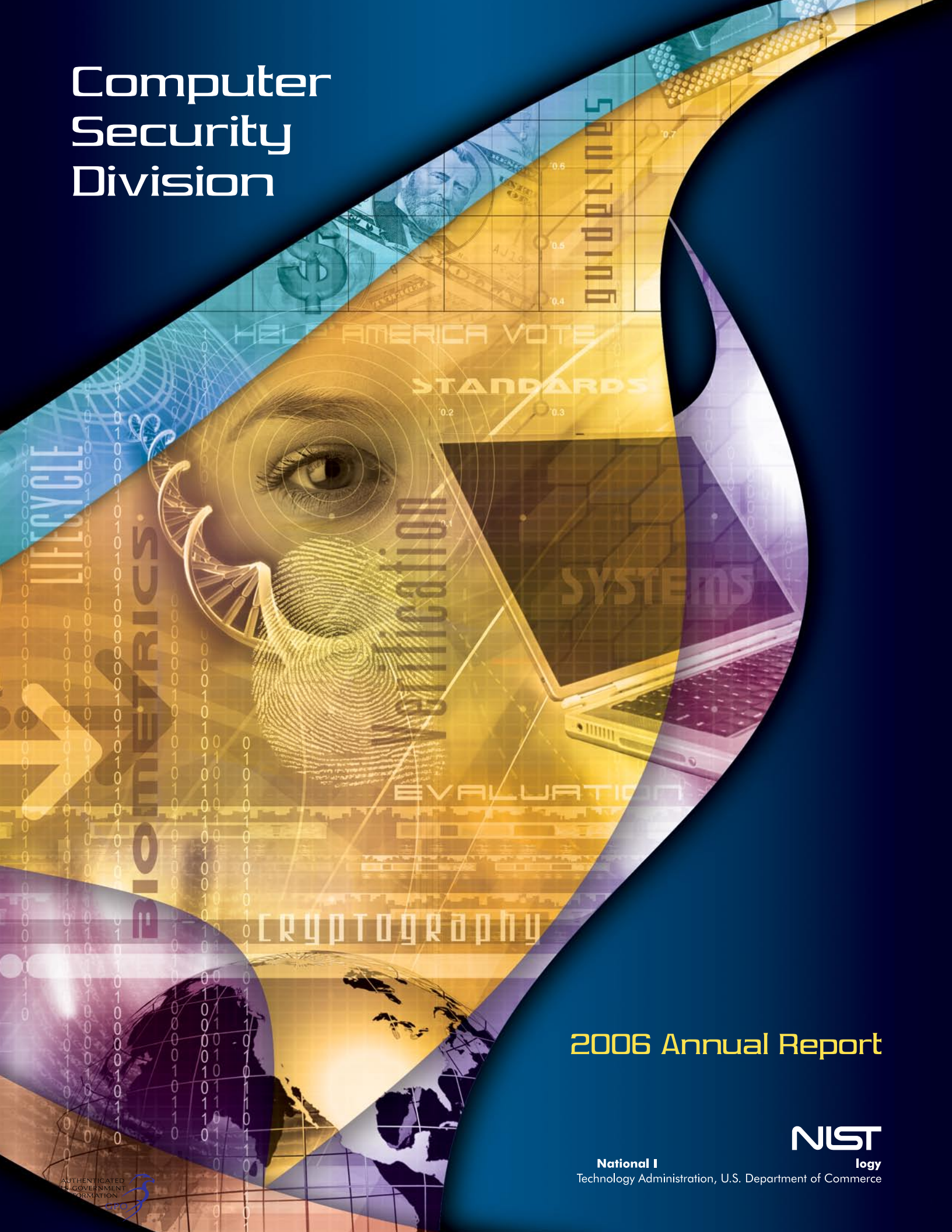
# Computer Security Division




## 2006 Annual Report

NIST
National I logy
Technology Administration, U.S. Department of Commerce

# Table of Contents

# Welcome

In 2006, the Computer Security Division (CSD) of NIST's Information Technology Laboratory engaged in a number of initiatives for improving information system security in the Federal government. Both automated tool development and increased outreach activities were initiated to communicate information technology risks, vulnerabilities, and protection requirements—particularly for new and emerging technologies. The CSD continued to research and publicize IT vulnerabilities. Emphasis was placed on development of techniques for affordable security and privacy mechanisms for Federal information systems. We continued to develop standards, metrics, tests, and validation programs to promote, measure, and validate security in systems and services. We also developed guidance to increase secure IT planning, implementation, management, and operation. Affected customer organizations include federal, state, and local governments, the healthcare community, colleges and universities, small businesses, the private sector, and the international community.

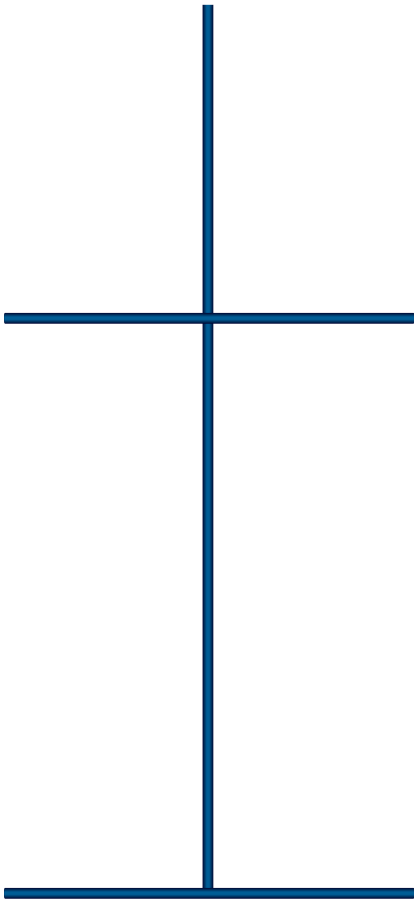
This year also brought additional security challenges along with the ever-advancing improvements in technology, improvements in citizens' access to government systems and information, faster communications, reduced paperwork, and streamlined processes. Our work this year met those security challenges with a breadth and depth of security areas intended to allow our customers to accomplish their missions while providing for confidentiality of their information, maintaining the availability of their resources and ensuring the integrity of their data. High priority was given to initiating a competitive program for replacement of current secure hashing algorithms employed in data source and content integrity protection mechanisms.

One highlight of our work in 2006 was expanding and refining the Federal Information Processing Standards (FIPS) 201 standard suites and supporting implementation of Homeland Security Presidential Directive 12's mandate for common procedures and mechanisms for identity verification of Federal employees and contractors. We also continued our progress in fulfilling the mandates of the Federal Information Security Management Act of 2002 (FISMA), which resulted in revision of NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*; coordination of the draft SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*; and publication of FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. The Cryptographic Module Validation Program was expanded to include 13 laboratories in 4 countries and continues to ensure the protection of sensitive information in computer and telecommunication systems, including voice systems. Research and development efforts included security for Radio Frequency IDentification (RFID) devices and other wireless communications systems, digital forensic tools and methods, Internet security protocols, and expansion of the National Vulnerability Database.

We will continue to strive to provide products and services that protect and enhance confidence in the nation's information technology systems.

William Curtis Barker
Division Chief

# Division Organization



**William Curtis Barker**
***Division Chief***

**Security Management & Assistance Group**

**Elizabeth Chew**
***Group Manager***

**Security Technology Group**

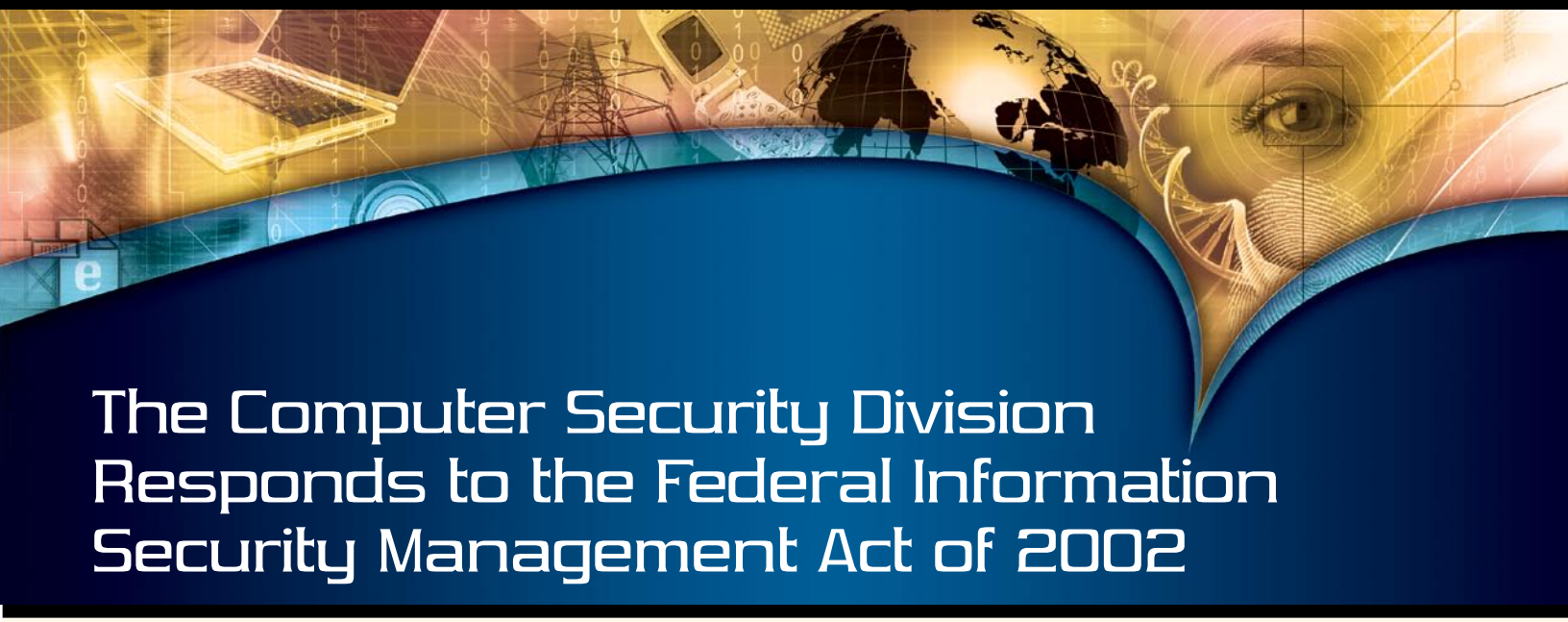
**William Burr**
***Group Manager***

**Security Testing & Metrics Group**

**Ray Snouffer**
***Group Manager***

**Security Research & Emerging Technologies**

**Timothy Grance**
***Group Manager***



# The Computer Security Division Responds to the Federal Information Security Management Act of 2002

The E-Government Act [Public Law 107-347] passed by the 107th Congress and signed into law by the President in December 2002 recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act of 2002 (FISMA), included duties and responsibilities for the Computer Security Division in Section 303 "National Institute of Standards and Technology." Work to date includes—

- **Provide assistance in using NIST guides to comply with FISMA** – Information Technology Laboratory (ITL) Computer Security Bulletin *Understanding the New NIST Standards and Guidelines Required by FISMA: How Three Mandated Documents are Changing the Dynamic of Information Security for the Federal Government* (issued November 2004).

- **Provide a specification for minimum security requirements for Federal information and information systems using a standardized, risk-based approach** – Developed FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems* (issued March 2006).

- **Define minimum information security requirements (management, operational, and technical security controls) for information and information systems in each such category** – Developed SP 800-53, *Recommended Security Controls for Federal Information Systems* (revision 1 issued December 2006).

- **Identify methods for assessing effectiveness of security requirements** - SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (second public draft issued April 2006).

- **Bring the security planning process up to date with key standards and guidelines developed by NIST** – SP 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems* (issued February 2006).

- **Provide assistance to Agencies and private sector** – Conduct ongoing, substantial reimbursable and non-reimbursable assistance support, including many outreach efforts such as the Federal Information Systems Security Educators' Association (FISSEA), the Federal Computer Security Program Managers' Forum (FCSM Forum), the Small Business Corner, and the Program Review for Information Security Management Assistance (PRISMA).

- **Evaluate security policies and technologies from the private sector and national security systems for potential Federal agency use** – Host a growing repository of Federal agency security practices, public/private security practices, and security configuration checklists for IT products. In conjunction with the Government of Canada's Communications Security Establishment, CSD leads the Cryptographic Module Validation Program (CMVP). The Common Criteria Evaluation and Validation Scheme (CCEVS) and CMVP facilitate security testing of IT products usable by the Federal government.

- **Solicit recommendations of the Information Security and Privacy Advisory Board on draft standards and guidelines** – Solicit recommendations of the Board regularly at quarterly meetings.

- **Provide outreach, workshops, and briefings** – Conduct ongoing awareness briefings and outreach to our customer community and beyond to ensure comprehension of guidance and awareness of planned and future activities. We also hold workshops to identify areas our customer community wishes addressed, and to scope guidance in a collaborative and open format.

- **Satisfy annual NIST reporting requirement** – Produce an annual report as a NIST Interagency Report (IR). The 2003, 2004, and 2005 Annual Reports are available via the Web or upon request.

# Security Management and Assistance

**STRATEGIC GOAL** ▸ ***Develop and improve mechanisms to protect the integrity, confidentiality, and authenticity of Federal agency information by developing security mechanisms, standards, testing methods, and supporting infrastructure requirements and methods.***

## Overview

Information security is an integral element of sound management. Information and computer systems are critical assets that support the mission of an organization. Protecting them can be as important as protecting other organizational resources, such as money, physical assets, or employees. However, including security considerations in the management of information and computers does not completely eliminate the possibility that these assets will be harmed.

Ultimately, responsibility for the success of an organization lies with its senior management. They establish the organization's computer security program and its overall program goals, objectives, and priorities in order to support the mission of the organization. They are also responsible for ensuring that required resources are applied to the program.

Collaboration with a number of entities is critical for success. Federally, we collaborate with the U.S. Office of Management and Budget (OMB), the U.S. Government Accountability Office (GAO), the National Security Agency (NSA), the Chief Information Officers (CIO) Council, and all Executive Branch agencies. We also work closely with a number of information technology organizations and standards bodies, as well as public and private organizations.

Major initiatives in this area include the FISMA Implementation Project; extended outreach initiatives and information security training, awareness and education; and producing and updating NIST Special Publications on security management topics. Key to the success of this area is our ability to interact with a broad constituency—Federal and nonfederal—in order to ensure that our program is consistent with national objectives related to or impacted by information security.

## FISMA Implementation Project

In response to FISMA, we continue to develop key security standards and guidelines for Federal agencies and their support contractors that will fundamentally change how the government protects its most important information systems. Phase I of the project includes the development of—

- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* (Completed);
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems* (Completed);
- NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* (Completed);
- NIST SP 800-53 Revision 1, *Recommended Security Controls for Federal Information Systems* (Completed 12/2006);
- NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Target Completion July 2007);
- NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System* (Completed); and
- NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories* (Completed).

The security standards and guidelines developed in Phase I will assist Federal agencies in—

- Implementing the individual steps in the risk management framework as part of a well-defined and disciplined system development life cycle process;
- Demonstrating compliance to specific requirements contained within the legislation; and
- Establishing a level of security due diligence across the Federal government.

In FY 2007, we will host the NIST Information Security Seminar Series, a series of workshops to assist in clarification of NIST standards and guidelines. The initial seminar is scheduled on January 10, 2007, and will feature—

- NIST personnel providing an in-depth look at NIST SP 800-53; and
- Representatives from the U.S. Office of Management and Budget (OMB), the U.S. Government Accountability Office (GAO), and the Inspectors General (IG) community speaking about FISMA guidance and answering questions.

Phase II of the FISMA Implementation Project will focus on the development of a program for credentialing public and private sector organizations to provide security assessment services for Federal agencies. The security services involve the comprehensive assessment of the management, operational, and technical security controls in Federal information systems to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. On April 26, 2006, we hosted the FISMA Implementation Project Phase II Workshop on Credentialing Program for Security Assessment Service Providers. The purpose of the workshop was to discuss requirements and possible options for the credentialing of security assessment providers. In FY 2007, a workshop will be held to further define Phase II activities.

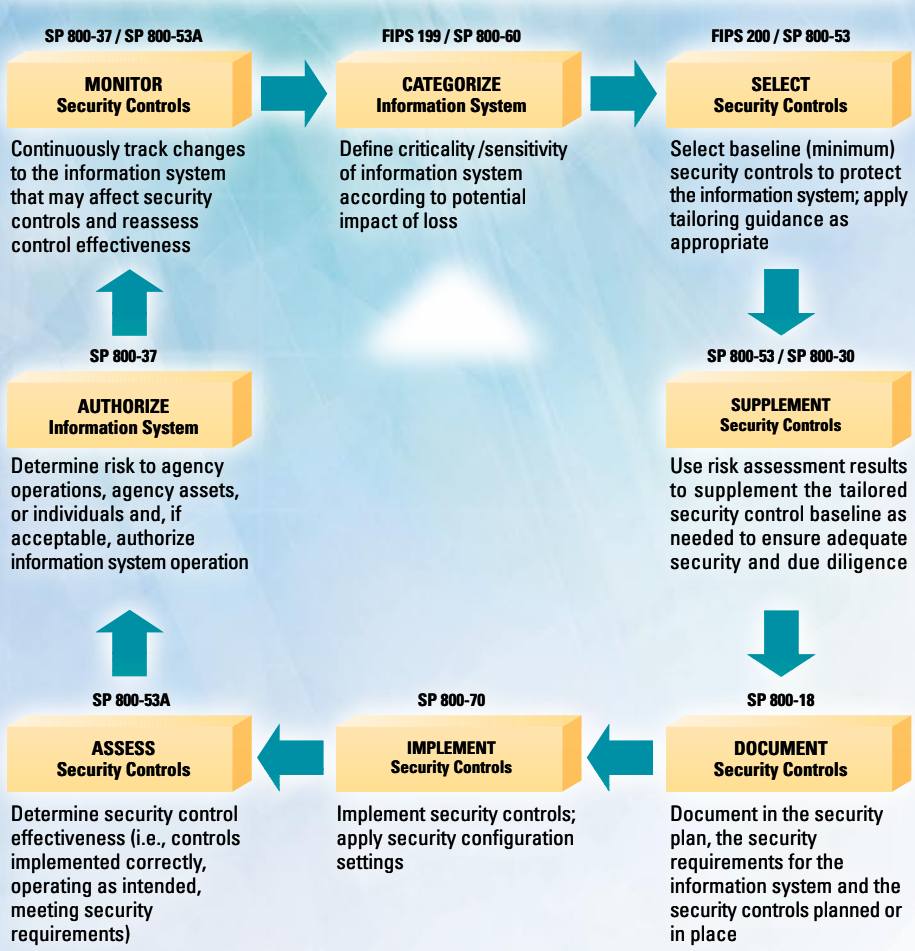
---

http://csrc.nist.gov/sec-cert
Contact: Ms. Elizabeth Chew
(301) 975-5236
elizabeth.chew@nist.gov

### Minimum Security Requirements and Security Controls

Following the approval and publication of FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, we began the biennial review and update cycle for NIST SP 800-53. This cycle is important to ensure that the security controls listed in SP 800-53 and the minimum security controls populating the control baselines represent the current state of the practice in safeguards and countermeasures for Federal information systems. During the past year, we received many insightful comments from government and industry on the format, structure, and content of SP 800-53. The recommendations for modifications reflect (1) customer experience gained from employing the security controls; (2) changing threat environments; and (3) new technologies that are available and can impact information security. In addition to proposing necessary changes to SP 800-53, it was also important to maintain a degree of stability within the publication as customers gained a better understanding of the security controls and began to employ the controls within their organizational information systems. In the first major update to this publication, the basic structure/concepts have been maintained, while the material has been significantly refined. NIST SP 800-53, Revision 1, focuses on improving the clarity of the security controls, eliminating redundancies among controls, and expanding the supplemental guidance for the controls in key areas. Specific changes include—

- Additions to the security control catalog, reflecting new controls and control enhancements that will provide customers with greater choices in supplementing their minimum baseline security controls;
- Additions to the minimum security control baselines reflecting an increased need for protection within Federal information systems and to better align the controls with current Federal policy and recommended security practices;
- Expansion of the Media Protection family to address the powerful, highly mobile processing and storage devices routinely used by today's Federal agencies and the increasingly diverse environments where the new technologies are employed;
- Employment of new concepts in the Certification, Accreditation, and Assessment family to promote more cost-effective assessments, extend the life of security accreditations over time, and reduce the paperwork associated with reaccreditations;
- Modifications to the Identification and Authentication controls addressing multifactor authentication;
- A more thorough discussion of the implications of using external information system services and external service providers on the security state of the information system and the associated risks to organizational operations, organizational assets, and individuals;




- Improved guidance in the process of selecting and specifying security controls for an information system with a closer alignment to the NIST Risk Management Framework (RMF);
- Application of Special Publication 800-53 security controls to industrial control systems; and
- New and expanded guidance on the process of updating security controls after security incidents, when threat levels are elevated, or when significant changes occur in the information system.

The proposed modifications to the catalog of security controls and security control baselines completed a rigorous public review process to obtain government and private sector feedback and to build consensus for the changes. We continue to provide improvements to Special Publication 800-53 that will help Federal agencies and their contractors effectively select and specify security controls for their information systems—and do so using a risk-based approach that facilitates cost-effective information security.

---

http://csrc.nist.gov/sec-cert
Contact: Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

### Methods and Procedures for Assessing Security Controls

The selection and employment of appropriate security controls for an information system is an important task that can have major implications for the operations and assets of an organization. Once employed within an information system, security controls must be assessed to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. We continued to expand our guidance on assessing the effectiveness of security controls in Federal information systems. The second public draft of SP 800-53A contained significant improvements in a variety of areas based on the feedback obtained from government and industry during the initial public comment period. In addition to completing the remaining 12 families of assessment procedures for the security control families in SP 800-53, other improvements were made to make the material more user-friendly for assessors, auditors, and evaluators.

Security assessments play an important role in the information security programs of organizations. These assessments can be used to support a variety of security-related activities, including but not limited to (1) the testing and evaluation of security controls during the development of an information system; (2) the information system security certification and accreditation process; (3) the annual testing and evaluation of security controls required by FISMA; and (4) generalized security reviews. The results of security assessments contribute to the knowledge base of organizational officials with regard to the security status of the information system and the

overall risk to the operations and assets of the organization incurred by the operation of the system. The guidance in SP 800-53A will help achieve more secure information systems within the Federal government by—

- Enabling more consistent, comparable, and repeatable assessments of security controls;
- Facilitating more cost-effective assessments of security control effectiveness;
- Promoting a better understanding of the risks to organizational operations, organizational assets, or individuals resulting from the operation of information systems; and
- Creating more complete, reliable, and trustworthy information for organizational officials—to support security accreditation decisions and the annual FISMA reporting requirements.

---

http://csrc.nist.gov/sec-cert
Contact: Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

### Organizational Accreditation Program

Phase II of the FISMA Implementation Project is focusing on the development of a program for credentialing public and private sector organizations to provide security assessment services for Federal agencies in support of certification and accreditation of information systems. These security services involve the comprehensive assessment of the management, operational, and technical security controls in Federal information systems to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system.

Agencies must rely on competent and capable security assessors to adequately assess the security controls and provide the necessary assessment results accreditation that authorities require to make critical security accreditation decisions for information systems, and for providing reliable information for reporting on compliance to FISMA. In addition, security assessments require expertise in 17 separate security areas as defined by FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, and assessors must have an in-depth knowledge of the assessment procedures necessary for assessing these requirements. Agencies often do not have the required in-house resources or expertise needed to conduct the required assessments and thus are left with the uncertain task of acquiring competent and capable security assessment providers.

Organizations that successfully complete the credentialing program will be able to demonstrate competence in performing assessments of security controls implemented in an information system based on FISMA requirements and NIST standards and guidelines. Developing a network of accredited organizations that demonstrate competence in the provision of security assessment services will give Federal agencies greater confidence in the acquisition and use of such services and lead to—

- More consistent, comparable, and repeatable security controls assessments of Agencies' information security programs and systems;
- A better understanding of enterprise-wide mission risks resulting from the operation of information systems;
- More complete, reliable, and trustworthy information for authorizing officials—facilitating more informed information system security accreditation decisions; and
- More secure information systems within the Federal government including critical infrastructures.

Development of the organizational credentialing program consists of four segments—

- Development and selection of an appropriate accreditation model for determining the competency of organizations desiring to provide security assessment services in accordance with NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*;
- Development of detailed credentialing requirements for organizations seeking accreditation;
- Development of appropriate proficiency tests to determine the competency of prospective organizations seeking accreditation in key NIST Special Publications associated with the certification and accreditation of Federal information systems; and
- Development of a strategy for implementing the accreditation program and selection of an appropriate accreditation body to conduct the organizational accreditations.

There will be extensive public vetting (i.e., from consumers—Federal agencies, security assessment service providers, and accreditation bodies of security assessment service providers) of the credentialing program during each segment of development as described above. The vetting process will include public workshops to discuss various credentialing approaches, requirements and models, a public review of the proposed assessment

methods and procedures contained in SP 800-53A, and a public review of the implementation strategy for the credentialing program.

On April 26, 2006, we hosted the first FISMA Implementation Project Phase II Workshop. Over 450 attendees from Federal agencies, private sector organizations, and academia participated. The purpose of the workshop was to discuss requirements and possible options for the credentialing of security assessment providers. At the workshop, attendees were provided a detailed overview of the FISMA project, followed by the vision and strategy for FISMA Phase II, an outline of three potential credentialing options, and a preliminary set of credentialing requirements (exemplars). The organization credentialing options presented and discussed were—

- **Option 1: Consumer-based Credentialing** in which Federal agencies draw upon credentialing requirements and guidance established from the FISMA phase II project to credential and acquire security assessment services;
- **Option 2: Public or Private Credentialing** in which the community develops and operates a credentialing process for security assessment providers based on service provider capability requirements, evaluation criteria, and training requirements established from the FISMA phase II project—albeit without NIST sponsorship; and
- **Option 3: NIST Sponsored Credentialing** in which NIST sponsors (or partners with others) in the establishment of a credentialing process for security assessment providers based on service provider capability requirements, evaluation criteria, and training requirements established from the FISMA phase II project.

A follow-up workshop will be held in FY 2007 to further define and review the FISMA Implementation Project phase II credentialing program development.

---

http://csrc.nist.gov/sec-cert

Contacts: Mr. Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Ms. Pat Toth
(301) 975-5140
patricia.toth@nist.gov

## Guidelines and Documents

### Revision of the NIST Security Managers' Handbook

NIST SP 800-100, *Information Security Handbook: A Guide for Managers,* provides a broad overview of information security program elements to assist managers in understanding how to establish and implement an information security program. Typically, the organization looks to the program for overall responsibility to ensure the selection and implementation of appropriate security controls and to demonstrate the effectiveness of satisfying the controls' stated security requirements. The topics within this document were selected based on laws and regulations relevant to information security, including the Clinger-Cohen Act of 1996, FISMA, and the U.S. Office of Management and Budget (OMB) Circular A-130. The material in this handbook can be referenced for general information on a particular topic or can be used in the decision-making process for developing an information security program. The purpose of this publication is to inform members of the information security management team—Agency Heads, Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and security managers—about various aspects of information security that they will be expected to implement and oversee in their respective organizations. In addition, the handbook provides guidance for facilitating a more consistent approach to information security programs across the Federal government.

---

Contact: Ms. Pauline Bowen
(301) 975-2938
pauline.bowen@nist.gov

### Media Sanitization

Information systems capture, process, and store information using a wide variety of media. Information is recorded on data storage media and on the devices that create, process, or transmit the information. This information must be protected from creation to disposal in a way that is appropriate to the value of the information. When organizations discard media and devices, organizations and individuals should make sure that proper techniques are used to remove the data, or to destroy the media, to protect the confidentiality of the information.

Media sanitization is the process for removing confidential data from storage media, with reasonable assurance that the data cannot be retrieved and reconstructed. Data that has been improperly or unsuccessfully removed from media could be recreated by attackers or by unauthorized individuals. The sanitization process is especially critical when storage media are transferred, become obsolete, are no longer usable, or are no longer required by an information system. All of the residual magnetic, optical, or electrical representation of data that has been deleted from the media must not be easily recoverable.

SP 800-88, *Guidelines for Media Sanitization*, helps organizations securely manage the sanitization of information processed and stored on devices and media. The guide discusses in detail the decision process concerning media that has been identified for disposal or reuse, and media that is no longer going to be under the effective control of the organization. The guide, used along with local policies and procedures, will enable managers to make effective, risk-based decisions for the effective sanitization of the information recorded on the media and for the disposal of the media.

SP 800-88 discusses the basic types of information, the available sanitization methods, and the different types of media and provides information on techniques for removing data and disposing of media. The guide gives details on the procedures and principles that influence sanitization decisions and includes a decision matrix to aid the decision-making process. The appendices include tables of minimum recommended sanitization techniques for clearing, purging, or destroying various media. These tables can be used with the decision flowchart to identify the needed steps for media sanitization. Also included in the appendices are a list of tools and resources that can assist in decisions about media sanitization; information about media sanitization specifically targeted to home computer users; and a list of references.

An important step that Federal organizations should take to securely manage their information and media is to categorize their information in accordance with FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*. FIPS 199 requires Federal agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. Based on the results of categorization for confidentiality, organizations should then select appropriate sanitization methods to protect their information.

Organizations should track, document, verify media sanitization and destruction actions, and periodically test the sanitization equipment and procedures to ensure correct performance.

SP 800-88 recommends that organizations establish an information security governance structure for their media sanitization decisions. The guide describes the security responsibilities of everyone in the organization—from program managers and agency heads to users.

Media types are expected to change as other IT technologies change. However, the process for media sanitization should always focus on protecting the information that is recorded on the media.

Contacts: Mr. Matthew Scholl
(301) 975-2941
matthew.scholl@nist.gov

Mr. Richard Kissel
(301) 975-5017
richard.kissel@nist.gov

### Revision of the Risk Management Guide

The management of risk in an Agency is a continual and complex process that often is conducted without the awareness of those responsible for accepting, deciding, or managing those risks. In order to ensure that organizations are aware of the activities that make up the risk management processes, we plan to update SP 800-30, *Risk Management Guide for Information Technology Systems*, to focus on the single activity of risk assessment and how risk assessment fits into risk management. We also plan to release a guide on risk management and the Risk Management Framework.

The selection and specification of security controls for an information system is accomplished as part of an organization-wide information security program that involves the management of risk. The management of risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for an information system—the security controls necessary to protect individuals and the operations and assets of the organization. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, and regulations. The following activities related to managing risk (also known as the NIST *Risk Management Framework*) are paramount to an effective information security program and can be applied to both new and legacy information systems within the context of the system development life cycle. Each of the activities in the Risk Management Framework has an associated NIST security standard and/or guideline document that can be used by organizations implementing the framework. The framework represents an iterative security life cycle process that focuses on managing risk to enterprise missions:

- **Categorize** the information system and the information resident within that system based on a FIPS 199 impact analysis.
- **Select** an initial set of minimum baseline security controls (i.e., security control foundation) for the information system from SP 800-53, based on the FIPS 199 security categorization. Apply tailoring guidance as appropriate to obtain the control set used as the starting point for the assessment of risk associated with the use of the system.
- **Supplement** the initial set of tailored security controls based on an assessment of risk and local conditions, including organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances.
- **Document** the agreed-upon set of security controls in the system security plan, including the organization's rationale for any refinements or adjustments to the initial set of controls.
- **Implement** the security controls in the information system. For legacy or previously existing systems, some or all of the security controls selected may already be in place.
- **Assess** the security controls using appropriate methods and procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

- **Determine** the risk to organizational operations and assets or to individuals resulting from the operation of the information system.
- **Authorize** information system operation if the risk to organizational operations and assets, and to individuals, is acceptable.
- **Monitor** and assess selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the associated changes, and reporting the security status of the system to appropriate organizational officials on a regular basis.

### Supplementing the Tailored Baseline

The tailored security control baseline should be viewed as the foundation or starting point in the selection of adequate security controls for an information system. The tailored baseline represents, for a particular class of information system (derived from the FIPS 199 security categorization and modified appropriately for local conditions), the starting point for determining the needed level of security due diligence to be demonstrated by an organization toward the protection of its operations and assets. However, the final determination of the appropriate set of security controls necessary to provide adequate security for an information system is a function of the organization's assessment of risk and what is required to sufficiently mitigate the risks to organizational operations, organizational assets, or individuals. In many cases, additional security controls or control enhancements will be needed to address specific threats to and vulnerabilities in an information system or to satisfy the requirements of applicable laws, directives, Executive Orders, policies, standards, and regulations.

The risk assessment at this stage in the security control selection process provides important inputs to determine the sufficiency of the security controls in the tailored baseline—that is, the security controls needed to adequately protect the organization's operations (including mission, function, image, and reputation), the organization's assets, and individuals. The update to SP 800-30 will detail the risk assessment process used to supplement the tailored baseline in the conduct of the Risk Management Framework.

Contact: Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

### FISMA Reference Model

In October 2005, research began on developing a NIST SP that enhances Federal agencies' understanding of those information security activities associated with meeting the requirements of FISMA and assists in automating the process for managing FISMA compliance. To support process automation, this SP contains an eXtensible Markup Language (XML) schema that identifies key components and interdependencies of an effective information security program. Software tool developers will be able to use this document to automate the collection of core security data elements (e.g., information security plans, contingency plans, risk assessments) described in our standards and guidelines. This schema, when implemented by tool developers, will also enable independent security products to share data in a common format. Tools used for the collection of the data elements will have an application interface that supports the XML schema to assure maximum flexibility in the automation process. Further automating the collection of core security data elements will enable Federal agencies to more efficiently and cost-effectively manage their information security programs.

The FISMA Reference Model is expected to be available summer 2007.

Contacts: Ms. Elizabeth Chew
(301) 975-5236
elizabeth.chew@nist.gov

Mr. Kevin Stine
(301) 975-4483
kevin.stine@nist.gov

Ms. Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

### Return on Security Investment

One of our goals is to assist in developing approaches for agencies to determine cost-effective strategies in achieving a level of information security commensurate with the degree of risk and magnitude of likely harm.

This past year, we worked with economists in the NIST Building and Fire Research Laboratory (BFRL) to prototype a Return on Security Investment methodology. In FY 2007, BFRL will publish a NIST Interagency Report (NISTIR) titled *An Analytical Approach to Cost-Effective, Risk-Based Budgeting for Federal Information System Security*, to identify and illustrate one approach to simplify and strengthen capital planning for information system security in compliance with Federal policy and guidance. The report will provide the theoretical underpinnings of a methodology that may enable budgeting officials, system owners, and managers to select cost-effective strategies for optimizing the level of information system security to be achieved, given the level of vulnerability faced by the organization. This NISTIR will help to lay the foundation for simultaneously simplifying and strengthening capital planning for information system security by identifying and illustrating an approach enabling established, repeatable, automated processes that comply with Federal policy and guidance.

Contacts: Ms. Elizabeth Chew
(301) 975-5236
elizabeth.chew@nist.gov

Mr. Richard Kissel
(301) 975-5017
richard.kissel@nist.gov

Ms. Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

### Performance Metrics for Information Security

In May 2006, NIST released Draft SP 800-80, *Guide for Developing Performance Metrics for Information Security*. This publication was built upon the methodology contained in NIST SP 800-55, *Security Metrics Guide for Information Technology Systems*. SP 800-80 provides managers and decision makers the ability to measure the effectiveness of security control families and processes to meet an organization's security and strategic objectives, which was an expansion of the SP 800-55 focus on implementation of the security controls reported in SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*.

Development and implementation of the metrics contained in Draft SP 800-80 were aligned with the security control families described in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. Review of the SP 800-80 public comments determined that SP 800-55 and Draft SP 800-80 should be combined into one document.

Work on the SP800-55 Revision 1 to merge Draft SP 800-80 and SP 800-55 was initiated in August 2006. Combining SP 800-80 and SP 800-55 will provide security managers with the methodology and tools needed to measure how well a program is meeting strategic objectives supporting business operation, and for the specific development, selection, and implementation of IT system-level metrics to be used to measure the performance of information security controls and techniques. The result will be Draft 800-55 Revision 1, scheduled for release in fiscal year 2007.

---

Contacts: Ms. Elizabeth Chew
(301) 975-5236
elizabeth.chew@nist.gov

Mr. Kevin Stine
(301) 975-4483
kevin.stine@nist.gov

Ms. Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

### Revision of the Guide to Information Technology Security Training Requirements

In 2005, CSD began to update SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*. Published in April 1998, SP 800-16 contains a training methodology that Federal departments and agencies, as well as private sector and academic institutions, can use to develop information security training material.

We are updating the document to align it with information security training requirements contained in FISMA and the Office of Personnel Management (OPM) information security awareness and training requirement of June 2004.

We expect the draft update of SP 800-16 to be completed during 2007.

---

Contacts: Mr. Mark Wilson
(301) 975-3870
mark.wilson@nist.gov

### Information Security Guide for Government Executives

NIST Interagency Report (IR) 7359, *Information Security Guide for Government Executives* provides a broad overview of information security program concepts to assist senior leaders in understanding how to oversee and support the development and implementation of information security programs. Management is responsible for—

1. Establishing the organization's information security program;
2. Setting program goals and priorities that support the mission of the organization; and
3. Making sure resources are available to support the security program and make it successful.

Senior leadership commitment to security is more important now than ever before. Studies have shown that senior management's commitment to information security initiatives is the number one critical element that impacts an information security program's success. Meeting this need necessitates senior leadership to focus on effective information security governance and support, which requires integration of security into the strategic and daily operations of an organization. When considering this challenge, five key security questions emerge for the executive—

1. What are the information security laws, regulations, standards, and guidance that I need to understand to build an effective security program?
2. What are the key activities to build an effective security program?
3. Why do I need to invest in security?
4. Where do I need to focus my attention in accomplishing critical security goals?
5. Where can I learn more to assist me in evaluating the effectiveness of my security program?

---

Contacts: Ms. Pauline Bowen
(301) 975-2938
pauline.bowen@nist.gov

Ms. Elizabeth Chew
(301) 975-5236
elizabeth.chew@nist.gov

### Glossary of Key Information Security Terms

Over the years, CSD has produced many information security guidance documents with definitions of key terms used. The definition for any given term was not standardized; therefore, there were multiple definitions for a given term. In 2004, we wanted to increase consistency in definitions for key information security terms in our documents.

The first step was a review of NIST publications (NIST Interagency Reports, Special Publications, and Federal Information Processing Standards) to determine how key information security terms were defined in each document. This review was completed in 2005 and resulted in a listing of each term and all definitions for each term. The glossary was then assembled and edited. Several rounds of internal and external reviews were completed, and comments and suggestions were incorporated into the document. The document was published in April 2006 as NISTIR 7298, *Glossary of Key Information Security Terms*.

In 2007, the Glossary will be updated to reflect new terms and any different definitions used in our publications.

Contacts: Mr. Richard Kissel
(301) 975-5017
richard.kissel@nist.gov

Ms. Tanya Brewer
(301) 975-4534
tbrewer@nist.gov

### Program Review for Information Security Management Assistance

Several sources of guidance, policies, standards, and legislative acts provide many requirements for Federal agencies when protecting entrusted information. Various assessments, reviews, and inspections are an outcome of these information security requirements to monitor Federal agency compliance. The manner in which these monitoring approaches are implemented may be very different, impacting Agency resource constraints. FISMA charged NIST to provide technical assistance to Federal agencies regarding compliance with the standards and guidelines developed for securing information systems, as well as information security policies, procedures, and practices. NIST Interagency Report (NISTIR) 7358, *Program Review for Information Security Management Assistance* (PRISMA) provides an overview of our program review methodology. PRISMA is a tool that we developed and implemented for reviewing the complex information security requirements and posture of a Federal program or agency. This report is provided as a framework for instructional purposes as well as to assist information security personnel, internal reviewers, auditors, and agency Inspector General (IG) staff personnel.

Contact: Ms. Pauline Bowen
(301) 975-2938
pauline.bowen@nist.gov

## Outreach, Awareness, and Education

CSD provides IT security standards and guidelines to Federal government agencies in the Executive Branch. One of our constant challenges is to provide useful and timely materials to these agencies. When developing and producing our products, we engage in consensus building with the IT industry, academia, and Federal agencies in order to keep the quality of these products and services as high as possible. As part of this consensus-building process, every FIPS publication and SP we produce has an open public comment vetting process. At the same time, we reach out to engage other governments, other levels of U.S. Government, small- and medium-size businesses nationwide, and even directly to citizens.

One of the primary benefits of these outreach efforts to the public is the large collection of nonproprietary, nontechnology-biased knowledge that is provided free of charge to Federal agencies and the public. Through a range of organizations and efforts, we provide materials, information, and services useful from the Federal agency level to the home-user level. We house a Web site that is a central repository for all of the materials and resources we have developed, as well as pointers to other types of IT security work and resources. We also host several organizations that address specific portions of government and industry. These organizations are discussed in greater detail later in this report.

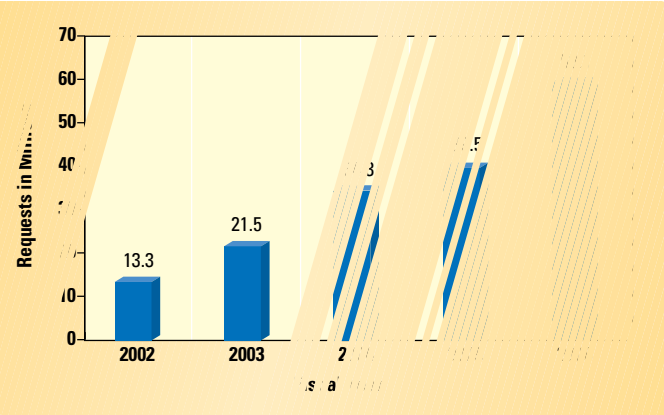
### Computer Security Resource Center

The Computer Security Resource Center (CSRC) is the Computer Security Division's Web site. CSRC is one of the top four most visited Web sites at NIST. We use the CSRC to encourage broad sharing of information security tools and practices, to provide "one-stop shopping" for information security standards and guidelines, and to identify and link key security Web resources to support the industry. The CSRC is an integral piece to all of the work we conduct and produce. It is our repository for everyone, public or private sector, wanting access to our documents and other IT security related information. CSRC serves as a vital link with the various groups we wish to reach.

During fiscal year 2006, CSRC had over 59 million requests—this includes the additional traffic coming from the National Vulnerability Database (NVD) that became active late in fiscal year 2005. Every document released for public comment or published through the Division has been posted to the CSRC.

During the past year, there has been a great deal of work to make the changes and improvements identified in the evaluation and analysis report that was drafted during 2003 and 2004. The site has been streamlined and simplified to make items easier to find, and an extensive site map has been developed. The search engine has been modified to find only results from the CSRC Web site, and not from other NIST Web servers or other non-NIST

Web sites. Several years ago, a publication awareness notification e-mail list was established to help keep those interested up to date with the latest publications posted to the CSRC Web site. Details on how to subscribe to this list are provided on the front page of CSRC. There are currently over 2,500 subscribers to this list.




CSRC will continue to grow and be updated in 2007. We are currently working on plans to improve the internal processes and policies of how to manage and update the CSRC Web site, as well as some redesign of the Web pages.

---

http://csrc.nist.gov/
Contact: Mr. Patrick O'Reilly
(301) 975-4751
patrick.oreilly@nist.gov

### The Information Security and Privacy Advisory Board

The Information Security and Privacy Advisory Board (ISPAB) is a Federal advisory committee that brings together senior professionals from industry, government, and academia to help advise the National Institute of Standards and Technology, the U.S. Office of Management and Budget (OMB), the Secretary of Commerce, and appropriate committees of the U.S. Congress about information security and privacy issues pertaining to unclassified Federal government information systems.

The membership of the Board consists of 12 individuals and a Chairperson. The Director of NIST approves membership appointments and appoints the Chairperson. Each Board member serves for a four-year term. The Board's membership draws from experience at all levels of information security and privacy work. The members' careers cover government, industry, and academia. Members have worked in the Executive and Legislative branches of the Federal government, civil service, senior executive service, the military, some of the largest corporations worldwide, small and medium-size businesses, and some of the top universities in the nation. The members' experience, likewise, covers a broad spectrum of activities including many different engineering disciplines, computer programming, systems analysis, mathematics, management positions, information technology auditing, legal experience, an extensive history of professional publications, and professional journalism. Members have worked (and in many cases, continue to work in their full-time jobs) on the development and evolution of some of the most important pieces of information security and privacy in the Federal government, including the Privacy Act of 1974, the Computer Security Act of 1987, the E-Government Act (including FISMA), and numerous e-government services and initiatives.

This combination of experienced, dynamic, and knowledgeable professionals on an advisory board provides NIST and the Federal government with a rich, varied pool of people conversant with an extraordinary range of topics. They bring great depth to a field that has an exceptional rate of change.

ISPAB was originally created by the Computer Security Act of 1987 [Public Law 100-35] as the Computer System Security and Privacy Advisory Board. As a result of FISMA, the Board's name was changed and its mandate was amended. The scope and objectives of the Board are to—

- Identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy;
- Advise NIST, the Secretary of Commerce, and the Director of OMB on information security and privacy issues pertaining to Federal government information systems, including thorough review of proposed standards and guidelines developed by NIST; and
- Annually report the Board's findings to the Secretary of Commerce, the Director of OMB, the Director of the National Security Agency, and the appropriate committees of the Congress.

The Board meets quarterly and all meetings are open to the public. We provide the Board with its Secretariat.

The Board has been very active in the past year. The work the Board completed this previous year included letters issued in November 2005 to Mr. Joshua Bolten, Director of OMB. The letters offer comments and advice on the review of the National Information Assurance Partnership (NIAP) and SHA-1's cryptanalytic attacks. A letter was also written to the new Director of OMB, Mr. Rob Portman, with recommendations regarding NIAP. These papers are publicly available in their entirety online.

The Board has also received numerous briefings from Federal and private sector representatives on a wide range of privacy and security topics in the past year.

*Pictured above, Left to Right:* **Back row** *Philip Reitinger, Howard A. Schmidt, Daniel Chenok, Fred Schneider, Brian Gouker, Joseph A. Guirreri;* **Front row** *Rebecca C. Leng, Leslie A. Reis, Susan Landau, Pauline Bowen, F. Lynn McNulty —* **Pictured right**, *Left to Right: Jaren P. Doherty, Peggy Himes*

Several areas of interest that the Board will be following in the coming year include privacy technology, Real ID, biometrics and ID management, security metrics, geospatial security and privacy issues, FISMA Reauthorization (and other legislative support), Information Systems Security Line of Business – (ISS LOB), national security community activities in areas relevant to civilian agency security (e.g., architectures), SCADA security, healthcare IT, security funding, the role of chiefs (such as CPO and CSO), NIST's outreach and partnering approaches, and cyber security leadership in the Executive Branch.

---

http://csrc.nist.gov/ispab/
Contact: Ms. Pauline Bowen
(301) 975-2938
pauline.bowen@nist.gov

### Federal Information Systems Security Educators' Association

The Federal Information Systems Security Educators' Association (FISSEA) is an organization run by and for Federal information systems security professionals. FISSEA assists Federal agencies in meeting their computer security training responsibilities. FISSEA strives to elevate the general level of information systems security knowledge for the Federal government and the Federally related workforce. FISSEA serves as a professional forum for the exchange of information and improvement of information systems security awareness, training, and education programs. It also seeks to provide for the professional development of its members.

Membership is open to information systems security professionals, trainers, educators, and managers who are responsible for information systems security training programs in Federal agencies, as well as contractors of these Agencies and faculty members of accredited educational institutions. There are no membership fees for FISSEA; all that is required is a willingness to share products, information, and experiences. Business is administered by an 11-member Executive Board that meets monthly. Board members serve two-year terms, and elections are held during the annual conference.

Each year an award is presented to a candidate selected as Educator of the Year; this award honors distinguished accomplishments in information systems security training programs. The Educator of the Year for 2005, awarded in March 2006, was Ms. K. Rudolph of Native Intelligence. There is also a contest for information security posters, Web sites, and awareness tools with the winning entries listed on the FISSEA Web site. FISSEA has a quarterly newsletter, an actively maintained Web site, and a listserve as a means of communication for members. Members are encouraged to participate in the annual FISSEA Conference and to serve on the FISSEA ad hoc task groups. We assist FISSEA with its operations by providing staff support for several of its activities and by being FISSEA's host agency.

FISSEA membership in 2006 spanned Federal agencies, industry, military, contractors, state governments, academia, the press, and foreign organizations to reach over 1,200 members in a total of 15 countries. The nearly 700 Federal agency members represent 89 Agencies from the Executive and Legislative branches of government.

Federal Information Systems Security Educators' Association
AWARENESS • TRAINING • EDUCATION

FISSEA conducted two free workshops during 2006. "What's New in Security Awareness, Training, and Education" was held on April 25th and was conducted by FISSEA Board members Barbara Cuffie, Louis Numkin, Susan Hansche, and Jim Litchko. On August 30th, Mark Wilson (NIST) and Susan Hansche (FISSEA Board) conducted "Identifying Step One of Information Security Role-based Training – Who Has Significant Security Responsibilities?" FISSEA will continue to offer free workshops in 2007.

The 2007 FISSEA Conference, "FISSEA 20: Looking Forward . . . Securing Today," will be held March 12-13, 2007 at the Bethesda North Marriott Hotel and Conference Center in Bethesda, Maryland. Information security awareness, resources, and FISMA will be discussed in the two-day, two-track conference. The FISSEA Conference provides a great networking opportunity for attendees. There will also be a one-day vendor exhibition. Further information regarding the conference is available on the FISSEA Web site.

---

http://csrc.nist.gov/fissea/

Contacts: Mr. Mark Wilson
(301) 975-3870
mark.wilson@nist.gov

Ms. Peggy Himes
(301) 975-2489
peggy.himes@nist.gov

### Small and Medium-Size Business Outreach

What do a business's invoices have in common with e-mail? If both are done on the same computer, the business owner may want to think more about computer security. Information—payroll records, proprietary information, client or employee data—is essential to a business's success. A computer failure or other system breach could cost a business anything from its reputation to damages and recovery costs. The small business owner who recognizes the threat of computer crime and takes steps to deter inappropriate activities is less likely to become a victim.

The vulnerability of any one small business may not seem significant to many other than the owner and employees of that business. However, over 20 million U.S. businesses—over 95 percent of all U.S. businesses—are small and medium-size businesses (SMBs) of 500 employees or less. Therefore, a vulnerability common to a large percentage of all SMBs could pose a threat to the Nation's economic base. In the special arena of information security, vulnerable SMBs also run the risk of being compromised for use in crimes against governmental or large industrial systems upon which everyone relies. SMBs frequently cannot justify an extensive security program or a full-time expert. Nonetheless, they confront serious security challenges and must address security requirements based on identified needs.

The difficulty for these businesses is to identify needed security mechanisms and training that are practical and cost-effective. Such businesses also need to become more educated in terms of security so that limited resources are well applied to meet the most obvious and serious threats.


To address this need, NIST, the Small Business Administration (SBA), and the Federal Bureau of Investigation (FBI) entered into a co-sponsorship agreement for the purpose of conducting a series of training meetings on computer security for small businesses. The purpose of the meetings is to have individuals knowledgeable in computer security provide an overview of information security threats, vulnerabilities, and corresponding protective tools and techniques with a special emphasis on providing useful information that small business personnel can apply directly or use to task contractor personnel. In 2006, eighteen SMB workshops were held across the country.

While NIST, the SBA, and the FBI recognized the quality and effectiveness of these workshops, there are limits to our outreach capabilities. The National Cyber Security Alliance (NCSA), funded primarily by the Department of Homeland Security, began a pilot project "Train the Trainers" which would address this limitation. The pilot project recruited six volunteer presenters. We hosted a training day on September 20, 2006, for the volunteer presenters to be trained in scheduling and providing the information security workshop presentation. With this training completed, the volunteer presenters are providing SMB information security workshops in their home areas.

In 2007, the SMB outreach effort will focus on expanding opportunities to reach more small businesses. Further development of our Web site is planned. Discussions are under way with SBA and the FBI to expand the original partnership and to determine new avenues for this outreach project.

In January 2007, two half-day workshops will be held San Jose and San Francisco, CA. Similar workshops will be held in March 2007 in Sacramento and Silicon Valley, CA. In addition to these workshops, an additional three trips will be undertaken to provide workshops in other underserved U.S. areas.

Finally, we plan to send a representative to the 2007 InfraGard National Congress, where a presentation on this outreach may be given.

---

http://csrc.nist.gov/securebiz/

Contacts: Mr. Richard Kissel
(301) 975-5017
richard.kissel@nist.gov

http://sbc.nist.gov/

Ms. Tanya Brewer
(301) 975-4534
tbrewer@nist.gov

## Federal Computer Security Program Managers' Forum

The Federal Computer Security Program Managers' Forum (Forum) is an informal group of over 500 members sponsored by NIST to promote the sharing of security related information among Federal agencies. The Forum strives to provide an ongoing opportunity for managers of Federal information security programs to exchange information security materials in a timely manner, to build upon the experiences of other programs, and to reduce possible duplication of effort. It provides an organizational mechanism for us to exchange information directly with Federal agency information security program managers in fulfillment of our leadership mandate under FISMA. It assists us in establishing and maintaining relationships with other individuals or organizations that are actively addressing information security issues within the Federal government. Finally, it helps us and Federal agencies in establishing and maintaining a strong, proactive stance in the identification and resolution of new strategic and tactical IT security issues as they emerge.

The Forum hosts the Federal Agency Security Practices (FASP) Web site, maintains an extensive e-mail list, and holds an annual off-site workshop and bimonthly meetings to discusses current issues and developments of interest to those responsible for protecting sensitive (unclassified) Federal systems [except "Warner Amendment" systems, as defined in 44 USC 3502 (2)]. Ms. Marianne Swanson serves as the Chairperson of the Forum. We also serve as the secretariat of the Forum, providing necessary administrative and logistical support. Participation in Forum meetings is open to Federal government employees who participate in the management of their organization's information security program. There are no membership dues.

Topics of discussion at Forum meetings in the last year have included briefings on personal identity verification (PIV), a special workshop on the proposed changes to NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, National Vulnerability Database and patch management, risk assessment, accreditation approaches, and the Cryptographic Module Validation Program. This year's annual off-site meeting featured updates on the computer security activities of the U.S. Government Accountability Office, NIST, the U.S. Office of Management and Budget, and the activities of the Department of Homeland Security. Briefings were also provided on media sanitization, configuration checklists, the Security Line of Business, enterprise architecture, wireless security, and updates on several NIST Special Publications.

---

http://csrc.nist.gov/organizations/cspmf.html
Contact: Ms. Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

## Security Practices and Policies

Today's Federal networks and systems are highly interconnected and interdependent with nonfederal systems. Protection of the Nation's critical infrastructures is dependent upon effective information security solutions and practices that minimize vulnerabilities associated with a variety of threats. The broader sharing of such practices will enhance the overall security of the Nation. Information security practices from the public and private sector can sometimes be applied to enhance the overall performance of Federal information security programs. We are helping to facilitate a sharing of these practices and implementation guidelines in multiple ways.

The Federal Agency Security Practices (FASP) effort was initiated as a result of the success of the Federal Chief Information Officers Council's Federal Best Security Practices (BSP) pilot effort to identify, evaluate, and disseminate best practices for critical infrastructure protection and security. We were asked to undertake the transition of this pilot effort to an operational program. As a result, we developed the FASP Web site. The FASP site contains agency policies, procedures and practices, the Federal Chief Information Officers Council's pilot BSPs, and a Frequently Asked Questions (FAQ) section. The FASP site differs from the BSP pilot in material provided and complexity.

The FASP area contains a list of categories found in many of the NIST Special Publications. Based on these categories, agencies are encouraged to submit their IT security information and IT security practices for posting on the FASP site so they may be shared with others. Any information on, or samples of, position descriptions for security positions and statements of work for contracting security-related activities are also encouraged. In the past year, 19 practices and examples were added to the collection, bringing the total to 188.

We also invite public and private organizations to submit their information security practices to be considered for inclusion on the list of practices maintained on the Web site. Policies and procedures may be submitted to us in any area of information security, including accreditation, audit trails, authorization of processing, budget planning and justification, certification, contingency planning, data integrity, disaster planning, documentation, hardware and system maintenance, identification and authentication, incident handling and response, life cycle, network security, personnel security, physical and environmental protection, production input/output controls, security policy, program management, review of security controls, risk management, security awareness training and education (to include specific course and awareness materials), and security planning.

The coming year will see an effort to continue the momentum to expand the number of sample practices and policies made available to Federal agencies and the public. We are currently identifying robust sources for more samples to add to this growing repository.

---

http://fasp.nist.gov/

Contacts: Ms. Pauline Bowen
(301) 975-3293
pauline.bowen@nist.gov

Mr. Mark Wilson
(301) 975-3870
mark.wilson@nist.gov

# Security Testing and Metrics

**STRATEGIC GOAL** ▸ ***Improve the security and technical quality of cryptographic products needed by Federal agencies (in the United States, Canada, and United Kingdom) and industry by developing standards, test methods and validation criteria, and the accreditation of independent third party testing laboratories.***

## Overview

Every IT product available makes a claim as to functionality and/or offered security. When protecting sensitive data, government agencies need to have a minimum level of assurance that a product's stated security claim is valid. There are also legislative restrictions regarding certain types of technology, such as cryptography, that require Federal agencies to use only tested and validated products.

Federal agencies, industry, and the public rely on cryptography for the protection of information and communications used in electronic commerce, critical infrastructure, and other application areas. At the core of all products offering cryptographic services is the cryptographic module. Cryptographic modules, which contain cryptographic algorithms, are used in products and systems to provide security services such as confidentiality, integrity, and authentication. Although cryptography is used to provide security, weaknesses such as poor design or weak algorithms can render the product insecure and place highly sensitive information at risk. Adequate testing and validation of the cryptographic module and its underlying cryptographic algorithms against established standards is essential to provide security assurance.

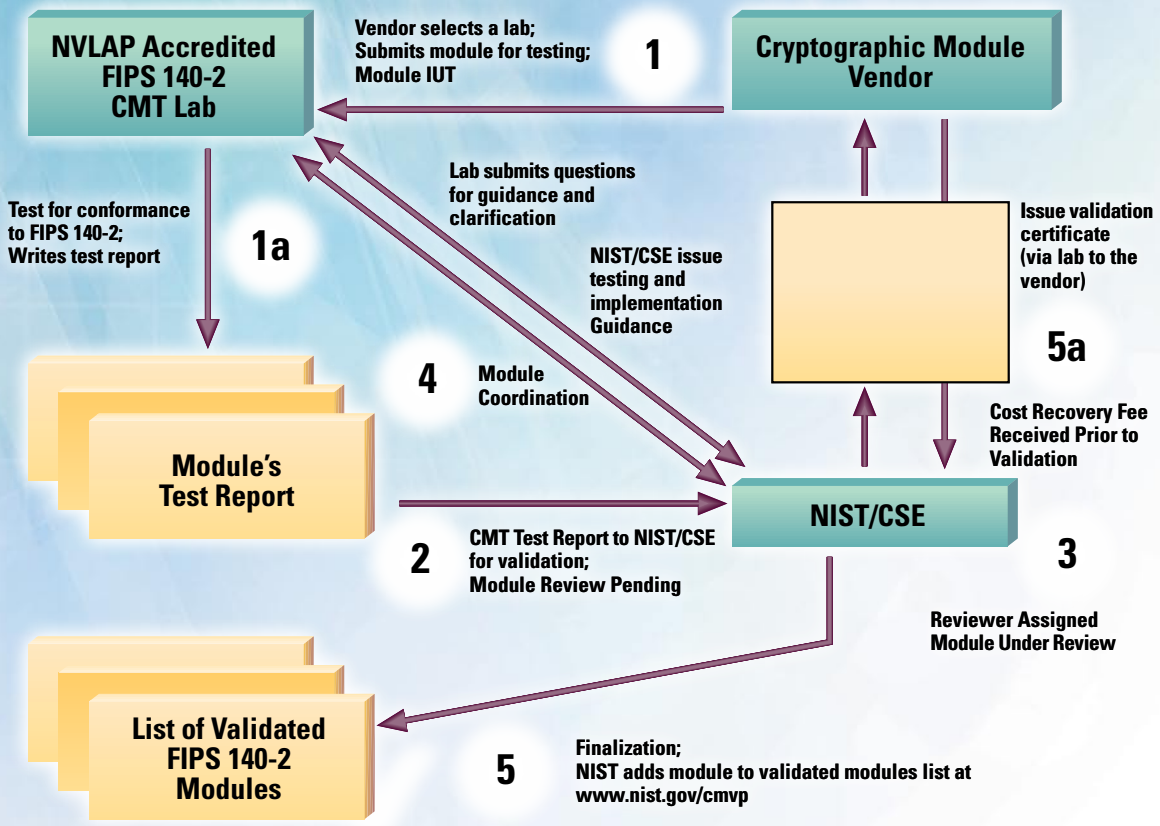
Our testing-focused activities include the validation of cryptographic modules and cryptographic algorithm implementations, accreditation of independent testing laboratories, development of test suites, providing technical support to industry forums, and conducting education, training, and outreach programs.

Activities in this area have historically, and continue to, involve large amounts of collaboration and the facilitation of relationships with other entities. Federal agencies that have collaborated recently with these activities are the Department of State, the Department of Commerce, the Department of Defense, the General Services Administration, the National Aeronautics and Space Administration, the National Security Agency, the Department of Energy, the U.S. Office of Management and Budget, the Social Security Administration, the United States Postal Service, the Department of Veterans Affairs, the Federal Aviation Administration, and NIST's National Voluntary Laboratory Accreditation Program. The list of industry entities that have worked with us in this area is long and includes the American National Standards Institute (ANSI), Oracle, Cisco Systems, Lucent Technologies, Microsoft Corporation, International Business Machines (IBM), VISA, MasterCard, Computer Associates, RSA Security, Research in Motion, Sun Microsystems, Network Associates, Entrust, and Fortress Technologies. The Division also has collaborated at the global level with Canada, the United Kingdom, France, Germany, India, Japan, and Korea in this area.

## Validation Programs and Laboratory Accreditation

The underlying philosophy of the Cryptographic Module Validation Program (CMVP) and the Cryptographic Algorithm Validation Program (CAVP) is that the user community needs strong independently tested and commercially available cryptographic products. The programs work with the commercial sector and the cryptographic community to achieve security, interoperability, and assurance. Directly associated with this philosophy is the goal to promote the use of validated products and provide Federal agencies with a security metric to use in procuring cryptographic modules. The testing performed by accredited laboratories provides this metric. Federal agencies, industry, and the public can choose products from the CMVP Validated Modules List and have confidence that the products meet the claimed level of security.

The CMVP offers a documented methodology for conformance testing through a defined set of security requirements in FIPS 140-2, *Security*




*Requirements for Cryptographic Modules*, and other cryptographic standards. We developed the standard and an associated metric (the Derived Test Requirements) to ensure repeatability of tests and equivalency in results across the testing laboratories. The commercial Cryptographic Module Testing (CMT) laboratories accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) provide vendors of cryptographic modules a choice of testing facilities and promote healthy competition.

### Laboratory Accreditation

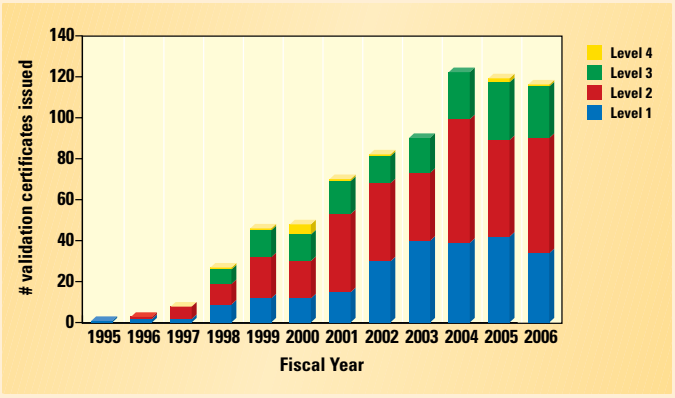
Vendors of cryptographic modules and algorithms use independent, private sector testing laboratories accredited as CMT laboratories by NVLAP to have their cryptographic modules validated by the Cryptographic Module Validation Program (CMVP) and their cryptographic algorithms validated by the Cryptographic Algorithm Validation Program (CAVP). As the worldwide growth and use of cryptographic modules has increased, demand to meet the testing needs for both algorithms and modules developed by vendors has also grown. NVLAP has received several applications for the accreditation of CMT Laboratories, which has resulted in the accreditation of one new U.S. based CMT Laboratory in 2006 and one other laboratory in the accreditation process. This brings the current total number of accredited CMT Laboratories to 13, spanning locations in the United States, Canada, the United Kingdom, and Germany. A complete list may be found at **http://csrc.nist.gov/cryptval/1401labs.htm**.

On October 11, 2006, after more than two years of negotiations, the NIST CMVP and the Information-technology Promotion Agency (IPA) of the Government of Japan signed and established a non-binding programmatic relationship between the CMVP and the Japanese CMVP (JCMVP) for the development and sharing of programmatic guidance. The basis of this understanding and of the relationship between CMVP and JCMVP is to support, to the extent possible, Japanese CMTLs to become accredited by NVLAP for cryptographic module testing, and to assist JCMVP to accurately comprehend CMVP requirements and technical guidance. To facilitate this, the JCMVP intends to discuss its interpretation of the CMVP and FIPS 140-2 requirements, in order to request guidance on the program and other related issues as appropriate. Accreditation of CMT Laboratories in Japan is anticipated during FY 2007.

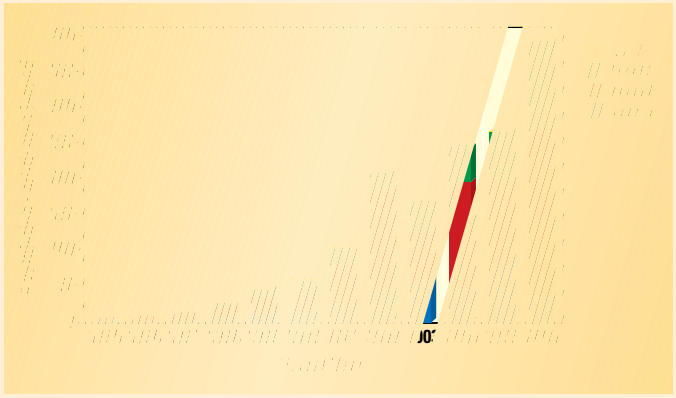
---

http://ts.nist.gov/Standards/214.cfm
Contact: Mr. Randall Easter
(301) 975-4641
randall.easter@nist.gov

FIPS 140-1 and FIPS 140-2 Validation Certificates Issued by Year and Level




FIPS 140-1 and FIPS 140-2 Validated Modules by Year and Level



## Cryptographic Module Validation Program and Cryptographic Algorithm Validation Program

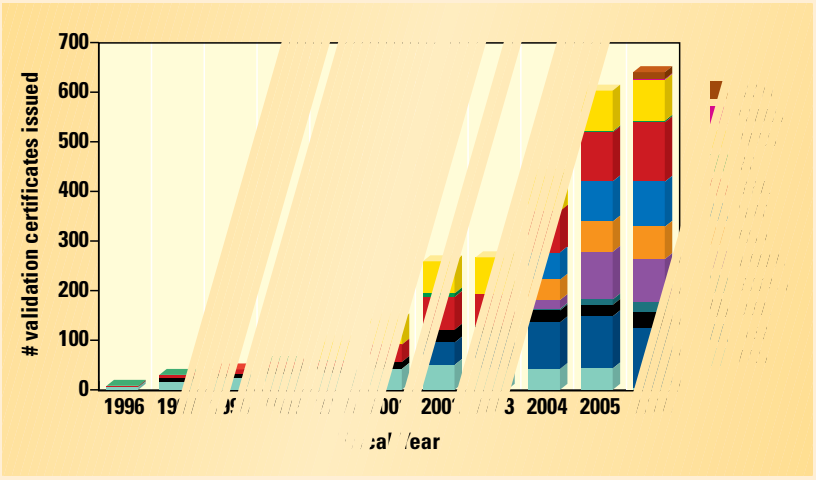
The CMVP and the CAVP are separate, collaborative programs based on a partnership between NIST's Computer Security Division (CSD) and the Communication Security Establishment (CSE) of the Government of Canada. The programs provide Federal agencies—in the United States, Canada, and the United Kingdom—with confidence that a validated cryptographic module meets a claimed level of security and that a validated cryptographic algorithm has been implemented correctly. The CMVP/CAVP validate modules and algorithms used in a wide variety of products including secure Internet browsers, secure radios, smart cards, space based communications, tokens, and products supporting Public Key Infrastructure and electronic commerce. One module may be used in several products so that a small number of modules may account for hundreds of products. Likewise, the CAVP validates cryptographic algorithms that may be housed in one or more cryptographic modules.

To give a sense of the quality improvement that both the CMVP and the CAVP achieve, consider that our statistics from the testing laboratories show that out of the first 200 modules tested, 48 percent of the cryptographic modules and 27 percent of the cryptographic algorithms brought in for voluntary testing had security flaws that were corrected during testing. In other words, without this program, the Federal government would have had only a 50-50 chance of buying correctly implemented cryptography. To date, over 720 certificates have been issued, which represents over 1,500 validated modules by the CMVP. These modules have been developed by over 175 international vendors.

This year, the CMVP issued 110 module validation certificates. While the number of module validation certificates issued in 2006 was commensurate with the number in 2005, the number of actual modules represented increased by 50 percent over 2005. The number of modules in the CMVP pre-validation queue continues to grow, representing significant growth in future validation efforts. The CAVP issued 635 algorithm validation certificates, as compared to 611 algorithm validation certificates in 2005. Part of the increase in the number of algorithm validation certificates issued is due to the addition of the validation testing for the CMAC Mode for Authentication applicable to both the Advanced Encryption Standard (AES) and Triple Data Encryption Algorithm (TDEA) algorithms.

The new mode of operation—the CMAC algorithm—is a message authentication code (MAC) algorithm based on a symmetric key block cipher. It may be used to provide assurance of the authenticity and hence the integrity of binary data. CMAC can be considered a mode of operation

The Progress of the CAVP



of the block cipher because it is based on an approved symmetric key block cipher, such as the AES algorithm and the TDEA.

---

http://csrc.nist.gov/cryptval/

CMVP Contact: Mr. Randall Easter
(301) 975-4641
randall.easter@nist.gov

CAVP Contact: Ms. Sharon Keller
(301) 975-2910
sharon.keller@nist.gov

### Automated Security Testing and Test Suite Development

Each approved and recommended cryptographic algorithm has an associated reference called a FIPS publication or a NIST SP. The detailed instructions on how to implement the specific algorithm are found in these references. Based on these instructions, we design and develop validation test suites containing tests that verify that the detailed instructions of an algorithm are implemented correctly and completely. These tests exercise the mathematical formulas involved in the algorithm to assure that they work properly for each possible scenario. If the implementer deviates from these instructions or excludes any part of the instructions, the validation test will fail, indicating that the algorithm implementation does not function properly.

These validation tests are designed to assist in the detection of accidental implementation errors and are not designed to detect intentional attempts to misrepresent conformance. Thus, validation should not be interpreted as an evaluation or endorsement of overall product security.

There are several types of validation testing for each approved cryptographic algorithm. These include, but are not limited to, Known Answer Tests, Monte Carlo Tests, and Multi-block Message Tests. The Known Answer Tests are designed to test the conformance of the implementation under test (IUT) to the various specifications in the reference. This involves testing the components of the algorithm to assure that they are implemented correctly. The Monte Carlo Test is designed to exercise the entire IUT. This test is designed to detect the presence of implementation flaws that are not detected with the controlled input of the Known Answer Tests. The types of implementation flaws detected by this validation test include pointer problems, insufficient allocation of space, improper error handling, and incorrect behavior of the IUT. The Multi-block Message Test (MMT) is designed to test the ability of the implementation to process multi-block messages, which require the chaining of information from one block to the next. Other types of validation testing exist to satisfy other testing requirements of cryptographic algorithms.

Automated security testing and test suite development are integral components of the Cryptographic Algorithm Validation Program (CAVP). The CAVP encompasses validation testing for FIPS-approved and NIST-recommended cryptographic algorithms. Cryptographic algorithm validation is a prerequisite to the Cryptographic Module Validation Program (CMVP). All of the tests under the CAVP are handled by the 13 third-party laboratories that are accredited as CMT laboratories by NVLAP. We develop and maintain a Cryptographic Algorithm Validation System (CAVS) tool which automates the validation testing. The CAVS currently has algorithm validation testing for the following cryptographic algorithms—

- The Triple Data Encryption Standard Algorithm (TDES)
- The Advanced Encryption Standard (AES) algorithm
- The Digital Signature Standard (DSS)
- Hashing algorithms SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512
- Three random number generator (RNG) algorithms
- The RSA algorithm
- The Keyed-Hash Message Authentication Code (HMAC)
- The Counter with Cipher Block Chaining-Message Authentication Code (CCM) mode
- The CMAC Mode for Authentication
- The Elliptic Curve Digital Signature Algorithm (ECDSA).

In FY 2007, we will be adding validation testing for the following algorithms—

- SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*
- SP 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*
- Draft FIPS 186-3, *Digital Signature Standard (DSS)*—an updated DSS to accommodate for the increased SHA sizes and key sizes
- Transport Layer Security (TLS) protocol
- IEEE 802.11i protocol

---

http://csrc.nist.gov/cryptval/
Contact: Ms. Sharon Keller
(301) 975-2910
sharon.keller@nist.gov

## Cryptographic Validation Standards

With the passage of FISMA, there is no longer a statutory provision to allow for agencies to waive mandatory FIPS. Therefore, except when using National Security Agency-approved cryptography, all Agencies must use cryptography validated under FIPS 140-2, *Security Requirements for Cryptographic Modules*. This standard specifically requires all hardware, software, and

firmware employing cryptography—whether commercial-off-the-shelf or government-produced—to be validated through the Cryptographic Module Validation Program (CMVP) when used for the protection of sensitive unclassified information. Agency acquisition, development, and use of any hardware, software, or firmware using unvalidated cryptography for the protection of sensitive unclassified information are not permitted and no other validation process can substitute for FIPS validation.

### Revision of FIPS 140-2, *Security Requirements for Cryptographic Modules*

FIPS 140-2, *Security Requirements for Cryptographic Modules* provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks. The standard provides users with a specification of security features that are required at each of four security levels; flexibility in choosing security requirements; a guide to ensuring that the cryptographic modules incorporate necessary security features; and the assurance that the modules are compliant with cryptography-based standards.

In addition to constant analysis for new technologies, the standard is officially reexamined and reaffirmed every five years. In the fall of 2004, FIPS 140-2 entered the regularly scheduled 5-year review for revision to FIPS 140-3. We are developing FIPS 140-3 to meet the new and revised requirements of Federal agencies for cryptographic systems, and to address technological and economic changes that have occurred since the issuance of FIPS 140-2 in 2001. As the first step in the development of FIPS 140-3, we invited comments from the public, users, the information technology industry, and Federal, state, and local government organizations concerning the need for and recommendations for a new standard. We were specifically interested in comments in the areas of compatibility with industry standards, new technology areas, introduction of additional levels of security, additional requirements specific to physical security, and portability of applications (including operating systems) based on platform and/or environment.

In September 2005, a workshop was conducted to address the areas of physical security protection methods and current state of the art in methods of attacks and compromise of cryptographic modules. The first draft of FIPS 140-3 underwent further development and research in FY 2006 as we reviewed the comments received and addressed the areas of the standard identified for improvement. The current draft identifies five, rather than four, increasingly demanding levels of security assurance. Among other recommended changes were the stronger requirements on user authentication and data integrity verification, a new section focused on software modules, and the requirements to mitigate against noninvasive attacks that were not even feasible several years ago.

In the second quarter of FY 2007, the draft standard will be presented to the public for comment. Upon the completion of the 90-day comment period and following the review of the received comments, we may schedule a public workshop to discuss any complex technological issues. A second draft of FIPS 140-3 should be published by late FY 2007 or early FY 2008. Once the comments to the second draft are reviewed, the final version of FIPS 140-3 will be submitted to the Secretary of Commerce. Six months after the Secretary's signature, the new standard will take effect. In parallel we are developing a set of the Derived Test Requirements for FIPS 140-3 and a plan to facilitate the transition from FIPS 140-2 to FIPS 140-3.

---

http://csrc.nist.gov/cryptval/
Contact: Dr. Allen Roginsky
(301) 975-3603
allen.roginsky@nist.gov

### ISO Standardization of Cryptographic Module Testing

Work reached fruition during 2006 on the establishment of FIPS 140-2, *Security Requirements for Cryptographic Modules*, as an International Organization for Standardization (ISO) standard with the publishing in March 2006 of ISO/IEC 19790, *Security requirements for cryptographic modules*. With the publishing of ISO/IEC 19790, Subcommittee 27 (SC27) approved and began work on ISO/IEC 24759, *Test requirements for cryptographic modules*. This project is registered in the work program of the International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee 1 Subcommittee 27 on IT Security Techniques (ISO/IEC JTC 1/SC 27-IT Security Techniques). When completed, this effort will bring consistent testing of cryptographic modules in the global community.

---

http://csrc.nist.gov/cryptval/
Contact: Mr. Randall Easter
(301) 975-4641
randall.easter@nist.gov

# Security Technology

**STRATEGIC GOAL** ▸ *Develop and improve mechanisms to protect the integrity, confidentiality, and authenticity of Federal agency information by developing security mechanisms, standards, testing methods, and supporting infrastructure requirements and methods.*

## Overview

Our work in cryptography is making an impact within and outside the Federal government. Strong cryptography improves the security of systems and the information they process. IT users also enjoy the enhanced availability in the marketplace of secure applications through cryptography, Public Key Infrastructure (PKI), and e-authentication. Work in this area addresses such topics as secret and public key cryptographic techniques, advanced authentication systems, cryptographic protocols and interfaces, public key certificate management, biometrics, smart tokens, cryptographic key escrowing, and security architectures. This year, the work called for in the Homeland Security Presidential Directive 12 (HSPD-12) has continued. A few examples of the impact this work has had include changes to Federal employee identification methods, how users authenticate their identity when needing government services online, and the technical aspects of passports issued to U.S. citizens.

CSD collaborates with a number of national and international agencies and standards bodies to develop secure, interoperable security standards. Federal agency collaborators include the Department of Energy, the Department of State, the National Security Agency (NSA), and the Communications Security Establishment of Canada, while national and international standards bodies include the American Standards Committee (ASC) X9 (financial industry standards), the International Organization for Standardization (ISO), the Institute of Electrical and Electronic Engineers (IEEE) and the Internet Engineering Task Force (IETF). Industry collaborators include BC5 Technologies, Certicom, Entrust Technologies, Hewlett Packard, InfoGard, Microsoft, NTRU, Pitney Bowes, RSA Security, Spyrus, and Wells Fargo.

## Cryptographic Standards Toolkit

The Cryptographic Standards toolkit (CS-Toolkit) provides a basis for the selection of cryptographic security components and functionality for the protection of the U.S. Government's data, communications, and operations. The CS-Toolkit helps to ensure a worldwide government and industry use of strong, interoperable cryptography by using standard algorithms. The CS-Toolkit also provides guidance and education in the use of cryptography. It includes a wide variety of cryptographic algorithms and techniques for encryption, authentication, digital signatures, key establishment, and random number generation. The CS-Toolkit is a collection of standards and guidelines; it does not include software implementations of these algorithms.

### Hash Algorithms

A hash function takes binary data, called the message, and produces a condensed representation, called the message digest. A cryptographic hash function is a hash function that is designed to achieve certain security properties and is typically used with other cryptographic algorithms, such as digital signature algorithms, key derivation algorithms, keyed-hash message authentication codes, or in the generation of random numbers (bits). As a security primitive, cryptographic hash functions are frequently embedded in Internet protocols or in other applications; the two most commonly used cryptographic hash functions are MD5, which has been broken and is no longer approved for Federal agency use, and the NIST-approved SHA-1.

FIPS 180-2, *Secure Hash Standard*, specifies five algorithms for computing cryptographic hash functions—SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512. These five algorithms are called secure because, for a given algorithm, it is computationally infeasible (1) to find a message that

corresponds to a given message digest, and (2) to find two different messages that produce the same message digest.

In 2005, a vulnerability was identified in the SHA-1 hash algorithm. In response, NIST held two cryptographic hash function workshops to assess the status of NIST's approved hash functions and to discuss the latest hash function research. NIST has decided that it would be prudent to develop one or more additional hash functions through a public competition similar to the development process for the Advanced Encryption Standard (AES). Based on feedback from the workshops, draft minimum acceptability requirements, submission requirements, and evaluation criteria have been provided for public comment, with the expectation that the competition will be launched in 2007.

In the past year, a revised version of the Digital Signature Standard (DSS), to be known as FIPS 186-3, was provided for public review and comment, as well as a related document, NIST SP 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications*. The DSS revision included additional key sizes for the Digital Signature Algorithm (DSA) to provide higher security strengths and guidance on the use of RSA and the Elliptic Curve Digital Signature Algorithm (ECDSA) to promote interoperability. SP 800-89 specifies methods for obtaining the assurances necessary to determine that digital signatures are valid. SP 800-89 has been completed, and the comments received on the draft of FIPS 186-3 are being addressed.

Random numbers are needed to provide the required security for most cryptographic algorithms. For example, random numbers are used to generate the keys needed for encryption and digital signature applications. NIST SP 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators (DRBGs)*, was completed and is available on our Web site. Additional work is being conducted with Accredited Standards Committee X9 (ASC X9) to provide guidance for the development of entropy sources and the construction of Random Bit Generators from entropy sources and DRBGs.

An authenticated encryption algorithm called the Galois Counter Mode (GCM) was submitted to NIST as part of the ongoing development of modes of operation of AES. GCM provides assurance of the authenticity of data as well as its confidentiality. GCM is parallelizable and efficient, so it is especially attractive for high-throughput applications, such as high-speed Internet routers. The algorithm will be recommended in SP 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication*. A draft of this document was provided for a period of public review in the last year and is expected to be published soon.

Another mode of operation of the AES algorithm is slated for recommendation soon—the AES Key Wrap (AESKW). Like GCM, AESKW uses the AES algorithm in a manner that combines assurance of confidentiality with authenticity. AESKW is intended for the protection of cryptographic keys and other specialized data without requiring a nonce, i.e., a unique per-message value. Although AESKW is not efficient, its security is believed to be particularly robust. A draft specification is expected to be provided for public review this year.

---

Contacts: Ms. Shu-jen Chang (Hash functions)
(301) 975-2940
shu-jen.chang@nist.gov

Dr. Morris Dworkin (Modes)
(301) 975-2354
morris.dworkin@nist.gov

Ms. Elaine Barker (Digital signatures, RNG)
(301) 975-2911
ebarker@nist.gov

## Key Management

### *Recommendation for Key Management*

The requirements for key management continue to expand as new types of devices and connectivity mechanisms become available (e.g., laptops, broadband access, Blackberries). We are continuing to address the needs of the Federal government by defining the basic principles required for key management, including key establishment, wireless applications, and the PKI (Public Key Infrastructure).

Modifications were made to SP 800-57, *Recommendation for Key Management—Part 1: General*, that included an indication of the appropriate hash functions to be used for additional applications, depending on the security strength. Part 1 provides general guidance and best practices for the management of cryptographic keying material. Part 3 of SP 800-57 on application-specific guidance is under development and is expected to be available for initial public comment in 2007. Part 3 is intended to address the key management issues associated with currently available cryptographic mechanisms.

### *Key Establishment using Public Key Cryptography*

Key management efforts have included the completion of SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, and the commencement of a related document, SP 800-56B, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography* (e.g., RSA).

***Key Management for Wireless Applications***

As they become a more convenient way to access the Internet, wireless technologies are being more widely adopted by government agencies. However, while wireless technologies can provide connections for mobile users, they are also vulnerable to various attacks. Security protocols have been developed by the Institute of Electrical and Electronics Engineers, Inc. (IEEE), the Internet Engineering Task Force (IETF), and other industry standards bodies in order to protect wireless networks and communications.

A new feature for wireless service is to allow a fast transition between different access points, called a handoff. This fast handoff proposes a new challenge to cryptographic key management. To make the handoff truly fast, cryptographic keys are derived and distributed among different access points so that whenever a mobile station is roaming to a different access point, the keys are ready for a secure connection. A key hierarchy is derived from a master key for the fast handoff purpose.

The primary security concerns are related to key establishment among multiple key holders. This is further complicated because, unlike a cellular system, a mobile station determines when to make a transition from one access point to another. This makes it more difficult for the network to coordinate the key establishment among multiple parties in a secure manner.

In order to make proper recommendations on key management in a timely manner for government agencies, we worked with IEEE 802.11 Task Group R to develop key management protocols and key derivation functions. The early involvement has made it possible to influence the industry standards in a more efficient and direct way to comply with government requirements. We are also simultaneously developing recommendations on key management for wireless and mobility, which will be included as one of the SP 800 series of documents. It is planned to extend the practice to other wireless standards, such as IEEE 802.16, in 2007.

***Public Key Infrastructure***

We continue to support the development and enhancement of key management standards related to Public Key Infrastructure (PKI). This standards work is primarily performed in the Internet Engineering Task Force (IETF), where NIST contributes coeditors for three documents under development within the Public Key Infrastructure X.509 (PKIX) working group. In 2006, work continued on a revised version of the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. This document, which profiles the X.509 standard for public key certificates and CRLs, is used as the basis for the development of most PKI products and the deployment of PKIs in both the public and private sector. NIST is also editing a companion document that specifies the encoding of certificates and CRLs that include public keys and digital signatures that are based on elliptic curves and the NIST-approved hash functions. Work on a third document, the *Server-based Certificate Validation Protocol (SCVP)*, neared completion in FY 2006. SCVP specifies a protocol that allows the work of validating certificates to be off-loaded to a delegated validation server.

We are also developing procedures and tools to determine the functionality and standards conformance of PKI components. NIST serves as cochair of the Path Discovery and Validation Working Group, a Federal multiagency working group that works with commercial vendors to increase the number of applications that are capable of using PKI to authenticate users. The working group concentrates on identifying applications that can utilize the Federal PKI and the Federal Bridge Certification Authority (FBCA) to authenticate users who have been issued credentials by different organizations. The working group uses certification path discovery and validation test suites that were developed by NIST to verify the ability of applications to build and validate certification paths as required to perform cross-organization validation of credentials.

In addition to PKI standards and testing, we are focused on deploying a robust and comprehensive Federal PKI (FPKI). NIST is a member of the FPKI Policy Authority, which manages the FBCA and the Common Policy Root CA, and arbitrates requests by Agencies or other entities to join the FPKI. During 2006, the FBCA was directed to cross-certify with four agency PKIs, one corporate PKI, and a commercial Bridge CA. Most notably, the FBCA cross-certified with the CertiPath bridge CA, which serves the aerospace industry. Cross-certification with industry bridge CAs is expected to be the primary means for FPKI recognition of academic and industry partners in the future.

While agency PKIs for the early adopters are cross-certified with the FBCA, agencies currently deploying PKI are procuring the services of approved PKI service providers operating under a common certificate policy. NIST is a key participant in the Shared Service Provider Working Group that evaluates and approves the operations of these service providers. During 2006, a fourth shared service provider was approved and was issued the requisite CA certificate by the Common Policy Root CA. At the end of 2006, three additional service providers were in the review process.

---

Contacts: Ms. Shu-jen Chang (Hash functions)
(301) 975-2940
shu-jen.chang@nist.gov

Ms. Elaine Barker (Digital signatures, RNG, SP 800-56B, SP 800-57)
(301) 975-2911
ebarker@nist.gov

Dr. Morris Dworkin (Modes)
(301) 975-2354
morris.dworkin@nist.gov

Dr. Lily Chen (Wireless)
(301) 975-6974
lily.chen@nist.gov

Mr. Tim Polk (PKI)
(301) 975-3348
william.polk@nist.gov

Dr. David Cooper (PKI)
(301) 975-3194
david.cooper@nist.gov

## Authentication

CSD has expanded its efforts to develop technical guidance for electronic authentication. This program area began with the development of SP 800-63, *Electronic Authentication Guideline*, which supports the Office of Management and Budget (OMB) memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*. The OMB policy memorandum defined four levels of authentication in terms of the assurance that an asserted identity is valid. Our guidance provides technical requirements and example authentication technologies that work by making individuals demonstrate possession and control of a secret for each of the four levels. This year, we began updating SP 800-63 to address additional authentication mechanisms that are now available in the marketplace.

In 2005, we studied other technologies that could be used to support electronic authentication, including knowledge based authentication (KBA) and biometrics. KBA refers to a class of techniques for testing the personal knowledge of an individual as a way to remotely verify the individual's claimed identity. KBA is a particularly useful tool to remotely authenticate individuals who conduct business electronically with Federal agencies or businesses infrequently; however, since this information is private but not actually secret, confidence in the identity of an individual may be hard to achieve. This year, we completed a draft guidance document on the use of KBA that we plan to publish as SP 800-63 Part B, *Knowledge Based Electronic Authentication Guideline*. Also, in 2005, we held a workshop to examine remote authentication protocols and biometrics. Based on the results of the workshop, in collaboration with industry, we helped to form the International Committee for Information Technology Standards (INCITS) M1 Ad Hoc group to continue studying the role of biometrics in the remote authentication of individuals across open networks. This group developed a technical report on its findings in 2006.

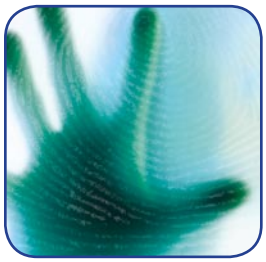
This year, we received sponsorship from the Department of Homeland Security (DHS) to begin a new multiyear project related to authentication effectiveness metrics. Through this project, we will investigate ways to develop metrics and a schema for assessing the effectiveness of various authentication mechanisms for local and remote environments, where each may deploy a variety of methods including password-based, knowledge-based, and biometric-based technologies. This year, we also began surveying the authentication industry for known and emerging methods of establishing, authenticating, and securely communicating user and device identification information to a service, device, or system. Based on the survey, we plan to develop a NIST Interagency Report on known and emerging authentication methods.

To maximize our results, we are collaborating with both Federal agencies and industry partners. Federal agencies include OMB, DHS, the General Services Administration, and the Federal Identity and Credentialing Committee. Industry partners include Financial Service Technology Consortium, Electronic Authentication Partnership, Fidelity Investments, Wells Fargo Bank, Electrosoft Services, VeriSign, and RSA Security.

Contacts: Mr. William Burr
(301) 975-2934
william.burr@nist.gov

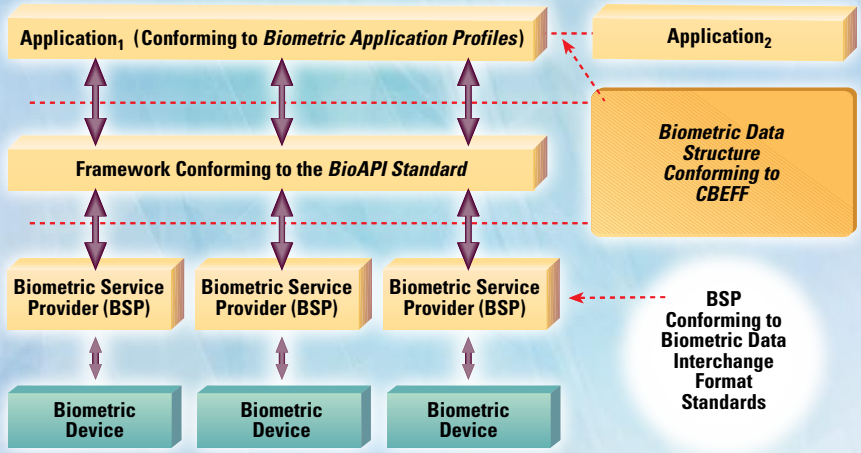
Ms. Donna Dodson
(301) 975-3669
donna.dodson@nist.gov

## Biometrics



Biometric technologies consist of automated methods of identifying a person or verifying the identity of a person based upon recognition of a physiological or behavioral characteristic. Examples of biological characteristics include hand, finger, facial, and iris. Behavioral characteristics are traits that are learned or acquired, such as dynamic signature verification and keystroke dynamics. For decades, biometric technologies were primarily used in law enforcement applications. Currently, they are increasingly being used in multiple public and private sector applications worldwide to authenticate a person's identity, secure national borders, and restrict access to secure sites including buildings and computer networks. Used alone, or together with other authentication technologies such as tokens and encryption, biometric technologies can provide higher degrees of security than other technologies employed alone and can also be used to overcome their weaknesses. Biometric technologies can be found in identification cards, loyalty programs, associated with the management of welfare programs, and in such diverse environments as amusement parks, banks, mobile devices, passport programs, driver licenses, and colleges and school lunch programs.

Government and other consumers need biometric-based, high-performance, interoperable (standards-based) information technology systems developed in a timely fashion. In the absence of timely open systems standards development, migration from proprietary systems to open-systems, standard-based solutions is usually more difficult and expensive. Deploying these new information technology systems for homeland security, for preventing ID theft, and for other government and commercial applications requires both national and international consensus standards for biometrics. These biometric standards support the mass market adoption of biometric technologies by helping customers to achieve higher levels of security and interoperability in personal authentication and identification applications using biometric-based, open-systems solutions. Therefore, supporting the national strategy on biometrics and the development of these standards is the cornerstone of our biometrics standards program. We are responding to government and market requirements for open-system standards by accelerating development of formal national and international biometric




standards and associated conformity assessments. This strategy requires comprehensively identifying and planning for the development of the required biometric standards and associated research and technology developments and testing.

In order to meet these immediate government and private sector needs for high performance and highly secure open systems, in the past years we have worked in close partnership with other U.S. Government agencies and U.S. industry to establish standards bodies for accelerating the development of formal national and international biometric standards of high relevance to the Nation. Our program experts also work in close collaboration with the NIST Information Access Division's biometric experts. This program is a major catalyst for biometric standardization and adoption of biometric standards.

Our strategy in this program includes—

- Leveraging existing consortia standards such as the Biometric Application Programming Interface (BioAPI)—developed by the BioAPI Consortium—and the Common Biometric Exchange Formats Framework (CBEFF)—initially developed under a Working Group sponsored by NIST and the Biometric Consortium;
- Managing formal national and international biometric standards developments;
- Providing expert technical leaders for critical standards projects;
- Participating in the National Science and Technology Council Subcommittee on Biometrics, as well as acting as an advisor to other Federal government agencies, including the Department of Homeland Security, the National Security Agency, and the Department of Defense Biometrics Task Force;
- Supporting required administrative infrastructures (for example, the ISO/IEC JTC 1 SC 37 Secretariat);
- Working through biometric standards "incubators" (such as the Biometric Consortium and the BioAPI Consortium);
- Promoting fast processing of consortia specifications into national/international standards; and
- Initiating development of technical implementations and software development for conformity assessment and interoperability tests to Application Profiles as required.

Our biometric standards program is supporting national and international biometric standards and conformity assessment through the development of conformance testing suite (CTS) implementations for key biometric interfaces such as the BioAPI standard and CBEFF data structures. Conformance testing captures the technical description of a specification and measures whether an implementation faithfully implements the specification. A conformance test suite implementation is test software that is used to ascertain conformance to a testing methodology described in a specification or standard. At the end of 2005, we completed development of an implementation of a CTS for the national version of the BioAPI specification, as well as the development of a documentary standard under INCITS M1. This standard project was sponsored by NIST/ITL/CSD, the Department of Defense Biometrics Management Office (now the Biometric Task Force), the National Biometric Security Project (NBSP), Saflink Corporation, and The Biometric Foundation (TBF). The initial CTS implementation was developed using concepts and principles specified in the draft conformance testing methodology standard. In coordination with NIST/ITL/CSD, the Biometric Task Force independently developed a similar implementation of the BioAPI CTS. NIST and the Biometric Task Force performed intensive testing of the initial versions of these CTSs and conducted a successful cross–validation of the test results using a number of vendor biometric subsystems for different modalities claiming conformance to the BioAPI standard. These CTS implementations were simultaneously released at the end of February 2006. The National Science & Technology Council (NSTC) Subcommittee on Biometrics listed the BioAPI CTS developments as one of the "Technology Successes" of 2006. These test tools were developed in support of users within government agencies that are already requiring, or are interested in requiring in the near future, biometric subsystems conforming to the BioAPI standard, the possible establishment of conformity assessment programs to

validate conformance to the BioAPI standard, and other emerging standards. They were also developed to support product developers interested in offering products conforming to voluntary consensus biometric standards by using the same test tools available to users.

During 2006, we also started development of CBEFF Conformance Test Suite implementations. We initially developed a CTS implementation conforming to data elements defined in the international version of CBEFF. Testing of this implementation is underway. We have also developed a technical formulation of a CBEFF CTS architecture that will support CBEFF conformance testing of each of the components of a CBEFF structure, including (1) CBEFF headers (SBH), which contain information of the biometric modality and format on the biometric data included in the CBEFF Biometric Data Block (BDB), the creator of the biometric data, the biometric product identifier, and the security and integrity options adopted for the data structure; (2) BDBs that contain the biometric data formatted according to one of the biometric data interchange format standards; and (3) signature/security blocks which contain integrity/encryption information. Specific CBEFF CTS modules are under development and will be released after extensive testing. Based on the experience we gained during the CTS development, our experts have proposed technical changes to CBEFF and related standards to improve the specification of these structures and enhance their functionality.

We have continued to participate in related consortia efforts, including the U.S. Biometrics Consortium (BC) and the BioAPI Consortium. The BC, which is considered to be a biometrics incubator, serves as a U.S. Government focal point for biometrics. It currently consists of hundreds of members representing over 60 government agencies, industry, and academia. NIST cochairs the BC with NSA. The BC sponsors an annual conference, technical workshops, and biometrics technical developments. The BC 2006 conference was held at the Baltimore Convention Center in September. The two-and-a-half day conference, recognized by attendees as one of the largest conferences dedicated to biometrics worldwide, offered an intensive technical program that included a number of government program sessions (i.e., the Executive Office of the President of the United States, the NSTC Subcommittee on Biometrics, the Department of Defense (DoD), NIST, the Department of Homeland Security (DHS), and the Department of Justice), as well as sessions on biometric solutions and applications, biometric standards, biometrics and e-authentication, privacy, and advances in biometric technologies. The conference was sponsored by NIST/ITL, NSA, DoD's Biometric Task Force, DHS, the National Institute of Justice, the General Services Administration's Office of Technology Strategy, the Department of Transportation's Maritime Administration, and the Volpe Center. The conference had over 1,000 participants and over 100 speakers from government, industry, and academia.

NIST is also a member of the BioAPI Consortium and its Steering Committee. This consortium developed the BioAPI specification, which was approved as INCITS 358-2002. The BioAPI specification was approved as an International standard in 2006. Related standards, to extend its functionality, are under development in JTC 1/SC 37.

During 2006, the leadership of our biometric standards program, Fernando Podio, was a recipient of INCITS's Gene Milligan Award for Effective Committee Management and the ANSI Meritorious Service Award "for his role in advancing the development, adoption, and awareness of biometric standards". Other awards received by NIST/ITL experts participating in biometric standards development included an INCITS Team Award for their contributions to the INCITS M1 program of work as technical editors of biometric standards completed during the previous year.

***National Standards Work***

In late 2001, our biometric standards program helped to establish Technical Committee M1-Biometrics under the InterNational Committee for Information Technology Standards (INCITS M1). The purpose of INCITS M1 is to ensure a high-priority focused and comprehensive approach in the United States for the rapid development and approval of formal national and international generic biometric standards. These standards are considered to be critical for U.S. needs, such as homeland defense, the prevention of identity theft, and for other government and commercial applications based on biometric personal authentication. CSD provides a person to serve as the Chair of INCITS M1 and the Chair of one of the five Task Groups under the main Committee.

While we have worked with them for the last three years, INCITS M1 approved a number of biometric data interchange standards for different biometric modalities—face recognition, finger image, finger minutiae, finger pattern, iris recognition, hand geometry, and signature/sign—and is approaching completion of the first generation of these biometric data interchange formats. During 2006, INCITS also developed three critical biometric performance testing and reporting standards that users and testing laboratories can now use to test the performance of biometric systems. These standards describe a common set of methodologies and procedures to be followed for conducting technical performance testing and evaluations, and they can be incorporated in an "end-to-end" system approach or from an individual technical component perspective. INCITS M1 also approved two biometric application profiles, and completed the development of three additional profiles. INCITS M1 has developed 15 American National Standards for biometrics in the last three years.

INCITS M1 is currently developing conformance testing methodology standards for a number of the biometric data interchange formats. In addition to the development of these conformance testing methodologies, we co-sponsored with other INCITS M1 members the development of conformance testing methodology standards for key biometric technical

interface standards—the BioAPI specification and the Common Biometric Exchange Frameworks Format (CBEFF). The development of the BioAPI conformance testing methodology standard was completed during 2006 and is in final public review before approval as an American National Standard. Development of the conformance testing methodology standard for CBEFF data implementations started in the last quarter of 2006. In addition, INCITS M1 is addressing the development of standards to support multi-biometrics and biometric fusion data, a biometric sample quality standard, and a standard to specify biometric performance and interoperability testing of data interchange format standards. NIST experts have been very active in all of these standards developments.

***International Work***

In 2002, we successfully supported the establishment of Subcommittee 37-Biometrics under the ISO/IEC Joint Technical Committee 1 (ISO/IEC JTC 1/SC 37-Biometrics). INCITS M1 is the national Technical Committee responsible for representing the U.S. in JTC1/SC 37. CSD provides a person for the Chair of SC37, and NIST provides a person for the Chair of one of the six Working Groups under the main Subcommittee.

A large number of the projects within JTC 1/SC 37's program of work were initiated by the United States through INCITS M1. JTC 1/SC 37 has also approached completion of the first generation of biometric standards, including biometric data interchange formats for a number of biometric modalities and key biometric technical interface standards. During 2006, this Subcommittee also made significant progress in the development of other biometric standards, including biometric performance testing, as well as reporting standards and biometric profiles for interoperability and data interchange. During the last 2 years, 10 standards developed by JTC1/SC 37 have been published by ISO as international standards. Eight other standards are scheduled for approval as international standards during the last quarter of 2006 or the first quarter of 2007.

NIST experts are also very active in the development of JTC 1/SC 37's standards portfolio. We are involved in ongoing efforts within JTC 1/SC37 in defining a taxonomy to enable the Subcommittee to determine the issues that need to be resolved to ensure that conformance, interoperability, performance, and quality for the biometric data interchange format standards can be adequately addressed. New trends, industry initiatives, technology innovations, and new customers' needs for biometric-based authentication systems present challenges to open systems standards development bodies such as INCITS M1 and JTC 1/SC 37. Our experts, in collaboration with other INCITS M1 members from government, industry, and academia, in addition to a number of experts from many national bodies represented in JTC 1/SC 37, are examining innovations in biometrics technologies and personal recognition systems. We have taken steps to meet these new challenges and customers' needs. Both organizations are concurrently considering new projects to complement and enhance functionality of the existing standards and to meet these new users' requirements.

---

http://www.nist.gov/biometrics
Contact: Mr. Fernando Podio
(301) 975-2947
fernando@nist.gov

## Security Aspects of Electronic Voting

In 2002, Congress passed the Help America Vote Act (HAVA) to encourage the upgrade of voting equipment across the United States. HAVA established the Election Assistance Commission (EAC) and the Technical Guidelines Development Committee (TGDC), chaired by the Director of NIST. HAVA calls on NIST to provide technical support to the EAC and TGDC in efforts related to human factors, security, and laboratory accreditation. To explore and research issues related to the security and transparency of voting systems, the TGDC established the Security and Transparency Subcommittee (STS). As part of NIST's efforts led by the Software Diagnostics and Conformance Testing Division, we support the activities of the EAC, TGDC, and STS related to voting equipment security.

In the past year, we supported the TGDC's development of the next generation of the Voluntary Voting System Guidelines (VVSG), focusing on developing a security architecture that addresses significant threats to voting systems and enhancing voting system auditability. New and updated requirements developed for the next generation of the VVSG cover access control, secure software distribution and installation, setup validation, system event logging, cryptography, voter verified paper records, physical security, and communications. To support the development of the next generation of the VVSG, two workshops on voting system threats were held, and we conducted research to enhance the auditability of voting systems.

Plans for 2007 include final development of the next generation of the VVSG with the TGDC, developing tests for the security requirements found in the next generation of the VVSG, hosting the TGDC plenary meetings, supporting STS activities, and engaging the voting system vendor, state election official, and academic communities to explore ways to increase voting system security and transparency.

---

http://vote.nist.gov/
Contacts: Dr. Nelson Hastings
(301) 975-5237
nelson.hastings@nist.gov

Dr. Alicia Clay Jones
(301) 975-3641
alicia.clay@nist.gov

# Security Research and Emerging Technologies

**STRATEGIC GOAL** ▸ *Devise advanced security methods, tools, and guidelines through conducting near-term and midterm security research.*

## Overview

Our security research focus is to identify emerging technologies and conceive of new security solutions that will have a high impact on the critical information infrastructure. We perform research and development on behalf of government and industry from the earliest stages of technology development through proof-of-concept, reference and prototype implementations, and demonstrations. We work to transfer new technologies to industry, to produce new standards, and to develop tests, test methodologies, and assurance methods.

To keep pace with the rate of change in emerging technologies, we conduct a large amount of research in existing and emerging technology areas. Some of the many topics we research include smart card infrastructure and security, wireless and mobile device security, voice over Internet Protocol (IP) security issues, digital forensics tools and methods, access control and authorization management, Internet Protocol security, intrusion detection systems, quantum information system security and quantum cryptography, and vulnerability analysis. Our research helps to fulfill specific needs by the Federal government that would not be easily or reliably filled otherwise.

We collaborate extensively with government, academia and private sector entities. In the past year this included the National Security Agency, the Department of Defense, the Defense Advanced Research Projects Agency, the Department of Justice, the University of Maryland, George Mason University, Rutgers University, Purdue University, George Washington University, the University of Maryland-Baltimore County, Columbia University, Microsoft Corporation, Sun Microsystems, the Boeing Company, Intel Corporation, Lucent Technologies, Oracle Corporation, and MITRE.

## Identity Management

### Personal Identity Verification

Authentication of an individual's identity is a fundamental component of physical and logical access control processes. When individuals attempt to access security-sensitive buildings, computer systems, or data, an access control decision must be made. An accurate determination of identity is an important component in making sound access control decisions. A wide range of mechanisms are employed to accurately determine identity; as a result, the strength of the authentication that is achieved varies, depending upon the type of credential, the process used to issue the credential, and the authentication mechanism used to validate the credential.

On August 27, 2004, the President signed Homeland Security Presidential Directive 12 (HSPD-12), entitled "Policy for a Common Identification Standard for Federal Employees and Contractors." HSPD-12 requires the development and implementation of a government wide standard for secure and reliable forms of identification for Federal employees and contractors. As required by HSPD-12, the National Institute of Standards and Technology (NIST) issued FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*. Subsequently, NIST issued several special publications in support of FIPS 201.

To ensure interoperability and to enable agencies to meet the tight deadlines of HSPD-12, we provided substantial contribution towards implementing PIV this year. We continued to refine FIPS 201 and associated special publications based on the inputs received from actual implementations and lessons learned from the NIST reference implementation. According to vendors and government agencies, FIPS 201 and its associated special publications are

the most thoroughly tested and widely implemented standards in the history of smart card implementations. The success of the PIV program is based on the following contributions from NIST during the year:

Establishment of National PIV Program—NIST established the NIST Personal Identity Verification Program (NPIVP) to validate PIV system components required by FIPS 201. The program facilitates rigorous testing of PIV products through National Voluntary Laboratory Accreditation Program (NVLAP)-approved test laboratories. NIST and the test laboratories worked together to establish criteria for conformance to PIV products and to ensure tested products are interoperable. NIST developed and published conformance test suites through SP 800-85A (test PIV interfaces) and SP 800-85B (test PIV data model). We also developed test tools to automate the product testing and to enable consistent testing among the accredited test laboratories. Through an iterative test and validation process with the laboratories, NIST provided additional clarifications and details on the implementation of the PIV standard.

PIV Product Demonstrations—NIST sought voluntary participation by companies offering products and services supporting FIPS 201 for the PIV Demonstration. The PIV Demonstration took place from May 15 to June 14, 2006. Forty-four companies voluntarily participated through a Cooperative Research and Development Agreement (CRADA). Over 25 different Federal agencies and departments attended the PIV Demonstration. The PIV Demonstration provided us the opportunity to conduct proof of concept and interoperability demonstrations of products supporting FIPS 201 and accompanying special publications. The demonstration proved that commercial products are available to facilitate compliance with the HSPD-12 mandate for Federal agencies. The demonstration enabled the exchange of useful information between the participating companies and Federal agencies which aided agencies in implementing HSPD-12 solutions.

PIV Reference Implementation—To aid and guide proper PIV implementation, we also provided a reference implementation of the PIV standards. Specifically, NIST developed a PIV Card Simulator that behaves and responds exactly like a PIV Card. We also developed PIV Middleware that implements the Application Programming Interface (API) as specified in SP 800 73-1. Both the source code and executables were made available on the PIV website as a reference. Moreover, in response to the request for sample PIV data, NIST developed a software tool that generates PIV data consistent with FIPS 201. The data generator and sample data were made available on the PIV Web site. The software generated mandatory and optional PIV data elements.

Refinement of Standards —During the last year, we continued to enhance and refine existing standards and guidelines so that the implementing Agencies were able to interoperate and benefit from lessons learned. We revised FIPS 201, SP 800-73, SP 800-76, and SP 800-78 to incorporate changes in U.S. Office of Management and Budget (OMB) policies and to reduce the possibility of different interpretations. We identified gaps in PIV standards and immediately moved to develop missing specifications. Specifically, we developed standards for PIV Card Reader interoperability (SP 800-96), and updated unique agency code (SP 800-87) assignments.

Future plans include maintenance support activities such as developing implementation guidelines, creating more reference implementations, and refining standards. Our efforts will be focused on PIV-enabling applications so that the PIV Card can be used in access control systems to authenticate claimed identities. The primary applications we will focus on include physical access systems, e-mail signing, e-mail encryption, Web authentication, and smart card logon. We plan to publish our findings as NIST guidelines and recommendations. We also plan to provide recommendations to Federal agencies on adding other applications on a PIV Card or adding a PIV application on their existing smart cards.

---

http://csrc.nist.gov/piv-program/
Contact: Mr. William MacGregor
(301) 975-8721
william.macgregor@nist.gov

### Identity Credential Smart Card Interoperability

With the emergence of Homeland Security Presidential Directive 12 (HSPD-12), which mandates a government wide standard for secure and reliable forms of identification for Federal government employees and contractors, the use of smart cards will increase, both in private and public sectors, as the scope of the transactions that are subject to smart card usage likewise increases. This increased use necessitates more preparedness by the issuers and acceptors of smart cards to reduce fraud, abuse, and other inappropriate smart card security-related activities. Increased security around smart cards will improve the consumer perception of the technology and ultimately increase usage.

Existing U.S. and international smart card standards lack interoperability and security standards. Large-scale use of smart cards within the United States has lagged despite the potential benefits. This work provides technical support in the development of formal standards for smart card interoperability specifications.

According to various studies, identity theft continues to be a major and growing problem. The use of secure and strongly authenticated identity credentials is necessary for countering this growing problem. Smart cards provide the necessary elements of such a solution. They can provide cryptographic mechanisms, store biometrics and keys, and, using certain techniques, address privacy considerations.

During the year, we continued the development of ISO/IEC 24727 *Identification Cards – Integrated Circuit Cards Programming Interfaces*, the multipart standard resolving current voids and interoperability challenges found in existing standards.

This suite of standards established the architecture required to develop secure and interoperable frameworks for smart card technology and identity credentials. This enables interoperable and interchangeable smart card systems and eliminates consumer reliance on proprietary-based solutions that have been historically inherent in this industry. While existing standards provide the consumer with a solution, the existing options in these standards make it very difficult, almost impossible, to ensure seamless interoperability. Furthering the development of formally recognized international standards, through collaborative efforts with public and private sectors, will support organizations by providing an interoperable and secure method for interagency use of smart card technology.

ISO/IEC 24727 provides a set of programming interfaces for interactions between integrated circuit cards (ICCs) and applications to include multi-sector use of generic services for identification, authentication, and signature. ISO/IEC 24727 is specifically relevant to identity management applications desiring interoperability among diverse application domains. This standard defines interfaces such that independent implementations are interoperable. Card application and associated services are discoverable without the need for proprietary information.

The parts of ISO/IEC 24727 are—

- ISO/IEC 24727-1 specifies the framework and supporting mechanisms and interfaces. It provides essential background information for the subsequent parts.
- ISO/IEC 24727-2 details the functionality and related information structures available to the implementation of the application interface defined in ISO/IEC 24727-3. It provides a generic card interface.
- ISO/IEC 24727-3 details service access mechanisms for use by any application to include authentication protocols that are in use by identity systems (i.e., PIN, biometric, symmetric key). It provides a common application programming interface (API) and interoperable authentication protocols.
- ISO/IEC 24727-4 details the security model and interface for secure messaging within the framework. It provides API administration between Part 2 and Part 3.
- ISO/IEC 24727-5 will contain testing requirements for ensuring compliance.

At the time of this annual report, ISO/IEC 24727-1 had passed all necessary international ballot processes and will be imminently available to the public from ISO. With the exception of ISO/IEC 24727-5, all other parts are in various international ballot statuses.

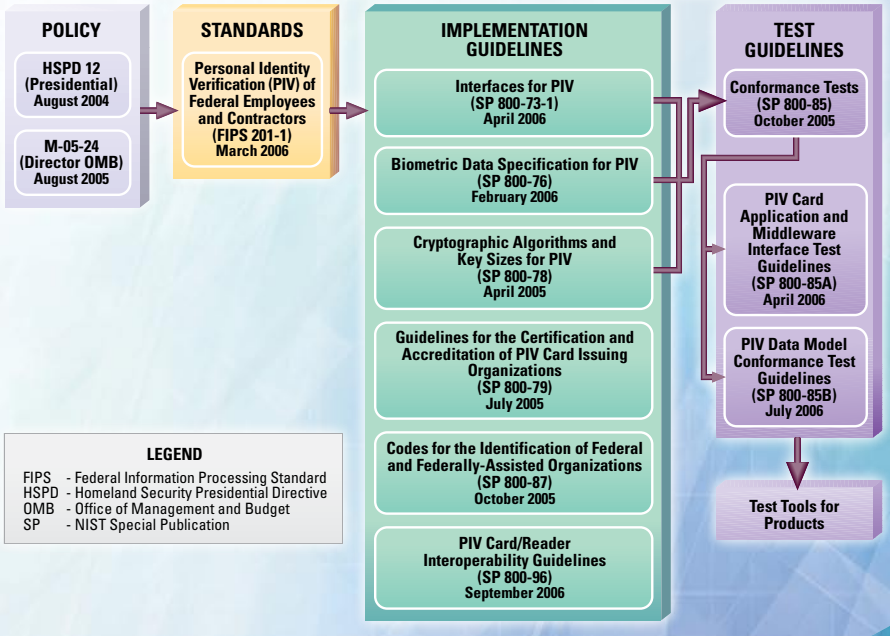
Although not yet finalized, this standard has been publicly adopted by the European community for the European Citizens Card and by Australia for their citizen social services card. We continue to work with the U.S. national standards committee to ensure compatibility with Federal credentials and to address the needs of nonfederal communities.

---

Contact: Ms. Teresa Schwarzhoff
(301) 975-5727
teresa.schwarzhoff@nist.gov

### NIST Personal Identity Verification Program (NPIVP)

The mission of the NIST Personal Identity Verification Program (NPIVP) is to validate Personal Identity Verification (PIV) components required by FIPS 201 for conformance to specifications in the FIPS 201 companion document SP 800 73-1, *Interfaces for Personal Identity Verification*. The two PIV components that come under the scope of NPIVP are PIV Smart Card Application and PIV Middleware. All of the tests under NPIVP are conducted



by third-party test facilities, which are accredited as Cryptographic Module Test (CMT) laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP) and have extended their scope of testing to include PIV Smart Card application and PIV Middleware test methods.

To facilitate development of PIV Smart Card Application and PIV Middleware for conformance to interface specifications in SP 800 73-1, NPIVP published SP 800-85A, *PIV Card Application and Middleware Interface Test Guidelines.* In addition to the tests, this document also provided an interpretation of SP 800 73-1 specifications through publication of C-language bindings for PIV Middleware interface commands as well as detailed mapping of PIV Card Command Interface return codes to PIV Middleware Interface return codes. We also developed an integrated toolkit called "PIV Interface Test Runner" for conducting tests on both PIV Card Application and PIV Middleware products, and provided the toolkit to NPIVP-accredited test laboratories.

In view of the tight HSPD-12 deadlines, the 10 CMT laboratories were initially given an interim designation by NPIVP to conduct PIV Card application and PIV Middleware tests. In 2006, the NPIVP team, working with NVLAP, undertook all the processes required to convert the interim designation to a permanent NVLAP accreditation. The processes included (1) designing and administering a proficiency test and evaluating the observations and insights provided by the laboratories that ran the tests; (2) submitting a written questionnaire and evaluating the answers provided; (3) updating the relevant NVLAP handbook to include tests relating to the two PIV components; and (4) providing a programmatic guidance handbook for NPIVP laboratories. PIV Card application tests conducted on eight PIV Smart Card Products submitted by some of the world's leading smart card vendors were validated, and Validation Certificates for conformance to SP 800 73-1 specifications were issued. On the PIV Middleware side, seven different products were validated and issued NPIVP certificates.

To facilitate development of card personalization products that can generate data for conformance to data model specifications in SP 800 73-1—as well as those in SP 800 76-1, *Biometric Data Specification for Personal Identity Verification*, and PIV PKI Certificate profiles—NPIVP published SP 800-85B, *PIV Data Model Test Guidelines*. NPIVP also developed the associated toolkit, "PIV Data Model Test Runner," and provided the toolkit to the U.S. General Services Administration (GSA) to support their FIPS 201 Evaluation Program that included evaluation of smart card personalization products.

---

http://www.nist.gov/npivp
Contact: Dr. Ramaswamy Chandramouli
(301) 975-5013
chandramouli@nist.gov

## Research in Emerging Technologies

### Policy Machine

As a major component of any host or network operating system, access control mechanisms come in a wide variety of forms, each with their individual attributes, functions, methods for configuring policy, and a tight coupling to a class of policies. To afford generalized protection, we have initiated a project (in part under sponsorship of the Department of Homeland Security) in pursuit of a standardized access control mechanism, referred to as the Policy Machine (PM), that requires changes only in its configuration in the enforcement of arbitrary and organization-specific, attribute-based access control policies. Included among the PM's enforceable policies are combinations of policy instances (e.g., Role-Based Access Control and Multi-Level Security). In our effort to devise a generic access control mechanism, we are constructing the PM in terms of what we believe to be abstractions, properties, and functions that are fundamental to policy configuration and enforcement. In its protection of objects under one or more policy instances, the PM categorizes users and resources and their attributes into policy classes and transparently enforces these policies through a series of fixed PM functions that are invoked in response to user or subject (process) access requests.

The specification and implementation of core PM features have been under development during the past year. In the coming year, we plan to build upon these core features by specifying advanced features to include enforcement of safety invariants, static separation of duty, multi state policies (also referred to as history-based policies), and combinations of policies.

If successful, we believe that the PM can benefit organizations in a number of ways, including—

- Increased productivity through the ability to better share greater volumes of resources among a more diversified user community;
- Decreased insider crime through the ability to automatically enforce organization-specific and fine-grained access control policies;
- Increased administrator productivity through better interfaces in configuring and visualizing access control policies; and
- Increased cooperation among organizations through the potential for the coordination, exchange, and interoperability of access control data.

---

Contacts: Mr. David Ferraiolo
(301) 975-3046
david.ferraiolo@nist.gov

Mr. Vincent Hu
(301) 975-4975
vhu@nist.gov

### Grid Security

While grid computing has become closer to reality due to the maturity of the current computing technologies, it has greater challenges compared to non-grid systems with infrastructure security issues such as authorization, directory services, and firewalls. There is some research available on grid security-related topics; however, most of the research is targeted to one specific grid system, is incomplete by making assumptions, or is ambiguous regarding the critical elements in their works. Because of the complexities of architecture and applications of the grid, a practical and conceptual guidance for grid security is needed.

In the coming year, we will first define or classify what a general grid system is, and then we will identify security requirements that are specific to grid computing (such as complex trust domain integrations). In the future, we will develop a reference implementation using already-developed tools (such as Globus and PM) to demonstrate how to configure a grid system to satisfy the security requirements.

The success of this project will:

- Promote (or accelerate) the adoption of grid systems in government and industry;
- Increase security and safety of non-grid distributed systems by applying the trust domain concept of grid; and
- Assist system architects, security administrators, and security managers whose expertise is related to grid in managing their systems.

---

Contacts: Dr. Vincent Hu
(301) 975-4975
vhu@nist.gov

Ms. Karen Scarfone
(301)975-8136
karen.scarfone@nist.gov

Mr. David Ferraiolo
(301) 975-3046
david.ferraiolo@nist.gov

### Mobile Ad Hoc Network and Wireless Security

In 2006, our research team released an updated open source implementation of mLab, a Mobile Ad Hoc Network (MANET) test bed. This test bed allows researchers the opportunity to validate ad hoc networking theories and simulations in practice, to test simulation assumptions, and to discover practical problems facing ad hoc network users and developers alike. The mLab tool allows users to create arbitrary network topologies and traffic scenarios in order to perform real-time performance measurements of routing protocols. By changing the logical topology of the network, mLab users can conduct tests in an ad hoc network without having to physically move the nodes in the ad hoc network. The tool allows users to replay

different mobility scenarios, captures wireless traffic for further analysis, and helps perform specification-based intrusion detection. The research team has published and presented the results at six international conferences.

A number of Intrusion Detection System (IDS) techniques for MANETs have been proposed in the research literature. These techniques include trust building and cluster-based voting schemes, host-based watchdogs, and finite state machines for specifying correct routing behavior. Comparing and evaluating the effectiveness of these IDS techniques has been hindered by the limited number of large-scale MANET deployments, the lack of publicly available network traces of actual MANET traffic, and the difficulty in defining typical application and mobility scenarios. Network simulation tools have allowed researchers to study MANET IDSs without purchasing mobile nodes or conducting costly and time-consuming field trial tests. These simulations, however, have been conducted using widely varying assumptions on background network traffic, mobility, previous security associations, and the type of malicious network activity. In 2007, our research team will be using the mLab test bed to create publicly available MANET network traces. These network traces will allow a broader range of researchers to compare the effectiveness of different MANET IDS techniques on the same data set, and conduct cost-effective and time-saving offline experiments with new IDS techniques without requiring expensive hardware.

---

http://csrc.nist.gov/manet
Contact: Dr. Tom Karygiannis
(301) 975-4728
karygiannis@nist.gov

### Automated Combinatorial Testing for Software

NIST research suggests that software faults are triggered by only a few variables interacting (1 to 6). These results have important implications for testing. If all faults in a system can be triggered by a combination of n or fewer parameters (where n is the number of parameters), then testing all

n-way combinations of parameters can provide high confidence that nearly all faults have been discovered. For example, if we know from historical failure data that failures for a particular application never involved more than four parameters, then testing all 4-way or 5-way combinations of parameters gives strong confidence that flaws will be found in testing.

A project initiated in 2006 seeks to take advantage of this empirical observation by developing software test methods and tools that can test all n-way combinations of parameter values. The methods have been demonstrated in a proof-of-concept study that was presented at a NASA conference and are being further developed through application to real-world projects at NIST and elsewhere.

This work uses two relatively recent advances in software engineering—algorithms for efficiently generating covering arrays and automated generation of test oracles using model checking. Covering arrays are test data sets that cover all n-way combinations of parameter values. Pairwise (all pairs of values) testing has been popular for some time, but our research indicates that pairwise testing is not sufficient for high assurance software. Model checking technology enables the construction of the results expected from a test case by exploring all states of a mathematical model of the system being tested. Tools developed in this project will have applications in high assurance software, safety and security, and combinatorial testing.

Our focus is on empirical results and real-world problems. Accomplishments to date include (1) the development of two new algorithms, including one that can be implemented on a cluster (parallel processing) system, to generate covering arrays that can produce optimal arrays for many applications and near-optimal arrays for large applications (more than one hundred variables); and (2) a proof-of-concept demonstration of integrating combinatorial testing with automated generation of test oracles using model checking. Plans for FY 2007 include expanding the work to Web application testing, demonstrating the methods and tools on large real-world problems, and planning the release of software for public use. We are working with researchers from several major universities, other NIST divisions and labs, and private industry.

---

http://csrc.nist.gov/acts

Contacts: Mr. Rick Kuhn
(301) 975-3337
kuhn@nist.gov

Dr. Raghu Kacker
Mathematical and Computational Sciences Division
(301) 975-2109
raghu.kacker@nist.gov

## Digital Handheld Device Forensics

The digital forensic community faces a constant challenge to stay on top of the latest technologies that may be used to recover evidence. One such area concerns handheld device forensics. Personal digital assistants (PDAs) and cell phones, including converged PDA/cell phone devices, are commonplace in today's society. They are used by individuals for both personal and professional purposes. Handheld device technologies are evolving rapidly with new products and features being introduced regularly. Rather than just placing calls, cellular devices can allow users to perform additional tasks such as Short Message Service (SMS) messaging, Multi-Media Messaging Service (MMS) messaging, Instant Messaging (IM), electronic mail exchange, Web browsing, Personal Information Management (PIM) maintenance (e.g., address book, task list, and calendar schedule), and even the reading, editing, and production of digital documents. When used over time, these devices tend to accumulate a significant amount of information that may pertain to an incident or crime.

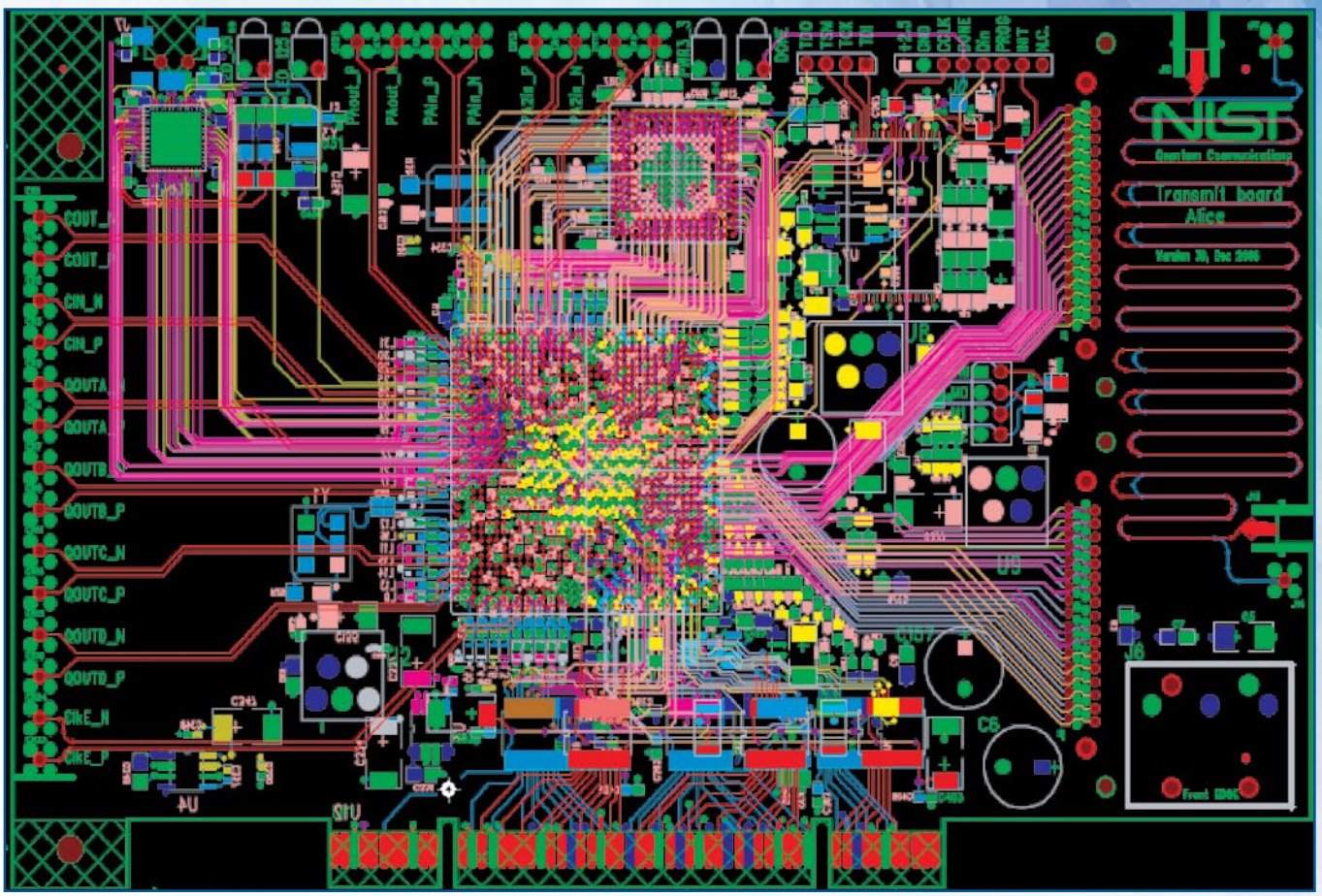
When a PDA or cellular phone is encountered during an investigation, many questions arise: What should be done about maintaining power? How should the overall state of the device and prevention of incoming/outgoing signals be handled? How should valuable or potentially relevant data contained on the device be examined? The key to answering these questions is an understanding of both the hardware and software characteristics of these devices and the intrinsic ability of available forensic tools.

We have worked this past year to produce NIST Interagency Report (NISTIR) 7250, *Cell Phone Forensic Tools: An Overview and Analysis*, which provides an overview of current forensic software tools designed for the acquisition, examination, and reporting of data residing on cellular handheld devices, and reviews their capabilities and limitations. Additionally, a companion report, SP 800-101, *Guidelines on Cell Phone Forensics*, was released for public comment, to provide recommendations on procedures and highlight key principles associated with the handling and examination of electronic evidence contained on cellular devices.

The intended audience of these publications is varied and broad, ranging from response team members handling a computer security incident to organizational security officials investigating an employee-related situation to forensic examiners involved in criminal investigations.

---

Contact: Mr. Wayne Jansen
(301) 975-5148
wayne.jansen@nist.gov




*The NIST custom printed circuit board for quantum key distribution*

### Quantum Cryptography and Information Systems

Quantum mechanics, the strange behavior of matter on the atomic scale, provides entirely new and uniquely powerful tools for computing and communications. This field could revolutionize many aspects of computing and secure communications, and could have enormous impacts on homeland security. Whereas current computers calculate linearly, quantum computers will be able to calculate enormous numbers of variables simultaneously. This capability is particularly useful in modeling complex situations with many variables (weather modeling, for example) and in solving extremely difficult equations (processing tasks that would literally take billions of years on conventional computers).

Exploiting quantum properties would be particularly valuable in cryptography, making codes that would be unbreakable by the best supercomputers of tomorrow or breaking codes in nanoseconds that could not be cracked in millions of years by the most powerful binary computers. Quantum information also can be used for remarkably secure communications. In this area, we are partnering closely with the Defense Advanced Research Projects Agency (DARPA).

Quantum cryptography is a set of methods for implementing cryptographic functions using the properties of quantum mechanics. Most research in quantum cryptography is directed toward generating a shared key between two parties, a process known as quantum key distribution (QKD). The shared keys may be used directly as keys for a conventional symmetric cryptographic algorithm, or as a one-time pad. A variety of protocols have been developed for quantum key distribution. However, they share two key features: (1) the idealized version of the protocol prevents an eavesdropper from obtaining enough information to intercept messages encoded by using the shared key as a one-time pad, and (2) the communicating parties can detect the presence of an eavesdropper because measuring the particles used in key distribution will introduce a significant error rate.

The most common type of quantum key distribution uses a scheme developed by Bennett and Brassard (known as BB84), in which polarized photons are sent between the communicating parties and used to develop the shared key. The BB84 protocol has been studied extensively and has been shown to be secure if implementations preserve assumptions regarding physical properties of the system. Many varieties of the BB84 scheme have been developed, and other forms of quantum key distribution have been proposed as well.

Quantum cryptography offers the potential for stronger security, but as with any information technology, QKD must be designed and implemented properly to provide the benefits promised. While often described in the popular literature as "unbreakable," quantum key distribution systems may be subject to a number of attacks depending on the implementation and the protocol. Vulnerabilities may be introduced in the physical systems, quantum protocols and the application software and operating systems used to process keys. Existing QKD systems are not able to guarantee the production and receipt of a single photon per time slice, as required by most quantum protocols. Multiple photons emitted in a single time slice may allow an attacker to obtain information on the shared key. Quantum protocols may also have weaknesses. Although BB84 is regarded as secure, researchers frequently introduce new protocols that differ radically from the BB84 scheme, and a number of these protocols have been shown to be vulnerable to attack. A third area of concern for QKD systems is the conventional computing platforms on which they must be based. Quantum cryptographic equipment must be integrated with the organization's network, potentially leaving the QKD system and its software open to conventional network attacks. Methods of evaluating and certifying QKD systems have not yet been incorporated into existing security evaluation methodologies.

Quantum cryptography is a relatively new field. Two firms, MagiQ Technologies (USA) and ID Quantique (Switzerland), have been developing and offering quantum cryptographic products since 1999. Others, including IBM, NEC, Fujitsu, Siemens, and Sony, have active research efforts that may result in products. Existing products are capable of key distribution through fiber optic cable for distances of only several tens of kilometers, but progress has been rapid. In addition to key distribution, quantum cryptographic products include quantum random number generators, single photon detectors, and photon sources.

The main objective of the NIST Quantum Information Program is to develop an extensible quantum information test bed and the scalable component technology essential to the practical realization of a quantum communication network. The test bed will demonstrate quantum communication and quantum cryptographic key distribution with a high data rate. This test bed will provide a measurement and standards infrastructure that will be open to the DARPA QuIST (Quantum Information Science and Technology) community and will enable wide-ranging experiments on both the physical- and network-layer aspects of a quantum communication system. The infrastructure will be used to provide calibration, testing, and development facilities for the QuIST community.

Within the Quantum Information Program, we are also developing and evaluating quantum cryptographic protocols and investigating means of integrating quantum and conventional network technology. Controlling access to a large network of resources is one of the most common security problems. Any pair of parties in a network should be able to communicate, but must be authorized to do so, while minimizing the number of cryptographic keys that must be distributed and maintained. This project will develop an authentication solution based on a combination of quantum cryptography and a conventional secret key system. Two significant advantages of this approach over conventional authentication protocols are (1) timestamps and exact clock synchronization between parties are not needed, and (2) even the trusted server cannot know the contents of the authentication ticket.

In the past year, NIST Information Technology Laboratory (ITL) researchers investigated methods to implement quantum computing with very noisy devices. This work may speed the development of practical quantum computing because it means that quantum computers will be able to tolerate imperfections and higher error rates in components. ITL staff also worked with NIST physicists to construct a QKD free-space test bed that represents a major increase in the attainable rate of quantum key generation, over 100 times faster than previously reported results. This year, using much of the infrastructure developed for the free-space test bed, these physicists implemented a fiber-based QKD test bed, which doubled their previous quantum key generation rate. Part of this work focused on methods that would allow QKD systems to operate using a standard telecommunication infrastructure. A quantum authentication and key distribution protocol that is integrated with conventional Internet security protocols was completed and published in 2005. In the coming year, ITL will continue work on fault-tolerant quantum computing, work with the NIST Physics Laboratory on a test bed for quantum components and quantum networks that can be integrated with the Internet, and investigate applications of quantum cryptography to the problem of secure routing. A method of producing entangled photon pairs suitable for use in quantum cryptographic protocols was developed in 2006, and work towards implementing the method has begun.

---

http://math.nist.gov/quantum/

Contacts: Mr. Rick Kuhn
(301) 975-3337
kuhn@nist.gov

Dr. Alan Mink (ANTD)
(301) 975-5681
alan.mink@nist.gov

## Automated Vulnerability Management and Measurement

### National Vulnerability Database

NIST maintains the National Vulnerability Database (NVD). NVD is sponsored by the Department of Homeland Security's National Cyber Security Division and is designed to complement their current suite of vulnerability management products. This publicly available resource is being accessed at a rate of 30 million times a year by the information technology security community.

NVD is a comprehensive cyber security vulnerability database that is updated daily with the latest vulnerabilities. Using a single search engine, one can find all publicly available U.S. Government vulnerability resources and references to industry resources. It contains over 20,000 analyzed vulnerabilities advisories with 20 new vulnerabilities added daily. In fiscal year 2006, over 6500 new vulnerabilities were add to the database.

NVD is a general-purpose tool that can be used for a variety of purposes. Recommended uses include—

- Viewing all publicly available U.S. Government vulnerability mitigation information;
- Learning how to mitigate vulnerabilities referenced within security products (e.g., intrusion detection systems);
- Keeping abreast of the latest vulnerabilities;
- Researching the vulnerability history of a product;
- Researching what vulnerabilities might exist on a computer that may not be detected by vulnerability scanners (e.g., vulnerabilities in obscure products); and
- Viewing statistics on vulnerability discovery.

NVD is built completely upon the Common Vulnerabilities and Exposures (CVE) naming standard and provides CVE with a fine-grained search engine and database. CVE is used by over 300 security products and services to uniquely identify vulnerabilities.

---

http://nvd.nist.gov
Contact: Mr. Peter Mell
(301) 975-5572
mell@nist.gov

### Common Vulnerability Scoring System

The Common Vulnerability Scoring System (CVSS) is an industry standard that was developed by a White House committee and is now being promoted by the international Forum of Incident Response and Security Teams (FIRST). CVSS enables the security community to calculate the impact of low level vulnerabilities within information technology systems. NIST security staff and mathematicians are providing the technical leadership and support for the development of the next version of CVSS. This scoring system will enable consistent and accurate measurement of low level security flaws that can be used by attackers to penetrate systems. We plan to recommend usage of CVSS by Federal agencies in order to bring more quantitative measurement of security deficiencies within the FISMA implementation process.

---

http://nvd.nist.gov/cvss/cvss.cfm
Contacts: Mr. Peter Mell
(301) 975-5572
mell@nist.gov

Ms. Karen Scarfone
(301) 975-8136
karen.scarfone@nist.gov

### Information Security Automation Program (ISAP) & Security Content Automation Protocol (SCAP)

The ISAP is a Department of Homeland Security (DHS)-sponsored initiative that includes interagency and interdepartmental participation from NIST, the National Security Agency (NSA), the Defense Information Systems Agency (DISA), the Department of Defense (DoD), the Army, and the Air Force. This program focuses on a standard, automated approach for the implementation of information system security controls, which includes the following objectives—

- Develop requirements for automated sharing of information security data;
- Customize and manage configuration baselines for various IT products;
- Assess information systems and report compliance status;
- Use standard metrics to weigh and aggregate potential vulnerability impact; and
- Remediate identified vulnerabilities.

Recognizing that NIST has the responsibility to produce security configuration guidance for the U.S. Government, and that NSA and DISA provide the same service to DoD, the ISAP consolidates data sources from these Agencies and provides the data in a standardized XML format. Consumers of this security-related data include both commercial-off-the-shelf (COTS) and government-off-the-shelf (GOTS) software products and initiatives for the purposes of automating the identification and remediation of vulnerabilities, measuring potential impact, and conducting compliance reporting in the various computing infrastructures. The freely available information contained in ISAP files includes, but is not limited to—

- Checking for vulnerabilities (security-related software flaws and misconfigurations) on an information technology asset;
- Mapping to higher-level policies, such as FISMA via NIST SP 800-53, DoD 8500 Information Assurance (IA) controls, etc.; and

- Providing a standard impact metric for vulnerabilities and a capability to aggregate impact scores to the Agency reporting level.

***The FISMA Connection***

As the NIST FISMA Implementation Project moves into Phase II, we continue to look for ways to help our customers employ the most cost-effective information security solutions for their enterprises. One of the key challenges in effectively employing security controls in information systems is to ensure that security configuration settings are properly established and enforced. It is also important to establish traceability from the high-level security requirements in the FISMA legislation down to the specific mechanisms that provide the security capability in the hardware and software components that compose the information system. To establish this important linkage from legislation and policy to the mandatory security requirements and controls described in FIPS 200 and SP 800-53, and ultimately to the mechanisms at the systems-implementation level, we established the SCAP as part of the ISAP governing program.

***SCAP Technical Composition***

Through the interagency/interdepartmental ISAP effort the Federal government, in cooperation with academia and private industry, uses and encourages widespread support for the SCAP, a suite of open standards—developed primarily by NSA, MITRE Corporation, and NIST—that provide technical specifications for expressing and exchanging security-related data. These interoperable standards identify, enumerate, assign, and facilitate the measurement and sharing of information security-relevant data. The SCAP is comprised of the following standards—

***Enumeration***

- Common Platform Enumeration – CPE (http://cpe.mitre.org)
- Common Vulnerability Enumeration – CVE (NIST SP 800-51)
- Common Configuration Enumeration – CCE (http://cce.mitre.org)

***Metrics/Scoring***

- Common Vulnerability Scoring System – CVSS (http://nvd.nist.gov/cvss.cfm)

***Languages for Expression***

- eXtensible Checklist Configuration Description Format – XCCDF (NIST Interagency Report [NISTIR] 7275)
- Open Vulnerability and Assessment Language – OVAL (NISTIR 7275)

The suite of standards within SCAP is extensible and will likely be expanded over time to include additional standards, such as Common Remediation Enumeration (CRE) and/or Open Vulnerability Remediation Language (OVRL).

The primary output from the SCAP is a security checklist in standard XML format that customers can use via their COTS products to help build, operate, measure, and maintain more secure information systems according to official government security guidelines. A security checklist is a document that contains instructions for securely configuring an information technology (IT) product for an operational environment or verifying that an IT product has already been securely configured. Checklists can take many forms, including files that can automatically set or verify security configurations. Having such automated methods has become increasingly important for several reasons, including the complexity of achieving compliance with various laws, Executive Orders, directives, policies, regulations, standards, and guidance; the increasing number of vulnerabilities in information systems; and the growing sophistication of threats against those vulnerabilities. Automation is also needed to ensure that the security controls and configuration settings are applied consistently within an information system and that the controls and settings can be effectively verified.

In response to these needs and working closely with government, industry, and academia, SCAP seeks to encourage the development of automated checklists, particularly those that are compliant or compatible with XCCDF and/or OVAL. These are widely used for automated checklists—XCCDF primarily for mapping policies and other sets of requirements to high-level technical checks, and OVAL primarily for mapping high-level technical checks to the low-level details of executing those checks on the operating systems or applications being assessed.

The SCAP Web site provides, or is scheduled to provide, automated security configuration and patching information for checklists obtained through the NIST Checklist Program (checklists.nist.gov), including Windows Vista, Windows 2003 Server, Windows XP, Windows 2000, RedHat Linux, desktop applications (e.g., Microsoft Office, Netscape Navigator, Internet Explorer), Oracle and Microsoft SQL server, Sun Solaris, and Web servers (e.g., IIS, Apache).

---

http://nvd.nist.gov/scap.cfm

Contacts: Mr. Stephen Quinn
(301) 975-6967
stephen.quinn@nist.gov

Mr. Peter Mell
(301) 975-5572
pmell@nist.gov


**Security Configuration Checklists for Commercial IT Products**

There are many threats to users' computers, ranging from remotely launched network service exploits to malicious code spread through e-mails, malicious Web sites, and file downloads. Vulnerabilities in IT products are discovered on a daily basis and many 'ready-to-use' exploits are widely available on the Internet. Because IT products are often intended for a variety of audiences, restrictive security controls are usually not enabled by default by the product vendor, so many IT products are immediately vulnerable "out-of-the-box." It is a complicated, arduous, and time-consuming task for even experienced system administrators to identify a reasonable set of security settings for many IT products. While the solutions to IT security are complex, one basic and effective tool is the security configuration checklist.

The goals of the NIST Checklist Program are—

- To facilitate the development and sharing of security configuration checklists by providing a framework for checklist providers/developers to submit checklists to NIST;
- To assist checklist developers in generating content that conforms to common baseline levels of security;
- To assist checklist providers/developers and users by providing guidelines for enhancing the documentation and usability of security guidance;
- To provide a managed process for the review, update, and maintenance of security checklists;
- To provide checklists in standard XML format as per the Security Content Automation Protocol (SCAP) for use by commercial-off-the-shelf (COTS) security tools; and
- To provide an easy-to-use repository of checklists.

This program also assists product vendors by providing their vendor-developed checklists to users via a government Web site to secure "out-of-the-box" installations. It is advisable for product users to consult the checklist repository for updates to pre-installed or vendor-supplied checklists.

A security configuration checklist (sometimes called a lockdown, hardening guide, or benchmark) is a series of instructions for configuring a product to a particular security level (or baseline). Typically, checklists are created by IT vendors for their own products; however, checklists are also created by other organizations such as consortia, academia, and government agencies. The use of well-written, standardized checklists can markedly reduce the vulnerability exposure of IT products. Checklists have proven particularly helpful to small organizations and individuals that have limited resources for securing their systems.

A checklist might include any of the following:

- Configuration files that automatically set various security settings (standard XML format such as that utilized in the SCAP, executables, security templates that modify settings, and scripts);
- Documentation (for example, a text file) that instructs the checklist user how to interactively configure software to recommended security settings;
- Documentation explaining the recommended methods to securely install and configure a device; and
- Policy documents that set forth guidelines for such things as auditing, authentication security (for example, passwords), and perimeter security.

Checklists can also include administrative practices (such as management and operational controls) for an IT product that go hand-in-hand with improvements to the product's security.

Many organizations and product vendors have created security checklists, and the checklists vary in terms of format, applicability, quality, and usability. Many checklists have become "outdated" in the course of the product life cycle as software updates and upgrades were released. The NIST Checklist Program established a centralized repository for checklist content and subsequent updates so that consumers could use this "one-stop-shop" to locate the most current security guidance documents. By defining applicable scenarios and distribution formats, the NIST Checklist program, in conjunction with the ISAP effort, assists organizations in securing their IT systems and determining ongoing compliance to legislation such as FISMA through the use of COTS products.

Although the use of security configuration checklists can greatly improve overall levels of security in organizations, checklists cannot ensure a system or a product is 100 percent secure. However, use of checklists that emphasize hardening of systems by reducing the attack surface, offer countermeasures against software flaws or "bugs" and suggest appropriate/current patches will result in greater levels of product security and protection from future threats.

We released the final version of SP 800-70, *Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers*, in May 2005; however, with the advent of the joint-agency ISAP, we are in the process of revising the SP 800-70 publication to encourage the production, submission, and maintenance of IT system-related checklists in standard XML format. The NIST Beta Checklists repository, released in May 2005, contains checklists and descriptions for over 110 checklists addressing approximately 130 platforms, including but not limited to, database systems, Dynamic Host Configuration Protocol (DHCP) servers, directory services, Domain Name System (DNS) servers, firewalls, multi functional peripherals, network routers, network switches, operating systems, vulnerability management software, Web browsers, Web servers, and popular desktop and office automation products.

The NIST Checklist program was officially integrated into the FISMA Implementation Project by a charter document entitled SP 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*. Although the principal goal of SP 800-68 was to recommend and explain tested, secure settings for Windows XP workstations, with the objective of simplifying the administrative burden of improving the security of Windows XP systems, the document also included mappings to the FISMA technical controls. This mapping gave rise to the notion that we should continue to provide mappings from the lower-level security recommendations to higher-level documents (NIST SP 800-53, the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), NSA Guides, etc.) so as to realize the fact that security and compliance are interrelated at the lowest level. By partnering with the NSA and DISA, the joint-agency effort quickly adopted a standard format for expressing both policy and system-level checklist content in standard XML format; specifically, XCCDF and OVAL. As a result, checklists can now be expressed in a more usable and consistent format which is being adopted by COTS security tool providers for securing IT systems, monitoring compliance, and facilitating measurement. The notion of partnering with vendors and private industry to produce original checklists and translate English-prose checklists into the standard format, associating compliance mappings among the various Federal agency security framework and guidance documents, is realized via the NIST Checklist's companion program, the Information Security Automation Program (ISAP). This comes at a time when organizations are concerned about ensuring that operationally deployed products (at least hundreds if not thousands) are updated with security patches and secure configuration. The need to automate this laborious, costly, and resource-consuming process has never been greater. By offering this service, the NIST Checklist program, in conjunction with ISAP, can help reduce the level of effort required to perform vulnerability identification, remediation, and compliance reporting and allow organizations to refocus valuable personnel resources on other problems.

This program is in cooperation with checklist development activities at Federal agencies, including DISA and NSA, private industry, Federally Funded Research and Development Centers (FFRDCs), academia, and not-for-profit organizations. Federal agencies continue to solicit participation agreements with product vendors and other checklist-producing organizations. We gratefully recognize the Department of Homeland Security as the original sponsor of this program.

---

http://checklists.nist.gov/
Contact: Mr. Stephen Quinn
(301) 975-6967
stephen.quinn@nist.gov

## Infrastructure Services, Protocols, and Applications

### Securing the Domain Name System (DNS)

The Domain Name System (DNS) is the method by which Internet addresses in mnemonic form such as **http://csrc.nist.gov** are converted into the equivalent numeric IP (Internet Protocol) addresses such as **129.6.13.39**. Certain servers throughout the world maintain the databases needed, as well as perform the translations. A DNS server trying to perform a translation may communicate with other Internet DNS servers if it does not have the data needed to translate the address itself.

Like any other Internet-based system, DNS is subject to several threats. To counter these threats, the Internet Engineering Task Force (IETF)—an international standards body—came up with a set of specifications for securing DNS called DNS Security Extensions (DNSSEC). In partnership with the Department of Homeland Security, we have been actively involved in promoting the deployment of DNSSEC since 2004.

As part of this continuing effort, we published guidelines for DNSSEC deployment through our document SP 800-81, *Secure Domain Name System (DNS) Deployment Guide*, in May 2006. Our outreach tasks also included—

- Publication of a technical paper titled "Challenges in Securing the Domain Name System" in the Jan/Feb 2006 issue of the journal "IEEE Security and Privacy";

- Contribution to the first-released draft of the document, "Signing the Domain Name System Root Zone: Technical Specification," embodying ideas for implementing DNSSEC at the highest level of the global DNS hierarchy; and

- Inclusion of three DNS-related controls in NIST SP 800-53r1, *Recommended Security Controls for Federal Information Systems*, thereby prescribing mandatory controls for securing the DNS infrastructure in all U.S. Government agencies within the next year.

In addition to technical papers, guideline documents, and mandatory controls, we are also involved in developing performance data related to deployment of the new security controls in DNS. We developed tests to measure the impact on performance on DNS zones due to supporting and providing additional security records related to "Authenticated Proof of Non-Existence," and published the results at http://www-x.antd.nist.gov/dnssec.

NIST has also initiated efforts with the U.S. General Services Administration (GSA) to set in motion the process for securing the top-most DNS domain of the U.S. Government (i.e., .gov). GSA is also coordinating with some leading DNS product vendors to facilitate implementation of DNSSEC specifications in their products, so that U.S. industry and the service sector as a whole can have access to DNS product offerings with security features, thus providing an impetus to the growth of e-commerce.

Contact: Dr. Ramaswamy Chandramouli
(301) 975-5013
mouli@nist.gov

Mr. Douglas Montgomery (ANTD)
(301) 975-3630
dougm@nist.gov

### Border Gateway Protocol

The Border Gateway Protocol (BGP) is an inter-autonomous system routing protocol. An autonomous system is a network or group of networks under a common administration and with common routing policies. BGP is used to exchange routing information for the Internet and is the protocol used between Internet service providers (ISPs).

The BGP project was initiated in February 2004. The project aims to help industry to understand the potential risks to inter-domain routing and the design and implementation trade-offs of the various BGP security mechanisms currently proposed in the Internet Engineering Task Force (IETF) community. Previously there was a lack of awareness and knowledge in the information technology (IT) sector of the potential threats, risks, mitigation techniques, and their costs. The project also seeks to expedite convergence towards standardized, implemented, and deployed BGP security solutions.

Our project efforts were directed during the past year to focus on characterizing the problem and design space for BGP security technologies. Our subsequent work has focused primarily on two activities – large-scale simulation modeling of focused BGP attacks and analytical models of threat versus countermeasure effectiveness. We are working with industry and government network operators and security experts to—

- Identify the threats and vulnerabilities of BGP/inter-domain routing;

- Document best common practices in securing the current BGP deployments; and

- Provide deployment and policy guidance for emerging BGP security technologies.

In the past year, we completed the design and implementation of a general framework for modeling attacks on BGP protocols. The simulation framework was used to conduct extensive modeling of the effects of attacks on BGP. Researchers also investigated a vulnerability that arises from interactions between BGP features and a component of the protocol designed to reduce instability. By exploiting this component, attackers could introduce significant delays or disable parts of the Internet. While this vulnerability had been suggested as a possibility, no previous study had determined the magnitude and extent of its effects. The study also outlined a countermeasure, using an optional component of the BGP protocol, to reduce the risk from this vulnerability. Results of the project were presented in workshops for both researchers and industry practitioners who have day-to-day responsibility for network operations with major ISPs. A guideline of best practices for securing BGP was completed and released as a draft for comment in 2006. The publication will be updated to reflect needs expressed in comments and then released in final form in spring 2007 to assist industry and government. To raise awareness of the need for routing security, a NIST Information Technology Laboratory researcher published an article in *IEEE Security & Privacy*, one of the most widely read journals in information security.

The focus of our 2007 activities will be to extend the modeling and analysis tools to incorporate significantly larger and more realistic topologies. In fiscal year 2007, we will continue to make active contributions to the IETF Routing Protocols Security Working Group and other Internet standards bodies, helping to move the results of this research into practice.

http://www.antd.nist.gov/iipp.shtml

Contact: Mr. Rick Kuhn
(301) 975-3337
kuhn@nist.gov

Mr. Douglas Montgomery (ANTD)
(301) 975-3630
dougm@nist.gov

### Internet Protocol Version 6 (IPv6) and Internet Protocol Security (IPsec)

The Internet Protocol Version 6 (IPv6) is an updated version of the current Internet Protocol, IPv4. It has been, and continues to be, developed and defined by the Internet Engineering Task Force (IETF) in a series of consensus-based standard documents—Requests for Comment (RFCs), which are approved standards documents; and Internet Drafts (IDs), which are works-in-progress that may progress to become standards. These documents define the contents and behavior of network communications at every level of the networking stack, from applications down to the physical layer.

The primary motivations for the development of IPv6 were to increase the number of unique IP addresses and to handle the needs of new Internet applications and devices. In addition, IPv6 was designed with the following goals: increased ease of network management and configuration, expandable IP headers, improved mobility and security, and quality of service controls.

The U.S. Office of Management and Budget (OMB) has mandated that government agencies will incorporate IPv6 capability into their backbone (routers, gateways, etc.) by 2008. NIST personnel are actively participating in the Federal IPv6 Working Group, formed to help government agencies plan and execute the transition in an interoperable and secure manner. We are also developing an IPv6 profile to define which pieces and features of IPv6 are mandatory for government agencies, which are optional, and where these elements are definitively defined. A test and branding program is also being explored.

Internet Protocol Security (IPsec) is a framework of open standards for ensuring private communications over IP networks, which has become the most popular network layer security control. It can provide several types of data protection—confidentiality; integrity; data origin authentication; prevention of packet replay and traffic analysis; and access control. IPsec typically uses the Internet Key Exchange (IKE) protocol to negotiate IPsec connection settings, exchange keys, authenticate endpoints to each other, and establish security associations, which define the security of IPsec-protected connections. IPsec and IKE were added to IPv4 after the fact, but are now integrated into all of the major operating systems. For IPv6, IPsec and IKE are planned to be an integral part of the network protocols.

IPsec has several uses with the most common being a virtual private network (VPN). This is a virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and IP information transmitted between networks. Although VPNs can reduce the risks of networking, they cannot totally eliminate them. For example, a VPN implementation may have flaws in algorithms or software, or insecure configuration settings and values that attackers can exploit.

We are currently writing a guidance document on IPv6 and IPsec, to be released in FY 2007. This document will describe IPv6's new and expanded protocols, services, and capabilities. It will characterize new security threats posed by the transition to IPv6. It will issue guidance on IPv6 deployment, including transition, integration, configuration, and testing. It will also include several practical IPv6 transition scenarios. In addition, our personnel are also planning research on the challenges posed to intrusion detection systems (IDSs) and firewalls by adding IPv6 to the network.

---

Contacts: Ms. Sheila Frankel
(301) 975-3297
sheila.frankel@nist.gov

Mr. Douglas Montgomery (ANTD)
(301) 975-3630
dougm@nist.gov

### Wireless Security Standards

Many organizations and users have found that wireless communications and devices are convenient, flexible, and easy to use. Users of wireless local area network (WLAN) or Wi-Fi devices have the flexibility to move from one place to another while maintaining connectivity with the network. Wi-Fi, short for Wireless Fidelity, is an operability certification for WLAN products based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard that is widely used today. Wireless personal networks allow users to share data and applications with network systems and other users with compatible devices without being tied to printer cables and other peripheral device connections. Users of handheld devices such as PDAs and cellular phones can synchronize data between PDAs and personal computers, and can use network services such as wireless e-mail, Web browsing and Internet access. Further, wireless communications can help first responders to emergencies gain critical information, coordinate efforts, and keep communications working when other methods may be overwhelmed or non functioning.

While wireless networks are exposed to many of the same risks as wired networks, they are vulnerable to additional risks as well. Wireless networks transmit data through radio frequencies and are open to intruders unless protected. Intruders have exploited this openness to access systems, destroy or steal data, and launch attacks that tie up network bandwidth and deny service to authorized users.

This past year, a Special Publication dealing with wireless security issues was completed. This report, SP 800-97 (*Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11*i), provides readers with a detailed explanation of next-generation 802.11 wireless security. It describes the inherently flawed Wired Equivalent Privacy (WEP) and explains 802.11i's two-step approach (interim and long-term) to providing effective wireless security. It describes secure methods used to authenticate users in a wireless environment and presents several sample case studies of wireless deployment. It also includes guidance on best practices for establishing secure wireless networks using the emerging Wi-Fi technology. This SP will be published in FY 2007.

---

Contact: Ms. Sheila Frankel
(301) 975-3297
sheila.frankel@nist.gov

### Radio Frequency Identification Technology: Security Aspects

NIST SP 800-98, *Guidance for Securing Radio Frequency Identification (RFID) Systems*, was released for public review in September 2006. SP 800-98 provides an overview of RFID technology, the associated security and privacy risks, and recommended practices that will help organizations mitigate these risks, safeguard sensitive information, and protect the privacy of individuals.

SP 800-98 seeks to assist organizations in understanding the risks of RFID technology and security measures to mitigate those risks. It provides practical, real-world guidelines on how to initiate, design, implement, and operate RFID solutions in a manner that mitigates security and privacy risks. The document also provides background information on RFID applications, standards, and system components to assist in the understanding of RFID security risks and controls. This document presents information that is independent of particular hardware platforms, operating systems, and applications. The emphasis is on RFID solutions that are based on industry and international standards, although the existence of proprietary approaches is noted when they offer relevant security features not found in current standards.

This document has been created for executives, planners, systems analysts, security professionals, and engineers who are responsible for Federal business processes or information technology systems. Professionals with similar responsibilities outside the government should also benefit from the information this document provides. The document addresses both the needs of those considering an RFID implementation and those with an existing RFID solution. The document is also useful for those who seek an overview of RFID technology and related security issues. The final version of SP 800-98 will be available in early 2007.

---

Contact: Dr. Tom Karygiannis
(301) 975-4728
karygiannis@nist.gov

### Web Services Security

The advance of Web services technologies promises to have far-reaching effects on the Internet and enterprise networks. Web services based on the eXtensible Markup Language (XML), Simple Object Access Protocol (SOAP), and related open standards, and deployed in Service Oriented Architectures (SOAs) allow data and applications to interact without human intervention through dynamic and ad hoc connections. Web services technology can be implemented in a wide variety of architectures, can coexist with other technologies and software design approaches, and can be adopted in an evolutionary manner without requiring major transformations to legacy applications and databases.

The security challenges presented by the Web services approach are formidable and unavoidable. Many of the features that make Web services attractive, including greater accessibility of data, dynamic application-to-application connections, and relative autonomy (lack of human intervention) are at odds with traditional security models and controls. Difficult issues and unsolved problems exist, such as protecting—

- Confidentiality and integrity of data that is transmitted via Web services protocols in service-to-service transactions, including data that traverses intermediary (pass-through) services;

- Functional integrity of the Web services that requires both establishment in advance of the trustworthiness of services in orchestrations or choreographies, and the establishment of trust between services on a transaction-by-transaction basis; and

- Availability in the face of denial of service attacks that exploit vulnerabilities unique to Web service technologies, especially targeting core services, such as discovery service, on which other services rely.

In order to improve the understanding of different aspects of Web Services security, we have developed SP 800-95, *Guide to Secure Web Services*. This document discusses the different technologies and standards for securing Web services applications. It also provides some specific recommendations that web services application developers and architects can use to secure their applications. A draft of this publication was released for public comment in August 2006, and we plan to revise it and publish the final publication in 2007.

The SOA processing model requires the ability to secure SOAP messages and XML documents as they are forwarded along potentially long and complex chains of consumer, provider, and intermediary services. The nature of Web services processing makes those services subject to unique attacks, as well as variations on familiar attacks targeting Web servers.

The following is a summary of security techniques for Web Services that are discussed in the document—

- Confidentiality of Web Services Using XML Encryption: This is a specification from the World Wide Web Consortium (W3C), and it provides a mechanism to encrypt XML documents;

- Integrity of Web Services Using XML Signature: This is a specification produced jointly by the W3C and IETF. The power of XML signature is to selectively sign XML data;

- Web Services Authentication and Authorization using Security Assertion Markup Language (SAML) and eXtensible Access Control Markup Language (XACML) as proposed by the OASIS standards group;

- PKI for Web Services using XML Key Management Specification (XKMS); and

- WS-Security: This specification defines a set of SOAP header extensions for end-to-end SOAP messaging security. It supports message integrity and confidentiality by allowing communicating partners to exchange signed encrypted messages in a Web services environment.

We organized a workshop on "Web Services Security" that was held in Berkeley, California in May 2006 in collaboration with Purdue University. The workshop provided a forum for presentation, discussion, and dissemination of new results in the area of Web Services Security. We presented a paper titled "Guideline on Secure Web Services" at this workshop.

---

Contact: Dr. Anoop Singhal
(301) 975-4432
anoop.singhal@nist.gov

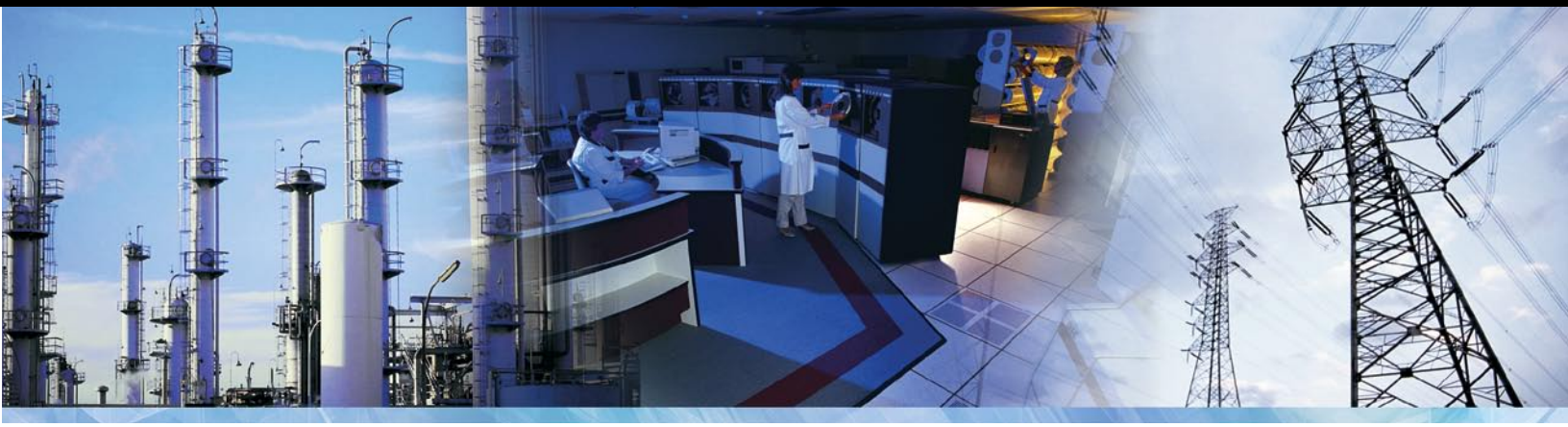
### Industrial Control Systems Security

Industrial control systems (ICSs) is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other smaller control system configurations often found in the industrial control sectors. Our work focuses on SCADA systems and DCSs, which are used in the electric, water, oil and gas, chemical, transportation, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (automotive, aerospace, and durable goods) industries.

SCADA systems are highly distributed systems used to control geographically dispersed assets, often scattered over thousands of square kilometers, where centralized data acquisition and control are critical to system operation. They are used in the distribution operations of water supply systems, oil and gas pipelines, electrical power grids, and railway transportation systems. A SCADA control center performs centralized monitoring and control for field sites over long-distance communications networks. This includes monitoring alarms and processing status data. Based on information received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices, which are often referred to as field devices. Field devices control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.

DCSs are used to control industrial processes such as electric power generation, oil and gas refineries, wastewater treatment, and chemical, food, and automotive production. DCSs are integrated as a control architecture containing a supervisory level of control overseeing multiple, integrated subsystems that are responsible for controlling the details of a localized process. DCSs are used extensively in process-based industries.

Most ICSs in use today were developed years ago, long before public and private networks, desktop computing, or the Internet were a common part of business operations. These systems were designed to meet performance, reliability, safety, and flexibility requirements and were typically physically isolated and based on proprietary hardware, software, and communication protocols. These proprietary communication protocols included basic error



detection and correction capabilities, but nothing that guaranteed secure communications. The need for cyber security measures within these systems was not anticipated, and, at the time, security for ICSs meant physically securing access to the network and the consoles that controlled the systems.

As microprocessor, personal computer, and networking technology evolved during the 1980s and 1990s, the design of ICSs changed to incorporate the latest technologies. Internet-based technologies started making their way into ICS designs in the late 1990s. These changes to ICSs exposed them to new types of threats and significantly increased the likelihood that they would be attacked. While security solutions have been designed to deal with these security issues in typical IT systems, special precautions must be taken when introducing these same solutions to ICS environments. In some cases, new IT security solutions are needed.

In the past year, we have collaborated with the NIST Manufacturing Engineering Laboratory (MEL) in developing a guide to ICS security, which was published as draft NIST SP 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*. The purpose of this document is to provide guidance for establishing secure SCADA systems and other ICSs. The document provides an overview of ICSs and typical system topologies, identifies typical vulnerabilities and threats to these systems, and provides recommended security countermeasures to mitigate the associated risks. The public draft of SP 800-82 was released in September 2006, and the final document is expected to be completed by late 2007. This guideline is being prepared for use by Federal agencies, but it may be used by non governmental organizations on a voluntary basis.

The draft underwent subject matter expert review by the NIST-led Process Control Security Requirements Forum (PCSRF), which was formed in the spring of 2001 by the MEL Intelligent Systems Division (ISD) in cooperation with the Computer Security Division (CSD). The PCSRF is a working group of users, vendors, and integrators in the process control industry that is addressing the cyber security requirements for industrial process control systems and components, including SCADA systems, DCS, Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), and Intelligent Electronic Devices (IED). Members of the PCSRF represent the critical infrastructures and related process-control industries including oil and gas, water, electric power, chemicals, pharmaceuticals, metals and mining, and pulp and paper. There are currently over 700 members in the PCSRF from government, industry, and academe. ISD leads the NIST effort with additional support provided from CSD and the NIST Electronics and Electrical Engineering Laboratory (EEEL).

---

http://www.isd.mel.nist.gov/projects/processcontrol/

Contacts: Mr. Keith Stouffer
Intelligent Systems Division, MEL
(301) 975-3877
keith.stouffer@nist.gov

Ms. Karen Scarfone
(301) 975-8136
karen.scarfone@nist.gov

### Guide to Secure Sockets Layer (SSL) Virtual Private Networks (VPNs)

SSL VPNs provide users with secure remote access to an organization's resources. An SSL VPN consists of one or more VPN devices to which users connect using their Web browsers. The traffic between the Web browser and SSL VPN device is encrypted with the SSL protocol. SSL VPNs can provide remote users with access to Web applications and client/server applications, as well as connectivity to internal networks. They offer versatility and ease of use because they use the SSL protocol, which is included with all standard Web browsers, so special client configuration or installation is often not required. In planning VPN deployment, many organizations are faced with a choice between an IPsec-based VPN and an SSL-based VPN. In 2005, we published NIST SP 800-77, *Guide to IPsec VPNs*. We are currently planning a complementary document, a Guide to SSL VPNs.

The purpose of the Guide to SSL VPNs will be to assist organizations in mitigating the risks associated with the transmission of sensitive information across networks by providing practical guidance on implementing SSL VPN-based security services. This document will present information that is independent of particular hardware platforms, operating systems, and applications, other than some real-world examples to illustrate particular concepts. The document will provide practical guidance for designing, implementing, configuring, security, monitoring, and maintaining SSL

VPN solutions. It will also provide an overview of complementary VPN technologies, such as SSH (Secure SHell) tunnels and IPsec. This SP will be published in FY 2007.

---

Contact: Ms. Sheila Frankel
(301) 975-3297
sheila.frankel@nist.gov

### Voice Over Internet Protocol Security Issues

Voice over IP (VoIP)—the transmission of voice over packet-switched IP networks—is one of the most important emerging trends in telecommunications. As with many new technologies, VoIP introduces both security risks and opportunities. For several years VoIP was a technology prospect, something on the horizon for the "future works" segment of telephony and networking papers. Now, however, telecommunications companies and other organizations have already moved, or are in the process of moving, their telephony infrastructure to their data networks. The VoIP solution provides a cheaper and clearer alternative to traditional Public Switched Telephone Network (PSTN) telephone lines. Although its implementation is widespread, the technology is still developing. It is growing rapidly throughout North America and Europe, but it sometimes can be difficult to integrate with existing systems. Nevertheless, VoIP will capture a significant portion of the telephony market given the fiscal savings and flexibility that it can provide.

VoIP systems take a wide variety of forms, including traditional telephone handsets, conferencing units, and mobile units. In addition to end-user equipment, VoIP systems include a variety of other components, including call processors/call managers, gateways, routers, firewalls, and protocols. Most of these components have counterparts used in data networks, but the performance demands of VoIP mean that ordinary network software and hardware must be supplemented with special VoIP components. Not only does VoIP require higher performance than most data systems, but critical services, such as Emergency 911, must be accommodated. One of the main sources of confusion for those new to VoIP is the (natural) assumption that because digitized voice travels in packets just like other data, existing network architectures and tools can be used without change. However, VoIP adds a number of complications to existing network technology, and these problems are magnified by security considerations.

Quality of Service (QoS) is fundamental to the operation of a VoIP network that meets users' quality expectations. However, the implementation of various security measures can cause a marked deterioration in QoS unless VoIP-specific equipment and architectures are used. These complications range from firewalls delaying or blocking call setups to encryption-produced latency and delay variation (jitter). Because of the time-critical nature of VoIP and its low tolerance for disruption and packet loss, many security measures implemented in traditional data networks are simply not applicable to VoIP in their current form; firewalls, intrusion detection systems, and other components must be specialized for VoIP. Most current VoIP systems use one of two standards—H.323 or the Session Initiation Protocol (SIP). Although SIP seems to be gaining in popularity, neither of these protocols has become dominant in the market yet, so it often makes sense to incorporate components that can support both.

With the introduction of VoIP, the need for security is compounded because now we must protect two invaluable assets—our data and our voice. Federal agencies are required by law to protect a great deal of information, even if it is unclassified. Both privacy-sensitive and financial data must be protected, as well as other government information that is categorized as sensitive but unclassified. Protecting the security of conversations is thus required. In a conventional office telephone system, intercepting conversations requires physical access to telephone lines or compromise of the office private branch exchange (PBX). Only particularly security-sensitive organizations bother to encrypt voice traffic over traditional telephone lines. The same cannot be said for Internet-based connections. For example, when ordering merchandise over the telephone, most people will read their credit card number to the person on the other end. The numbers are transmitted without encryption to the seller. In contrast, the risk of sending unencrypted data across the Internet is more significant. Packets sent from a user's home computer to an online retailer may pass through 15 to 20 systems that are not under the control of the user's ISP or the retailer. Anyone with access to these systems could install software that scans packets for credit card information. For this reason, online retailers use encryption software to protect a user's information and credit card number. So it stands to reason that if we are to transmit voice over the Internet Protocol, and specifically across the Internet, similar security measures must be applied.

The current Internet architecture does not provide the same physical wire security as the telephone lines. The key to securing VoIP is to use the security mechanisms like those deployed in data networks (firewalls, encryption, etc.) to emulate the security level currently enjoyed by PSTN network users.

VoIP can be done securely, but the path is not smooth. It will likely be several years before standards issues are settled and VoIP systems become a mainstream commodity. Until then, organizations must proceed cautiously and not assume that VoIP components are just more peripherals for the local network. Above all, it is important to keep in mind the unique requirements of VoIP, acquiring the right hardware and software to meet the challenges of VoIP security.

During the past year, CSD has considered the security implications of VoIP and worked to produce guidance for Federal agencies to use when developing and deploying VoIP systems. SP 800-58, *Security Considerations for Voice Over IP Systems*, was published in January 2005. This publication investigates the attacks and defenses relevant to VoIP and explores ways to provide appropriate levels of security for VoIP networks at reasonable cost. More than 1.2 million copies of the publication have been downloaded since its release. An updated publication is being prepared for 2007, to reflect changes in technology, revisions of standards, and new applications of VoIP and related technologies, such as video over Internet.

---

Contact: Mr. Rick Kuhn
(301) 975-3337
kuhn@nist.gov

## Technical Guidelines and Standards

### CSD's Part within National and International IT Security Standards Processes

The International Organization for Standardization (ISO) is a network of the national standards institutes of 148 countries, on the basis of one member per country. The scope of ISO covers standardization in all fields except electrical and electronic engineering standards, which are the responsibility of IEC, the International Electrotechnical Commission.

The IEC prepares and publishes international standards for all electrical, electronic, and related technologies, including electronics, magnetics and electromagnetics, electroacoustics, multimedia, telecommunication, and energy production and distribution, as well as associated general disciplines such as terminology and symbols, electromagnetic compatibility, measurement and performance, dependability, design and development, safety, and the environment.

Joint Technical Committee 1 (JTC1) was formed by ISO and IEC to be responsible for international standardization in the field of Information Technology. It develops, maintains, promotes, and facilitates IT standards required by global markets meeting business and user requirements concerning—

- design and development of IT systems and tools;
- performance and quality of IT products and systems;
- security of IT systems and information;
- portability of application programs;
- interoperability of IT products and systems;
- unified tools and environments;
- harmonized IT vocabulary; and
- user-friendly and ergonomically designed user interfaces.

JTC1 consists of a number of Subcommittees (SCs) and working groups that address specific technologies. SCs that produce standards relating to IT security include:

- SC 06 - Telecommunications and Information Exchange Between Systems
- SC 17 - Cards and Personal Identification
- SC 27 - IT Security Techniques
- SC 37 – Biometrics

JTC1 also has—

- Technical Committee 68 – Financial Services
- SC 2 - Operations and Procedures including Security
- SC 4 – Securities
- SC 6 - Financial Transaction Cards, Related Media and Operations
- SC 7 – Core Banking

American National Standards Institute (ANSI) is a private, nonprofit organization (501(c)(3)) that administers and coordinates the U.S. voluntary standardization and conformity assessment system.

***National Standardization***

ANSI facilitates the development of American National Standards (ANSs) by accrediting the procedures of standards-developing organizations (SDOs). The InterNational Committee for Information Technology Standards (INCITS) is accredited by ANSI.

***International Standardization***

ANSI promotes the use of U.S. standards internationally, advocates U.S. policy and technical positions in international and regional standards organizations, and encourages the adoption of international standards as national standards where they meet the needs of the user community.

ANSI is the sole U.S. representative and dues-paying member of the two major non-treaty international standards organizations ISO, and, via the U.S. National Committee (USNC), the IEC.

INCITS serves as the ANSI Technical Advisory Group (TAG) for ISO/IEC Joint Technical Committee 1. INCITS is sponsored by the Information Technology Industry (ITI) Council, a trade association representing the leading U.S. providers of information technology products and services. INCITS currently has more than 750 published standards.

INCITS is organized into Technical Committees that focus on the creation of standards for different technology areas. Technical committees that focus on IT security and IT security-related technologies include:

- B10 – Identification Cards and Related Devices
- CS1 – Cyber Security
- E22 – Item Authentication
- M1 – Biometrics
- T3 – Open Distributed Processing (ODP)
- T6 – Radio Frequency Identification (RFID) Technology

As a technical committee of INCITS, CS1 develops U.S. National, ANSI-accredited standards in the area of cyber security. Its scope encompasses—

- Management of information security and systems
- Management of third party information security service providers
- Intrusion detection
- Network security
- Incident handling
- IT security evaluation and assurance
- Security assessment of operational systems
- Security requirements for cryptographic modules
- Protection profiles
- Role based access control
- Security checklists
- Security metrics
- Cryptographic and non-cryptographic techniques and mechanisms including:
  - confidentiality
  - entity authentication
  - non-repudiation
  - key management
  - data integrity
  - message authentication
  - hash functions
  - digital signatures
- Future service and applications standards supporting the implementation of control objectives and controls as defined in ISO 27001, in the areas of—
  - business continuity
  - outsourcing
- Identity management, including:
  - identity management framework
  - role based access control
  - single sign-on
- Privacy technologies, including:
  - privacy framework
  - privacy reference architecture
  - privacy infrastructure
  - anonymity and credentials
  - specific privacy enhancing technologies.

The scope of CS1 explicitly excludes the areas of work on cyber security standardization presently underway in INCITS B10, M1, T3, T10 and T11; as well as other standard groups, such as the Alliance for Telecommunications

Industry Solutions, the Institute of Electrical and Electronics Engineers, Inc., the Internet Engineering Task Force, the Travel Industry Association of American, and Accredited Standards Committee (ASC) X9. The CS1 scope of work includes standardization in most of the same cyber security areas as are covered in the NIST Computer Security Division.

As the U.S. TAG to ISO/IEC JTC 1/SC 27, CS1 contributes to the SC 27 program of work on IT Security Techniques in terms, comments, and contributions on SC 27 standards projects; votes on SC 27 standards documents at various stages of development; and identifying U.S. experts to work on various SC 27 projects or to serve in various SC 27 leadership positions. All input from CS1 goes through INCITS to ANSI, then to SC 27. It is also a conduit for getting U.S.-based new work item proposals and U.S.-developed national standards into the international SC 27 standards development process.

Thus, NIST, through its membership on CS1, where Dan Benigni serves as the nonvoting chair, and Richard Kissel is the NIST Primary with vote, contributes to all CS1 national and international IT security standards efforts. NIST can also initiate IT security-related projects for national or international standardization through its membership on CS1. As an example, CSD staffer David Ferraiolo has recently discussed initiating a new project in CS1 concerning an access control mechanism that can be embedded into operating systems.

CS1 has created a task group called CS1.1 RBAC, with one national standards project called "Requirements for the Implementation of Role Based Access Control (RBAC)" INCITS Project 1794. This standard will provide implementation requirements for RBAC systems, which use RBAC components defined in INCITS 359-2004. The implementation requirements in this standard are intended to ensure the interchange of RBAC data (e.g., roles, permissions, users) and promote functional interoperability among RBAC services and applications.

In addition, CS1 has recently created another national standards project, "Minimum Security Guidelines for Protecting Personal Identifiable Information and Sensitive Information Stored on and Exchanged between Information Systems." The project is expected to result in an ANSI-INCITS Technical Report. In the future, this document may be submitted as an input document to SC 27. The document will also take into account certain publications in the NIST SP 800 series and incorporate those aspects that apply to the scope of protection of personal identifiable information.

As regards international efforts, CS1 has consistently, efficiently, and in a timely manner responded to all calls for contributions on all international security standards projects in ISO/IEC JTC1 SC 27. Contributions from CS1 members have included NIST publications. For instance, FIPS 199 and 200 have been cited as contributions to ongoing work at the international level.

---

Contact: Mr. Daniel Benigni
(301) 975-3279
benigni@nist.gov

### Overview of National and International IT Security Standards and Guidelines

NIST SP 800-99, *Guide to Information Technology Security Standards and Guidelines*, is expected to be released for public comment in March 2007. It provides an overview of IT security standards and guidelines, their uses, and who develops them. Much of the guide provides brief discussions of common IT-based technologies and security technologies, and selected U.S. Government acts and other legislation that govern IT security activities. The publication also explains the security standards and guidelines development process and principles.

### Securing Radio Frequency Identification (RFID) Systems

SP 900-98, *Guidance for Securing Radio Frequency Identification (RFID) Systems*, was released as a draft document for public comment in September 2006. This publication seeks to assist organizations in understanding the risks of RFID technology and security measures to mitigate those risks. It provides practical, real-world guidance on how to initiate, design, implement, and operate RFID solutions in a manner that mitigates security and privacy risks. The document also provides background information on RFID applications, standards, and system components to assist in the understanding of RFID security risks and controls. This document

presents information that is independent of particular hardware platforms, operating systems, and applications. The emphasis is on RFID solutions that are based on industry and international standards, although the existence of proprietary approaches is noted when they offer relevant security features not found in current standards.

### Secure Web Services

SP 800-95, *Guide to Secure Web Services*, was released as a draft document for public comment in August 2006. This publication seeks to assist organizations in understanding the challenges in integrating information security practices into Service Oriented Architecture (SOA) design and development based on Web services. The publication also provides practical, real-world guidance on current and emerging standards applicable to Web services, as well as background information on the most common security threats to SOAs based on Web services. This document presents information that is largely independent of particular hardware platforms, operating systems, and applications. Supplementary security devices (i.e., perimeter security appliances) are considered outside the scope of this publication. Interfaces between Web services components and supplementary controls are noted as such throughout this document on a case-by-case basis.

### Intrusion Detection and Prevention (IDP)

SP 800-94, *Guide to Intrusion Detection and Prevention (IDP) Systems* was released for public comment in August 2006, and replaces SP 800-31, *Intrusion Detection Systems*. SP 800-94 provides guidance on designing, implementing, configuring, securing, monitoring, and maintaining four classes of IDP systems: network-based, wireless, network behavior analysis software, and host-based. It focuses on enterprise IDP solutions, but most of the information in the publication is also applicable to standalone and small-scale IDP deployments.

### Computer Security Log Management

SP 800-92, *Guide to Computer Security Log Management*, was released for public comment in April 2006 and published as final in September 2006. It provides detailed information on developing, implementing, and maintaining effective log management practices throughout an enterprise. This includes guidance on establishing centralized log management infrastructures and log management processes. Recommendations are also provided on log management for individual systems.

### Forensics for Incident Response

SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, is intended to help organizations in handling computer security incidents and troubleshooting IT operational problems by providing practical guidance on performing computer and network forensics. SP 800-86, which was released as final in August 2006, describes the processes for performing effective forensics activities in support of incident response, and it provides advice regarding the use of different data sources, such as files, operating systems, network traffic, and applications.

### Test, Training, and Exercise Programs for IT Plans and Capabilities

SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, was published as final in September 2006. It provides guidance on maintaining IT plans, such as contingency and computer security incident response plans, in a state of readiness so that organizations can effectively respond to and manage adverse situations involving IT. Maintaining these plans includes training IT personnel to fulfill their roles and responsibilities, having plans exercised to validate policies and procedures, and having systems tested to ensure their operability.

### Malware Incident Prevention and Handling

SP 800-83, *Guide to Malware Incident Prevention and Handling*, provides recommendations for improving an organization's malware incident prevention measures through several layers of controls. The publication, which was released as final in November 2005, also gives extensive recommendations for enhancing an organization's existing incident response capability so that it is better prepared to handle malware incidents. The guide focuses on practical strategies for detection, containment, eradication, and recovery from incidents caused by any of several types of malware.

### Creating a Patch and Vulnerability Management Program

SP 800-40 Version 2, *Creating a Patch and Vulnerability Management Program*, was released in November 2005. This document provides guidance on creating a security patch and vulnerability management program and testing the effectiveness of that program. The primary audience is security managers who are responsible for designing and implementing the program. However, this document also contains information useful to system administrators and operations personnel who are responsible for applying patches and deploying solutions (i.e., information related to testing patches and enterprise patching software).

### Assessment of Access Control Systems

NIST Interagency Report (NISTIR) 7316, *Assessment of Access Control Systems*, was released in September 2006. The purpose of this document is to provide agencies with background information on access control policies, models, and mechanisms to assist them in securing their computer applications. The document discusses the capabilities, limitations, and qualities of the access control mechanisms that are embedded for each access control policy. This document is intended to provide practical and conceptual guidance for security managers, administrators, and procurement officers whose expertise is related to access control.

### E-mail Security

SP 800-45A, *Guidelines on Electronic Mail Security*, was released for public comment in August 2006. It is an update to the 2002 guideline. It is intended to aid organizations in the installation, configuration, and maintenance of secure mail servers and mail clients. Topics covered include e-mail standards, e-mail encryption and signing, mail server application security, and e-mail content filtering.

# Honors and Awards

## FED 100 AWARD – FEDERAL COMPUTER WEEK

**Curt Barker** was selected by Federal Computer Week to receive a 2006 "Fed 100" Award. The judges for these awards look for someone who has made a noticeable difference in an agency or in the community at large. Mr. Barker was recognized for managing arguably one of the Federal government's most ambitious information technology security efforts, the Personal Identity Verification (PIV) program. Under Mr. Barker's leadership, NIST produced Federal Information Processing Standards 201 quickly so that Federal agencies could meet the October 2006 deadline for compliance with Homeland Security Presidential Directive 12. "Perhaps his greatest gift is an ability to inspire extraordinary performance in the NIST PIV team," said Timothy Grance, manager of NIST's Systems and Network Security Group.

## FED 100 AWARD – FEDERAL COMPUTER WEEK

**Peter Mell** was selected by Federal Computer Week to receive a 2006 "Fed 100" Award. The judges for these awards look for someone who has made a noticeable difference in an agency or in the community at large. Mr. Mell was recognized for creating a National Vulnerability Database of all known cyber vulnerabilities. Compiled for publicly available sources, the Web-accessible database integrated four separate cyber vulnerability databases and added new services and additional cyber security information. In 2005, he analyzed about 5,000 vulnerabilities. Then he designed and coded the database and released it two months ahead of schedule. "Peter is a man of action determined to get the job done regardless of even daunting obstacles," said Tim Grance, manager of the Systems and Network Security group within CSD. "This project would normally take several years and involve a team of at least six personnel," Grance said. "Peter did it in eight months."

## FED 100 AWARD – FEDERAL COMPUTER WEEK

**Ron Ross** was selected by Federal Computer Week to receive a 2006 "Fed 100" Award. The judges for these awards look for someone who has made a noticeable difference in an agency or in the community at large. Dr. Ross was recognized for leading the development of major security guidelines for protecting Federal information and critical information systems. Those security guidelines, required by the Federal Information Security Management Act of 2002 (FISMA), define a consistent approach to setting security controls. As FISMA Implementation Project leader, Dr. Ross led teams in creating thousands of pages of guidelines for conducting security assessments, developing security plans, and providing security awareness training. He created a unified FISMA framework that gives Federal agencies a reasonable way to protect their critical information and information systems. "Ron's success in everything he does is his ability to embrace ideas from many sources and constructively integrate those into his analysis," said Joan Hash, former Acting Chief of CSD.

Dr. Ross also received the **Justice Management Division Award** from the U.S. Department of Justice and the Potomac Forum's **Leadership Award in Service to the Government IT Community** during 2006.

## GENE MILLIGAN AWARD FOR EFFECTIVE COMMITTEE MANAGEMENT

**Fernando Podio** was awarded the Gene Milligan Award for Effective Committee Management by the InterNational Committee for Information Technology Standards (INCITS) for his work with the Technical Committee M1, Biometrics. This award recognizes individuals who, as officers, have provided outstanding leadership to the subgroup in its national and/or international work, have demonstrated proficiency in achieving consensus in the national and/or international arenas, and have followed the approved procedures in an exemplary fashion.

## ANSI MERITORIOUS SERVICE AWARD

**Fernando Podio** was recognized by the InterNational Committee for Information Technology Standards (INCITS) for his role in advancing the development, adoption, and awareness of biometric standards.

# Computer Security Division Publications - 2006

| NIST Special Publications | | |
|---|---|---|
| SP 800-96 | PIV Card / Reader Interoperability Guidelines | September 2006 |
| SP 800-92 | Guide to Computer Security Log Management | September 2006 |
| SP 800-90 | Recommendation for Random Number Generation Using Deterministic Random Bit Generators | June 2006 |
| SP 800-88 | Guidelines for Media Sanitization | September 2006 |
| SP 800-87 | Codes for the Identification of Federal and Federally-Assisted Organizations | October 2005 |
| SP 800-86 | Guide to Integrating Forensic Techniques into Incident Response | August 2006 |
| SP 800-85B | PIV Data Model Test Guidelines | July 2006 |
| SP 800-85A | PIV Card Application and Middleware Interface Test Guidelines (SP800-73 compliance) | April 2006 |
| SP 800-84 | Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities | September 2006 |
| SP 800-83 | Guide to Malware Incident Prevention and Handling | November 2005 |
| SP 800-81 | Secure Domain Name System (DNS) Deployment Guide | May 2006 |
| SP 800-77 | Guide to IPsec VPNs | December 2005 |
| SP 800-76 | Biometric Data Specification for Personal Identity Verification | February 2006 |
| SP 800-73 Rev 1 | Interfaces for Personal Identity Verification | March 2006 |
| SP 800-69 | Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist | September 2006 |
| SP 800-68 | Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist | October 2005 |
| SP 800-56A | Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography | March 2006 |
| SP 800-40, Ver 2 | Creating a Patch and Vulnerability Management Program | November 2005 |
| SP 800-21 Rev 1 | Guideline for Implementing Cryptography in the Federal Government | December 2005 |
| SP 800-18 Rev 1 | Guide for Developing Security Plans for Federal Information Systems | February 2006 |

| NIST Draft Special Publications | | |
|---|---|---|
| SP 800-101 | Guidelines on Cell Phone Forensics | August 2006 |
| SP 800-100 | Information Security Handbook: A Guide for Managers | June 2006 |
| SP 800-98 | Guidance for Securing Radio Frequency Identification (RFID) Systems | September 2006 |
| SP 800-97 | Guide to IEEE 802.11i: Robust Security Networks | June 2006 |
| SP 800-95 | Guide to Secure Web Services | August 2006 |
| SP 800-94 | Guide to Intrusion Detection and Prevention (IDP) Systems | August 2006 |
| SP 800-89 | Recommendation for Obtaining Assurances for Digital Signature Applications | March 2006 |

| NIST Draft Special Publications *(continued)* | | |
|---|---|---|
| SP 800-82 | Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security | September 2006 |
| SP 800-80 | Guide for Developing Performance Metrics for Information Security | May 2006 |
| SP 800-78-1 | Cryptographic Algorithms and Key Sizes for Personal Identity Verification | July 2006 |
| SP 800-76-1 | Biometric Data Specification for Personal Identity Verification | September 2006 |
| SP 800-54 | Border Gateway Protocol Security | September 2006 |
| SP 800-53A | Guide for Assessing the Security Controls in Federal Information Systems | April 2006 |
| SP 800-53 Rev 1 | Recommended Security Controls for Federal Information Systems | July 2006 |
| SP 800-45A | Guidelines on Electronic Mail Security | August 2006 |
| SP 800-38D | Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication | April 2006 |

| Federal Information Processing Standards | | |
|---|---|---|
| FIPS 201-1 | Personal Identity Verification (PIV) of Federal Employees and Contractors | March 2006 |
| FIPS 200 | Minimum Security Requirements for Federal Information and Information Systems | March 2006 |
| FIPS 186-3 | Digital Signature Standard (DSS) | Draft, March 2006 |

| NIST Interagency Reports | | |
|---|---|---|
| NISTIR 7337 | Personal Identity Verification Demonstration Summary | August 2006 |
| NISTIR 7316 | Assessment of Access Control Systems | September 2006 |
| NISTIR 7313 | 5th Annual PKI R&D Workshop Proceedings: Making PKI Easy to Use | July 2006 |
| NISTIR 7298 | Glossary of Key Information Security Terms | May 2006 |
| NISTIR 7290 | Fingerprint Identification and Mobile Handheld Devices: An Overview and Implementation | March 2006 |
| NISTIR 7285 | Computer Security Division - 2005 Annual Report | February 2006 |
| NISTIR 7284 | Personal Identity Verification Card Management Report | January 2006 |
| NISTIR 7275 | Specification for the Extensible Configuration Checklist Description Format (XCCDF) | January 2006 |
| NISTIR 7250 | Cell Phone Forensic Tools: An Overview and Analysis | October 2005 |

| Information Technology Laboratory Bulletins written by the CSD | |
|---|---|
| September 2006 | Forensic Techniques: Helping Organizations Improve Their Responses To Information Security Incidents |
| August 2006 | Protecting Sensitive Information Processed And Stored In Information Technology (IT) Systems |
| June 2006 | Domain Name System (DNS) Services: NIST Recommendations For Secure Deployment |
| May 2006 | An Update On Cryptographic Standards, Guidelines, And Testing Requirements |
| April 2006 | Protecting Sensitive Information Transmitted In Public Networks |
| March 2006 | Minimum Security Requirements For Federal Information And Information Systems: FIPS 200 Approved By The Secretary Of Commerce |
| February 2006 | Creating A Program To Manage Security Patches And Vulnerabilities: NIST Recommendations For Improving System Security |
| January 2006 | Testing And Validation Of Personal Identity Verification (PIV) Components And Subsystems For Conformance To Federal Information Processing Standard 201 |
| December 2005 | Preventing And Handling Malware Incidents: How To Protect Information Technology Systems From Malicious Code And Software |
| November 2005 | Securing Microsoft Windows XP Systems: NIST Recommendations For Using A Security Configuration Checklist |
| October 2005 | National Vulnerability Database: Helping Information Technology System Users And Developers Find Current Information About Cyber Security Vulnerabilities |

# Ways to Engage Our Division and NIST

## Guest Research Internships at NIST

Opportunities are available at NIST for 6- to 24-month internships within the CSD. Qualified individuals should contact the CSD, provide a statement of qualifications, and indicate the area of work that is of interest. Generally speaking, the salary costs are borne by the sponsoring institution; however, in some cases, these guest research internships carry a small monthly stipend paid by NIST. For further information, contact Mr. Curt Barker, (301) 975-8443, curt.barker@nist.gov.

## Details at NIST for Government or Military Personnel

Opportunities are available at NIST for 6- to 24-month details at NIST in the CSD. Qualified individuals should contact the CSD, provide a statement of qualifications, and indicate the area of work that is of interest. Generally speaking, the salary costs are borne by the sponsoring agency; however, in some cases, agency salary costs may be reimbursed by NIST. For further information, contact Mr. Curt Barker, (301) 975-8443, curt.barker@nist.gov.

## Federal Computer Security Program Managers' Forum

The FCSPM Forum is covered in detail in the Outreach section of this report. Membership is free and open to Federal employees. For further information, contact Ms. Marianne Swanson, (301) 975-3293, marianne.swanson@nist.gov.

## Security Research

NIST occasionally undertakes security work, primarily in the area of research, funded by other agencies. Such sponsored work is accepted by NIST when it can cost-effectively further the goals of NIST and the sponsoring institution. For further information, contact Mr. Tim Grance, (301) 975-3359, tim.grance@nist.gov.

## Funding Opportunities at NIST

NIST funds industrial and academic research in a variety of ways. Our Advanced Technology Program co-funds high-risk, high-payoff projects with industry. The Small Business Innovation Research Program funds R&D proposals from small businesses. We also offer other grants to encourage work in specific fields: precision measurement, fire research, and materials science. Grants/awards supporting research at industry, academia, and other institutions are available on a competitive basis through several different Institute offices. For general information on NIST grants programs, contact Ms. Joyce Brigham, (301) 975-6329, joyce.brigham@nist.gov.

## Summer Undergraduate Research Fellowship (SURF)

Curious about physics, electronics, manufacturing, chemistry, materials science, or structural engineering? Intrigued by nanotechnology, fire research, information technology, or robotics? Tickled by biotechnology or biometrics? Have an intellectual fancy for superconductors or perhaps semiconductors?

Here's your chance to satisfy that curiosity. By spending part of your summer working elbow-to-elbow with researchers at NIST, one of the world's leading research organizations and home to three Nobel Prize winners. Gain valuable hands-on experience, work with cutting-edge technology, meet peers from across the Nation (from San Francisco to Puerto Rico, New York to New Mexico), and sample the Washington, D.C., area. And, get paid while you're learning. For further information, see **http://www.surf.nist.gov**, or contact NIST SURF Program, 100 Bureau Dr., Stop 8400, Gaithersburg, MD 20899-8499, (301) 975-4200, NIST_SURF_program@nist.gov.


**U.S. Department of Commerce**
Carlos M. Gutierrez, *Secretary*

**Technology Administration**
Robert Cresanti, *Under Secretary of Commerce for Technology*

**National Institute of Standards and Technology**
William Jeffrey, *Director*

NISTIR 7399

March 2007

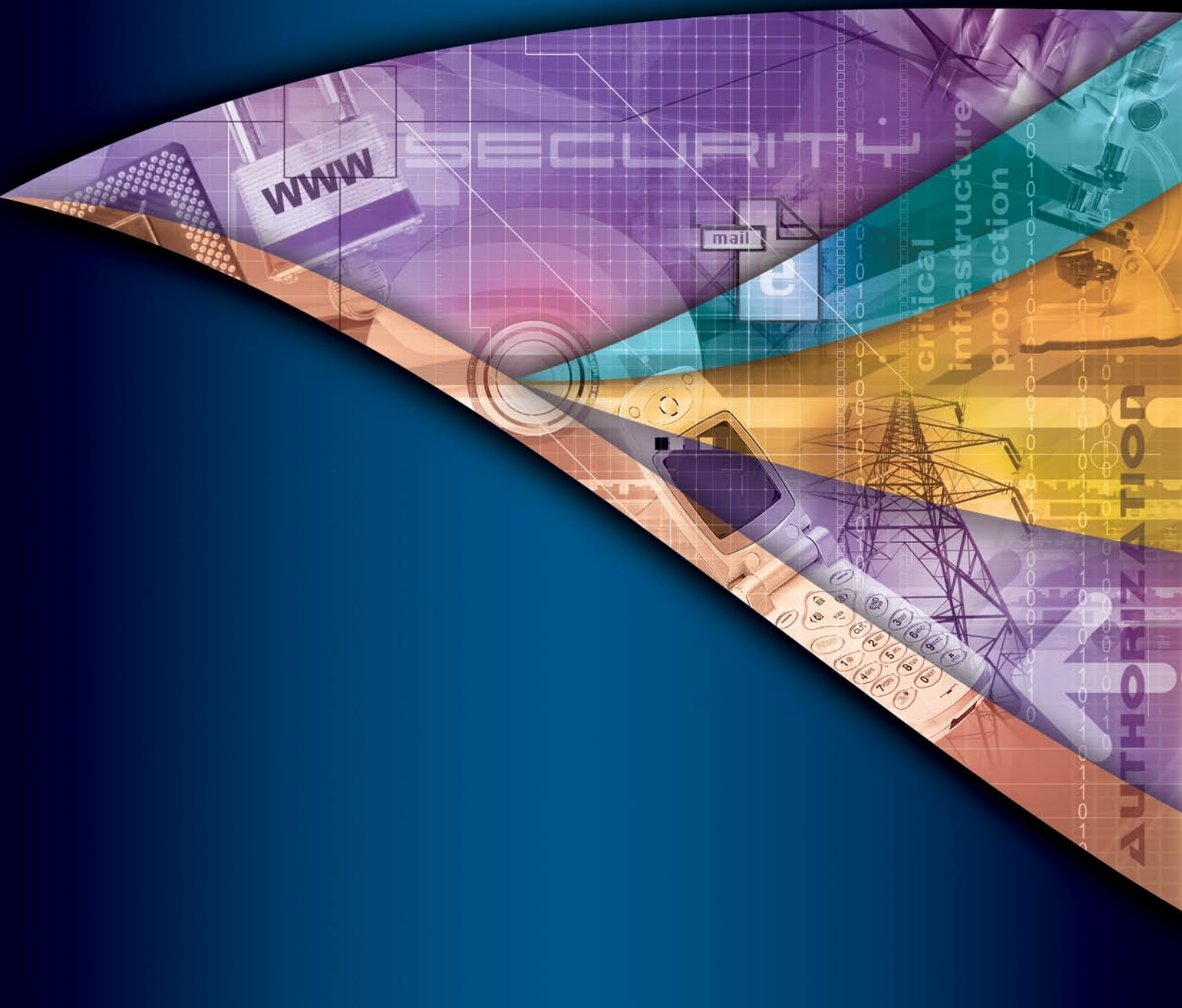
---

Tanya Brewer, *Editor*
Kevin Stine, *Editor*

**Computer Security Division**
Information Technology Laboratory
National Institute of Standards and Technology

Michael James, *Art Director*
The DesignPond

---


WWW
mail
critical
infrastructure
protection
AUTHORIZATION