There are a number of ways that security assurance in products and systems is achieved/determined, such as:

NIST, NSA or other Conformance Testing and Validation Suites
Testing and Certification
Evaluation and Validation
Advanced or Trusted Development Techniques
Performance Track Record/Users' Experiences
Warranties, Integrity Statements, and Liabilities
Secure Distribution

Note that the reliability of these methods can vary considerably. See Chapter 9 entitled "Assurance" in *An Introduction to Computer Security: The NIST Handbook NIST Computer Security Handbook* and the Common Criteria general information web page at *http://csrc.nist.gov/nistpubs/ and http://niap.nist.gov/cc-scheme* for a more in-depth discussion.

4. **Federal agencies should specifically be aware of the benefits that can be obtained through testing of commercial products against customer, government, or vendor-developed specifications.**

Two Government programs are of particular interest here – the National Information Assurance Partnership (NIAP)'s Common Criteria Evaluation and Validation Program and NIST's Cryptographic Module Validation Program (CMVP). The NIAP program focuses on *evaluations* of products (e.g., a firewall or operating system) against a set of security specifications. The CMVP program focuses on security *conformance testing* of a cryptographic module against Federal Information Processing Standard 140-1, *Security Requirements for Cryptographic Modules* and related Federal cryptographic algorithm standards.

The **NIST / NSA – sponsored NIAP** is a U.S. Government initiative designed to meet the security evaluation needs of both IT producers and consumers. The NIAP program is intended to foster the availability of objective methods for evaluating the security of IT products. In addition, NIAP is designed to foster the development of commercial testing laboratories that can provide the types of testing and evaluation services which will meet the demands of both producers and consumers. The NIAP focuses on evaluations conducted in accordance with the "Common Criteria" (ISO/IEC 15408) evaluation approach. In addition to containing a taxonomy of security functional requirements, the "Common Criteria" specifies seven predefined assurance packages, known as Evaluation Assurance Levels (EALs). While these may be more generally well-known, the Common Criteria provides the flexibility to allow producers and consumers to define their unique assurance requirements (i.e., use of one of the predefined EALs is not mandatory.)

Agencies may use the laboratories accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) to perform evaluations of products against security requirements expressed using the "Common Criteria." As the NIAP progresses, such security requirements, known as "protection profiles" will be developed by industry and government consumers. For those security requirements which may be appropriate to a broad segment of its Federal community, NIST intends to generally promulgate protection profiles as technical guidelines to the Federal community following an informal agency review and comment process. Testing can also be accomplished against vendor-developed security requirements associated with a vendor's specific product or system, known as a "security target." This testing can support vendor security claims. The evaluation conducted by accredited private sector laboratories under the auspices of NIAP provides for varying levels of assurance, to meet customer requirements. (See http://niap.nist.gov.)

The **Cryptographic Module Validation Program** (CMVP), which is jointly run with the Government of Canada's Communications Security Establishment, provides customers with assurance, through functional testing, that:

1) a cryptographic module meets one of the four security specification levels of Federal Information Processing Standard 140-1, *Security Requirements for Cryptographic Modules* (a mandatory Federal Information Processing Standard for sensitive (unclassified) applications and

2) that the FIPS-approved algorithms (e.g., Triple DES) are correctly implemented.

Assurance of the proper functioning of cryptographic modules and algorithms is considered critical because encryption techniques are used to protect sensitive data that is transmitted over untrusted paths (e.g., over the Internet). Additionally, the knowledge of and consequences resulting from unauthorized disclosure of information may not be apparent for some time (as compared, say, to the immediate awareness that a homepage has been defaced). The specifications for FIPS 140-1 and a current list of validated modules can be found at http://csrc.nist.gov/cryptval/

CMVP tested modules are often integrated into commercial products with additional (i.e., non-cryptographic) functionality. The assurance provided by CMVP concerning cryptographic modules does not imply assurance with regard to other aspects of the product into which the module is incorporated. The CC-NIAP evaluation approach described can be used to complement the CMVP (i.e., to evaluate other security requirements of the product), thereby addressing assurance of the overall product.

5. **Federal departments and agencies should acquire and use products appropriate to their risk environment and the cost-effective selection of security measures. Agencies should develop policies for the procurement and use of evaluated products as appropriate. When selecting products, agencies need to consider the**

threat/risk environment, cost-effectiveness, assurance level, and security functional specifications, as appropriate.

A listing of products which have been validated under the NIAP's Common Criteria Evaluation and Validation Program can be found via http://niap.nist.gov. At the time of this writing, no Common Criteria protection profiles have been designated as mandatory and binding by the Secretary of Commerce. It is NIST's intent to issue protection profiles (when appropriate) as technical security guidelines to the Federal community.

With specific regard to ***cryptographic modules and FIPS-approved cryptographic algorithms***, agencies are reminded that the use of modules tested as conformant to *Security Requirements for Cryptographic Modules* (Federal Information Processing Standard 140-1) has been made mandatory and binding by the Secretary of Commerce. NIST maintains a publicly available list of modules, which have been so validated, at http://csrc.nist.gov/cryptval/ .

6. **Federal Agencies should give substantial consideration in IT procurement and deployment for IT products that have been evaluated and tested by independent accredited laboratories against appropriate security specifications and requirements. Examples of these specifications will include NIST recommended protection profiles based on ISO/IEC 15408, the Common Criteria.**

The ultimate goal in purchasing a system is to obtain the necessary functionality and performance within cost and time constraints. Moreover, performance includes dependability and reliability and hence is directly impacted by security considerations. In general, third party testing and evaluation provides a significantly greater basis for customer confidence than many other assurance techniques. Yet, it is important to note that purchasing an evaluated product simply because it is evaluated and without due consideration of applicable functional and assurance requirements, may be neither useful nor cost effective. IT users need to consider their overall requirements and select the best products accordingly.

7. **Federal departments and agencies need to address how products (with appropriate assurance) are configured and integrated properly, securely and subject to the managerial operational approval process[5] so as to help ensure security is appropriately addressed on a system-wide basis.**

The overall assurance level of a system as a whole may be different (usually lower) than the assurance level of individual components. While product assurance is a crucial and necessary input into the system security process, all the usual policies, controls, and risk management processes must also be in place for a system to operate in a reasonably secure mode. There are typically specific configuration settings that must be employed for the product to operate in the secure manner desired. In addition, much attention must be paid to combining such products in order to provide an appropriate security solution

[5] This refers to the approval process discussed in Office of Management and Budget Circular A-130, Appendix III.

for a given risk and threat environment. Thus, in addition to employing products with appropriate security capabilities and assurance, review of the security of a system from a system-wide perspective supports the managerial operational approval process.

Agencies should also be aware of the interconnectivity and associated interdependence of organizations and that a risk accepted by one organization may inadvertently expose other organizations to the same risk.

Supplemental Information

Appendix I: *Fact Sheet -- National Security Telecommunications and Information Systems Security (NSTISSP) Number 11, National Information Assurance Acquisition Policy.* (NSTISSP Number 11 itself is "For Official Use Only" and therefore not included in this document.)

Appendix II: *National Security Telecommunications and Information Systems Security Committee Advisory Memorandum for the Strategy for Using the National Information Assurance Partnership (NIAP) for the Evaluation of Commercial Off-the-Shelf (COTS) Security Enabled Information Technology Products.* (NSTISSAM INFOSEC/2-00)