Computer Security Division

2005 Annual Report

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

Table of Contents

Welcome

This year the Computer Security Division (CSD) continued its efforts to improve information system security. This effort was accomplished through raising awareness of information technology risks, vulnerabilities, and protection requirements—particularly for new and emerging technologies. We continued to research, study, advise Agencies of IT vulnerabilities, and devise techniques for the cost-effective security and privacy of sensitive Federal 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. This effort was conducted to assist our ever-expanding customer base that now includes federal, state, and local governments, the healthcare community, colleges and universities, small businesses, the private sector, and the international community.

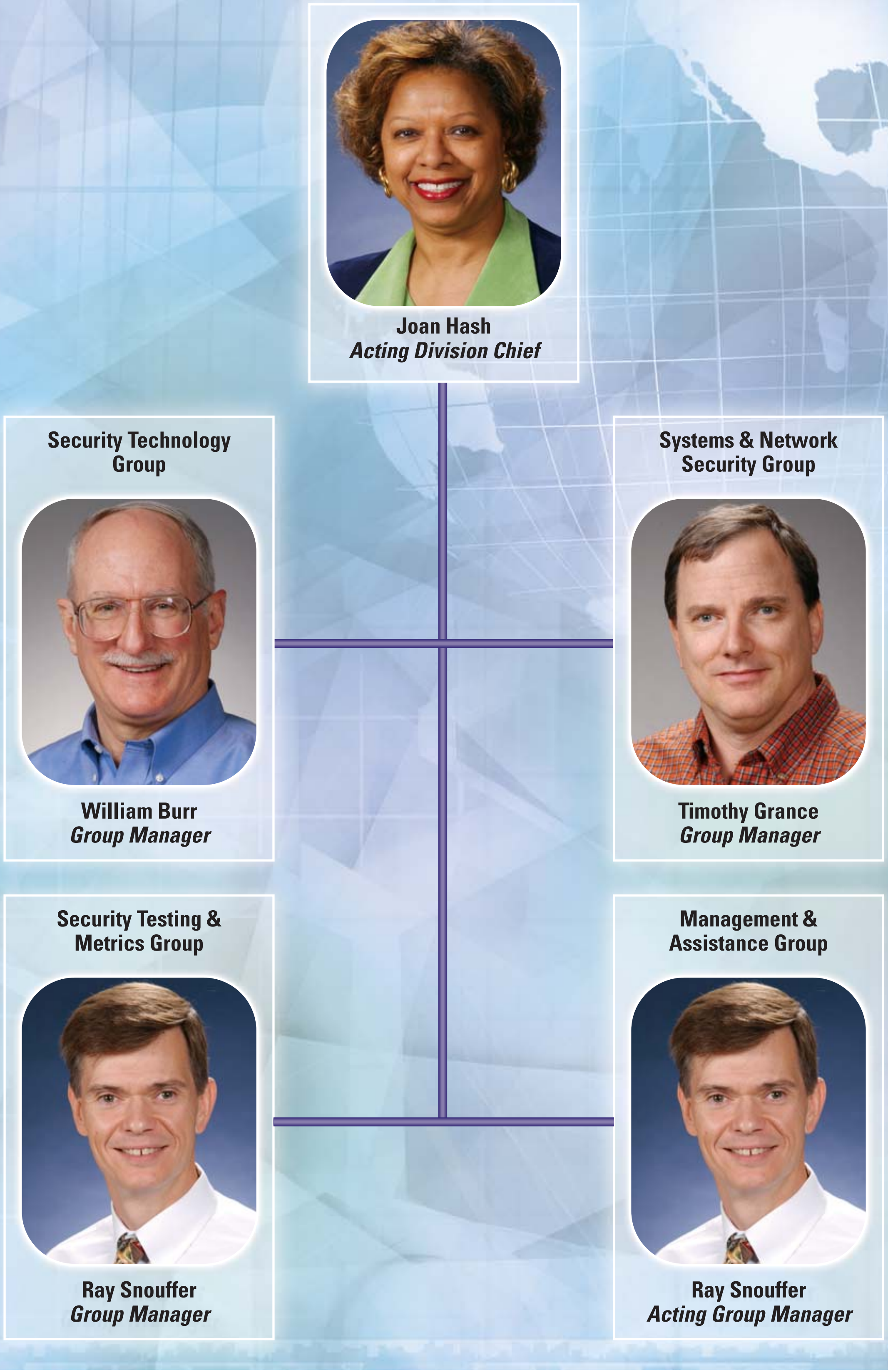
This year also brought additional security challenges along with the ever-advancing improvements in technology, improvements in citizens' access to government systems and information, faster communications, reduced paperwork, and streamlined processes. Our work this year met those security challenges 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.

Among the highlights of 2005 was further work on addressing the challenges of Homeland Security Presidential Directive 12 and facilitating the success of the timelines set for the new standard for identification and verification of Federal employees and contractors. We continued our progress in fulfilling the mandates of the Federal Information Security Management Act of 2002 (FISMA), which resulted in Special Publication (SP) 800-53, *Security Controls for Federal Information Systems*; a draft of SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*; and a draft of Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*. The work and expansion of the Cryptographic Module Validation Program continues to ensure the protection of sensitive information in computer and telecommunication systems, including voice systems, and has gained international interest. This, along with our further efforts concerning digital forensic tools and methods, Internet security protocols, creation of the National Vulnerability Database, and outreach to our customer community are just a few of the many accomplishments that mark 2005.

We know that the work we do is essential to building trust and confidence in products and services to the public we serve.

Joan Hash
Acting Division Chief

Division Organization



Joan Hash
Acting Division Chief

Security Technology Group

William Burr
Group Manager

Systems & Network Security Group

Timothy Grance
Group Manager

Security Testing & Metrics Group

Ray Snouffer
Group Manager

Management & Assistance Group

Ray Snouffer
Acting Group Manager

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

OVERVIEW

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 (FISMA), included duties and responsibilities for the Computer Security Division in Section 303 "National Institute of Standards and Technology." In 2005, we addressed these assignments as follows:

- **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* (first public draft issued July 2005).
- **Minimum information security requirements (management, operational, and technical security controls) for information and information systems in each such category** – Developed SP 800-53, *Security Controls for Federal Information Systems* (final version issued February 2005).
- **Methods for assessing effectiveness of security requirements** - SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (first public draft issued July 2005).
- **Procedures for capturing results of security requirement assessments and results of security program assessments** – SP 800-26 Revision 1, *Guide for Information Security Program Assessments and System Reporting Form* (first public draft issued August 2005).
- **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* (first public draft issued August 2005).
- **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.
- **Annual NIST reporting requirement** – Produce an annual report as a NIST Interagency Report (IR). The 2004 Annual Report was issued as NIST IR 7219, and is available via the Web or upon request.

OUTREACH, AWARENESS, AND EDUCATION

STRATEGIC GOAL ▸ *The Computer Security Division (CSD) will engage in outreach activities to Federal government agencies and, where appropriate, to industry, including small- and medium-sized businesses, in order to raise awareness of the importance and need for information technology (IT) security. These activities will increase the understanding of IT security vulnerabilities and possible corrective measures. Resulting raised awareness and knowledge will also assist appropriate persons in framing requests for necessary resources to implement better IT security measures. Finally, these outreach activities will facilitate a greater awareness of the Division's programs, projects, and resources available to Federal agencies and the public.*

OVERVIEW

CSD provides IT security standards and guidelines to Federal government agencies in the Executive Branch of the government. 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 Federal Information Processing Standard (FIPS) and Special Publication (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-sized businesses nationwide, and even directly to citizens.

One of the primary benefits of these outreach efforts to the public is the large collection of non-proprietary, non-technology-biased knowledge that is provided free of charge to the 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.

In 2005, CSD greatly expanded its outreach efforts with the private sector. We formed new coalitions to support small business outreach, made significant enhancements to the Computer Security Resource Center (CSRC), and continued utilizing the Federal Computer Security Managers' Forum and the Federal Agency Security Practices site to provide support to information security officers throughout the Federal sector. Numerous workshops and briefings were sponsored to support implementation of newly developed guidance, and feedback from constituents was very positive.

As we look forward to fiscal year 2006, we will continue to expand outreach efforts to new communities, enhance the CSRC, support the Information Security and Privacy Advisory Board in its advisory capacity, and support the Federal Information Systems Security Educators Association. The Federal Computer Security Managers' Forum will continue to be a valuable communication vehicle for the Federal agencies, and we will launch an aggressive campaign to explore new methods to get our message out.

REACHING OUR GOAL

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 Office of Management and Budget, 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 twelve individuals and a Chairperson. The Director of NIST approves membership appointments and appoints the Chairperson. Each Board member

ISPAB Members and Secretariat (l to r): Elaine Frye, Pauline Bowen, Lynn McNulty, Rebecca Leng, Alexander Popowycz, Joseph Guirreri, Morris Hymes, Sallie McDonald, Franklin Reeder, and Leslie Reis. Not pictured: Daniel Chenok, Susan Landau, Steven Lipner, and Howard Schmidt.

normally 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 Congressional branches of the Federal government, civil service, senior executive service, the military, some of the largest corporations worldwide, small and medium-sized 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 (one Board member is an attorney), an extensive history of professional publications, and professional journalism. Members have worked (and in many cases, are continuing 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 Federal Public Key Infrastructure (PKI) effort, 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.

The 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 Public Law 107-347, The E-Government Act of 2002, Title III, The Federal Information Security Management Act of 2002, 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 the Office of Management and Budget (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. One of the most significant pieces of work the Board completed this previous year was a letter issued in January 2005 to Mr. Joshua Bolten, Director of OMB. The letter offers comments and advice on Section 522 of the Consolidated Appropriations Act of 2005, Division H Transportation/Treasury, that provides for the establishment of statutory Chief Privacy Officers in Federal departments and agencies. Among the Board's four major categories of recommendations, three specific initiatives are particularly relevant to Section 522 and to its establishment of Chief Privacy Officers—

- Identifying government-wide, standardized privacy requirements or requirements definitions which can reflect mandates set forth in the Privacy Act, other statutes and regulations, and assisting in determining where there are policy gaps or conflicts;
- Establishing mechanisms to ensure that those government officials responsible for the protection of private information understand and can accommodate, to the extent permitted by statute and regulation, the needs for data sharing and data matching

of law enforcement agencies seeking to enhance homeland security; and

- Establishing a formal working relationship among privacy officials, information security officials, Agency CIO's, and the records management community, each of which has a major role in managing government data and setting records management policies.

The paper is publicly available in its entirety at **http://csrc.nist.gov/ispab/board-recommendations.html.**

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. Topics have included the Government Line of Business Initiative, the Department of Homeland Security's Annual Privacy Report, HIPAA compliance and privacy issues, radio frequency identification (RFID) Efforts of SRA, role of the Chief Privacy Officer—panel discussion, the Privacy Act, the Department of Commerce's RFID effort, a supervisory control and data acquisition (SCADA) briefing, a briefing on the National Information Assurance Partnership (NIAP) report, and personal identity verification (PIV) briefings.

Several areas of interest that the Board will be following in the coming year include credentialing of certification and accreditation organizations, privacy management issues within government systems, OMB's Security Line of Business Initiative, role of the Federal Chief Privacy Officer, continuity of operations efforts, Federal Enterprise Security Architecture, identity management and authentication issues such as personal identity verification (PIV), NIAP program activities, NIST outreach and partnering approaches, and cyber security leadership in the Executive Branch.

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

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

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 a 12-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 honoring distinguished accomplishments in information systems security training programs. The Educator of the Year for 2004, awarded in March 2005, was Dr. Gail-Joon Ahn. Dr. Ahn is an Assistant Professor in the Department of Software and Information Service at the University of North Carolina at Charlotte. 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 2005 spanned Federal agencies, industry, military, contractors, State governments, academia, the press, and foreign organizations to reach 1,188 members in a total of 14 countries. The nearly 700 Federal agency members represent 89 agencies from the Executive and Congressional branches of government.

FISSEA hosted three free workshops, How to Use NIST Special Publication 800-16, in November and December 2004 and January 2005. The workshops were presented by Mark Wilson, editor of Special Publication (SP) 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*. FISSEA will continue to offer free workshops in 2006.

The 2006 FISSEA Conference, Training for a Cyber Secure Future, will be held March 20-21, at the Bethesda North Marriott Hotel and Conference Center in Bethesda, Maryland. Information security awareness, resources, and the Federal Information Security Management Act of 2002 (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

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 2005, CSRC had over 26.5 million requests—an average of over 2.2 million requests per month. 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 had been 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 2006. There was a survey to assess public opinion of the site's recent changes and the current usefulness and ease-of-use. It is anticipated that the site will be further enhanced as results of the survey and public comments are received and taken into consideration. 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 re-design of the Web pages.

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

SMALL AND MEDIUM-SIZED 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 others 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-sized 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.

For the fourth year, a CSD representative has attended the Annual Small Business Development Centers Conference to reach out to this public-private organization sponsored by SBA. This was the second year we were invited to conduct a conference presentation detailing our program, and it was received very well with many attendees.

In October 2004, a half-day workshop was held at the Fairfax Chamber of Commerce facility in Fairfax, Virginia. The National Cyber Security Alliance (NCSA) arranged for and assisted in the promotion of the workshop.

Mr. Richard Kissel attended planning meetings hosted by the State Department's office on the Asia-Pacific Economic Cooperation (APEC). A focus of these meetings was an information security education outreach for small and medium businesses held during APEC's Spring 2005 meeting in Lima, Peru. Others attending these working meetings were representatives from the Carnegie Mellon Software Engineering Institute, the Internet Security Alliance, SBA, and the Department of Justice.

In May 2005, three workshops were held in Texas. A half-day workshop and a full-day workshop were held in San Antonio, and a half-day workshop was held in Austin under the sponsorship of the Texas State Government's Department of Information Resources.

In 2006, the SMB outreach effort will focus on expanding opportunities to reach 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 March 2006, six half-day workshops will be presented in southern California. San Diego, Santa Ana, and Los Angeles will be the sites of two half-day workshops each. Planning is ongoing for a series of six to eight workshops in Colorado and Wyoming in June 2006. Tentative locations are Colorado Springs, CO; Denver, CO; Cheyenne, WY; and Casper, WY. Discussions are also underway to host a separate series of workshops in North Dakota, South Dakota, and Minnesota in June 2006.

Finally, we plan to send a representative to the 2006 InfraGard National Congress, where a presentation on this outreach may be given.

http://csrc.nist.gov/securebiz/
http://sbc.nist.gov/
Contacts: Mr. Richard Kissel
(301) 975-5017
richard.kissel@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 the Federal Information Security Management Act of 2002 (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 bi-monthly meetings to discuss 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), Windows XP SP2, recommended security controls, voice over Internet protocol (IP) security considerations, certification and accreditation, and status reports on the NIST FISMA Project. This year's annual off-site meeting featured updates on the computer security activities of the Government Accountability Office, NIST, the Office of Management and Budget, and the activities of the Department of Homeland Security. Briefings were also provided on personal digital assistant (PDA) forensics, patch management and malware, radio frequency identification (RFID) technology, reporting tools, and updates on several NIST Special Publications. In the next year, there are plans to have a two-day workshop on reporting tools.

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

SECURITY MANAGEMENT AND GUIDANCE

STRATEGIC GOAL ▸ *The Computer Security Division (CSD) will provide Federal agencies with relevant, timely and useful computer security policy and management tools. The CSD will assist managers at all levels that deal with, or have ultimate responsibility for, information technology (IT) security programs in understanding the activities that must be initiated and completed to develop a sound information security program. This can include an awareness of and understanding of how to deal with new issues solely from a management view and how to effectively apply NIST guidelines and recommendations.*

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 critical 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 Office of Management and Budget (OMB), the 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 Federal Information Security Management Act of 2002 (FISMA) Implementation Project, guidance for implementing the Security Rule of the Healthcare Information Portability and Accountability Act (HIPAA), integrating security into the capital planning and investment control process, a guide to IT security in the system development life cycle, extended outreach initiatives and information security training, awareness, and education. Key to the success of this area is our ability to interact with a broad constituency—Federal and non-Federal—in order to ensure that our program is consistent with national objectives related to or impacted by information security.

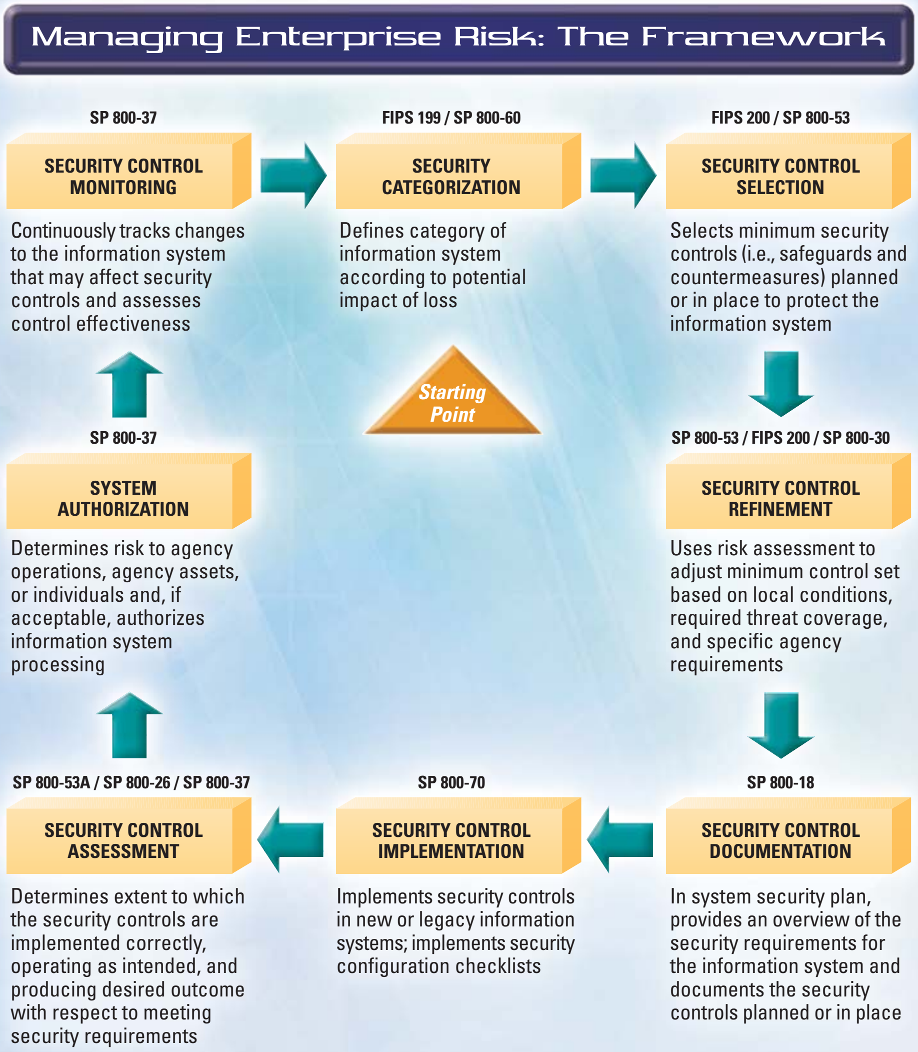
REACHING OUR GOAL

FISMA IMPLEMENTATION PROJECT

In response to the Federal Information Security Management Act of 2002 (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—

- **Standards** for categorizing information and information systems by mission impact or business case
- **Standards** for minimum security requirements for information and information systems
- **Guidelines** for mapping types of information and information systems to security categories
- **Guidelines** for identifying information systems as national security systems
- **Guidelines** for selecting appropriate security controls for information systems
- **Guidelines** for assessing security controls and determining security control effectiveness, and
- **Guidelines** for certifying and accrediting information systems.

At the core of the new security vision and strategy is the development and implementation of an enterprise risk management framework that addresses all aspects of information security throughout the System Development Life Cycle (SDLC). The framework provides a



Managing Enterprise Risk: The Framework

SP 800-37
SECURITY CONTROL MONITORING
Continuously tracks changes to the information system that may affect security controls and assesses control effectiveness

FIPS 199 / SP 800-60
SECURITY CATEGORIZATION
Defines category of information system according to potential impact of loss

FIPS 200 / SP 800-53
SECURITY CONTROL SELECTION
Selects minimum security controls (i.e., safeguards and countermeasures) planned or in place to protect the information system

Starting Point

SP 800-53 / FIPS 200 / SP 800-30
SECURITY CONTROL REFINEMENT
Uses risk assessment to adjust minimum control set based on local conditions, required threat coverage, and specific agency requirements

SP 800-18
SECURITY CONTROL DOCUMENTATION
In system security plan, provides an overview of the security requirements for the information system and documents the security controls planned or in place

SP 800-70
SECURITY CONTROL IMPLEMENTATION
Implements security controls in new or legacy information systems; implements security configuration checklists

SP 800-53A / SP 800-26 / SP 800-37
SECURITY CONTROL ASSESSMENT
Determines extent to which the security controls are implemented correctly, operating as intended, and producing desired outcome with respect to meeting security requirements

SP 800-37
SYSTEM AUTHORIZATION
Determines risk to agency operations, agency assets, or individuals and, if acceptable, authorizes information system processing

cost-effective, risk-based approach to protecting federal information and information systems and brings together all of the FISMA-related security standards and guidelines into an integrated package that supports the development of comprehensive, enterprise-wide information security programs. The key components of the risk framework include—

- **Determining** the importance or value of an information system to an enterprise's mission or business case
- **Establishing** a level of due diligence through the application of minimum (baseline) security controls
- **Refining** the security controls based on local conditions to meet specific enterprise security requirements
- **Documenting** the security controls for the enterprise information system in a comprehensive security plan
- **Implementing** the security controls in both legacy and new/developmental information systems
- **Assessing** the security controls in the enterprise information system to determine if they are effective
- **Determining**, based on assessment results, the risk to the enterprise's mission or business case by operating the information system
- **Authorizing** the information system for operation, if residual vulnerabilities are acceptable, and
- **Monitoring** the information system on a continuous basis to ensure adequate security for the enterprise.

The security standards and guidelines being developed in Phase I of the FISMA Implementation Project will assist Federal agencies in completing the individual steps in the risk management framework as part of a well-defined and disciplined SDLC process. The standards and guidelines will also help Federal agencies implement the provisions of FISMA, demonstrate compliance to specific requirements contained within the legislation, and establish a level of security due diligence across the Federal government.

http://csrc.nist.gov/sec-cert
Contacts: Ms. Joan Hash
(301) 975-5236
joan.hash@nist.gov

Mr. Ray Snouffer
(301) 975-5236
ray.snouffer@nist.gov

MINIMUM SECURITY REQUIREMENTS AND SECURITY CONTROLS

A key component of the FISMA legislation is the requirement to establish minimum security requirements for federal information and information systems. An initial public draft of Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, was completed during the past year and released for public comment in July 2005. This mandatory standard, which is due for final publication in early 2006 when approved by the Secretary of Commerce, specifies minimum security requirements for federal information and information systems in 17 security-related areas. Federal agencies and their support contractors will be required to meet the minimum security requirements in FIPS 200 by selecting the appropriate security controls and assurance requirements in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* (published in February 2005). Security controls are the management, operational, and technical safeguards and countermeasures prescribed for an information system which, taken together, adequately protect the confidentiality, integrity, and availability of the system and its information. The process of selecting appropriate security controls for organizational information systems to achieve adequate security is a multifaceted, risk-based activity involving management-level and operational-level personnel.

Security categorization of federal information and information systems, as required by FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems*, is the first step in the risk management process. Subsequent to the security categorization process, agencies must implement an appropriate set of security controls for their information systems that satisfy the minimum security requirements set forth in FIPS 200. The implemented set of security controls must be one of the three, appropriately tailored security control baselines from NIST Special Publication 800-53 that are associated with the designated impact level (e.g., low, moderate, or high) of the agency's information system as determined during the security categorization process. The application of the security control baselines defined in NIST Special Publication 800-53 represents the current state-of-the-practice safeguards and countermeasures for information systems. The catalog of security controls in NIST Special Publication 800-53 will be reviewed by us at least annually and, if necessary, revised and extended to reflect: (i) the experience gained from using the controls; (2) the changing security requirements within federal agencies; and (3) the new security technologies that may be available. The minimum security controls, selected from the catalog of security controls and defined in the low, moderate, and high security control baselines, are also expected to change over time as well, as the level of security and due diligence for mitigating risks within federal agencies increases. The proposed additions, deletions, or modifications to the catalog of security controls and the proposed changes to the security control baselines in NIST Special Publication 800-53 will go through a rigorous, public review process to obtain government and private sector feedback and to build consensus for the changes. State and local governments, as well as private sector organizations, are being encouraged to adopt the minimum security requirements and security controls on a voluntary basis to help protect the information infrastructure within the United States.

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

Mr. Arnold Johnson
(301) 975-3247
arnold.johnson@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 on 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. 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 (iv) 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. To assist Federal agencies in conducting assessments of the security controls in their information systems, we are developing a comprehensive set of assessment methods and procedures for each security control in Special Publication 800-53. An initial public draft of NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, was completed in July 2005 with the final publication expected in March 2006. The guideline 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
Contacts: Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

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

ORGANIZATIONAL ACCREDITATION PROGRAM

Phase II of the FISMA Implementation Project will focus on the development of a program for accrediting public and private sector organizations to provide security certification services for federal agencies. The term "accreditation" is used in two different contexts in the FISMA Implementation Project. "Security accreditation" is the official management decision to authorize operation of an information system. "Organizational accreditation" involves comprehensive proficiency testing and the demonstration of specialized skills in a particular area of interest. A security certification is a comprehensive assessment of the management, operational and technical security controls in an information system, made in support of security accreditation, 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. Organizations that participate in the accreditation program will be able to demonstrate competence in performing assessments of security controls implemented in an information system. Developing a network of accredited organizations with demonstrated competence in the provision of security certification services will give federal agencies greater confidence in the acquisition and use of such services and lead to increased information security for the federal government. The organizational accreditation project consists of four phases—

- Development and selection of an appropriate accreditation model for determining the competency of organizations desiring to provide security certification services in accordance with NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*
- Development of detailed accreditation 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 of the accreditation program during each phase of development as described above. The vetting process will include public workshops to discuss various accreditation approaches and models, a public review of the proposed assessment methods and procedures contained in Special Publication 800-53A, and a public review of the implementation strategy for the accreditation program. The first public workshop for the organizational accreditation program will be in spring 2006.

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

SECURITY PRACTICES AND POLICIES

Today's Federal networks and systems are highly interconnected and interdependent with non-Federal systems. Protection of the Nation's critical infrastructure 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, 43 practices and examples were added to the collection bringing the total to 169.

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) 975-2938
pauline.bowen@nist.gov

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

AUTOMATED SECURITY SELF-EVALUATION TOOL

An important element of measuring the status of information technology (IT) security within an organization is to perform routine self-assessments of an organization's IT systems. There are many methods and tools available to help agency officials determine the current status of their security programs relative to existing policy. Ideally many of these methods and tools would be implemented on an ongoing basis to systematically identify programmatic weaknesses and, where necessary, establish targets for continuing improvement. For a self-assessment to be effective, a risk assessment should be conducted in conjunction with or prior to the self-assessment. A self-assessment does not eliminate the need for a risk assessment.

The Automated Security Self-Evaluation Tool (ASSET) automates the process of completing a system self-assessment. ASSET will assist organizations in completing the self-assessment questionnaire contained in NIST Special Publication (SP) 800-26, *Security Self-Assessment Guide for Information Technology Systems*. ASSET may be used to gather data and generate reports related to the status of the self-assessment. The intent of this tool is to provide a centralized place for the collection of data used to assess a system. ASSET contains the specific control objectives and suggested techniques for measuring the security of a system or group of interconnected systems as described in SP 800-26. The control objectives and techniques are taken from long-standing requirements found in statute, policy and guidance on security.

The reporting features of ASSET are designed to provide users with a clear picture of the security status of their resources, as specified in SP 800-26. ASSET generates a system summary report, which provides a snapshot of assessment results. Unformatted reports can be exported to any popular spreadsheet or charting program. Formatted reports are available for export to Microsoft Excel. The results of the questionnaire can be used as input to a report evaluating an organization-wide IT security program. By sampling completed questionnaires, an agency can determine how well their policies and procedures are being followed and where resources should be expended. A Federal Information Security Management Act of 2002 (FISMA) reporting template has been developed to facilitate the extraction of data from ASSET–Manager to use in FISMA-required reports to the Office of Management and Budget.

The fourth version of ASSET, version 2.0, and new user's manual NIST Interagency Report (IR) 6885, *Automated Security Self-Evaluation Tool User Manual 2004 Edition*, were released in December 2004. The manual is intended to help users of ASSET understand each function of the tool and how the tool can be used to complete self-assessments.

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

ANTI-SPAM TECHNOLOGIES

E-mail is an extremely important and effective means of communication and is used by millions of Americans on a daily basis for personal and commercial purposes. Its convenience and efficiency, however, are increasingly threatened by the rise in the number of unsolicited commercial e-mail messages known as spam. It is generally agreed that spam currently accounts for over half of all e-mails received by Internet service providers' (ISPs') e-mail servers. Today, much of spam appears to contain false or misleading claims. The volume of spam also imposes significant costs on ISPs, businesses, and other organizations, since they can only handle a finite volume of e-mail without making further investments in their infrastructure. Spam also has become a security issue in that it is frequently now used to spread viruses and other malicious code.

As awareness of these new security issues rises, many entities that rely increasingly on the Internet as an important infrastructure are reassessing their responsibilities in dealing with spam, reassessing the risks they face and making changes in how they manage their responses to these security issues. Spam, and particularly phishing, must now be included in the ever-growing list of security issues they must consider when designing and managing their information technology systems.

Because of the international origins and destinations of many spam messages, spam is a global problem that requires international cooperation. As a result, multiple international fora, both public and private, are seeking to address this problem. In recognition of the negative impact of spam, the Organisation for Economic Co-Operation and Development (OECD), a 30-member international governmental organization, created a Task Force on Spam in July 2004. In the past year, Ms. Tanya Brewer has served as a member of this Task Force. The Task Force is a joint effort between the OECD

Committee for Information, Computer and Communications Policy; the OECD Working Party on Information Security and Privacy; and the OECD Committee on Consumer Policy. We have also participated in joint talks between the OECD Task Force, the Asian-Pacific Economic Cooperation (APEC), and the International Telecommunication Union (ITU).

We will continue to participate in broader U.S. government initiatives to combat spam, including finalization of a Toolkit being developed by the OECD Task Force on Spam and a joint meeting regarding spam between the OECD, APEC, and ITU in spring 2006. We will also consider ways we can further assist agencies or conduct relevant, useful research on anti-spam technologies.

http://csrc.nist.gov/spam/
Contacts: Ms. Tanya Brewer
(301) 975-4534
tbrewer@nist.gov

Dr. David Griffith
(301) 975-3512
david.griffith@nist.gov

NEW PROJECTS AND GUIDANCE

The past year has seen many new initiatives in the area of security management. While these efforts have not been larger projects, they nonetheless are important to the Federal agencies that will utilize the outcomes and final products. This report is not meant to be an exhaustive catalog of our work, but these initiatives we thought significant enough to be highlighted.

Revision of the Security Managers' Handbook

We are currently updating NIST Special Publication (SP) 800-12, *An Introduction to Computer Security: The NIST Handbook*, originally published in 1995. The draft Information Security Managers' Handbook provides a broad overview of information security program elements to assist managers in understanding how to establish and implement sound information security programs. It is the organization's responsibility to select and implement appropriate security controls and to demonstrate the effectiveness of satisfying their stated security requirements. A broad understanding of the necessary topics to be addressed in all aspects of information security is discussed throughout this handbook. The topics within the document were selected based on the laws and regulations relevant to information security, including the Clinger-Cohen Act of 1996, the Federal Information Security Management Act of 2002 (FISMA), and 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 a mature 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.

Performance Metrics for Information Security

In the past year, we have begun work on SP 800-80, *Guide to Performance Metrics for Information Security*. This publication is intended to provide to 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. Development and implementation of the metrics contained in this document are aligned with the security control families described in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. The metrics in this publication are not focused on enforcing compliance or measuring implementation of individual controls. The metrics are being discussed in the framework of the SP 800-53 control families because the framework is broad enough to encompass the most commonly named objectives of an information security program. The methodology used to develop the metrics in this guide is contained in NIST SP 800-55, *Security Metrics Guide for Information Technology Systems*. This methodology can be used to develop organization specific metrics that fall outside of the SP 800-53 framework or to customize those discussed herein.

The metrics contained in SP 800-55 focus on implementation of the security controls reported in the FISMA Self-Assessment Checklist. The focus in SP 800-80 is on providing IT security managers the methodology and tools needed to measure how their program complies with mandatory guidance, as well as how well their program is meeting strategic objectives supporting business operation.

Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

In March 2005, we published SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*. This SP summarizes the HIPAA security standards and explains some of the structure and organization of the HIPAA Security Rule. This publication helps to educate readers about information security terms used in the HIPAA Security Rule and to improve understanding of the meaning of the security standards set out in the Security Rule. This publication is also designed to direct readers to helpful information in other NIST publications on individual topics the HIPAA Security Rule addresses. Readers can draw upon these publications for consideration in implementing the Security Rule. This publication is intended as an aid to understanding security concepts discussed in the HIPAA Security Rule, and does not supplement, replace, or supersede the HIPAA Security Rule itself.

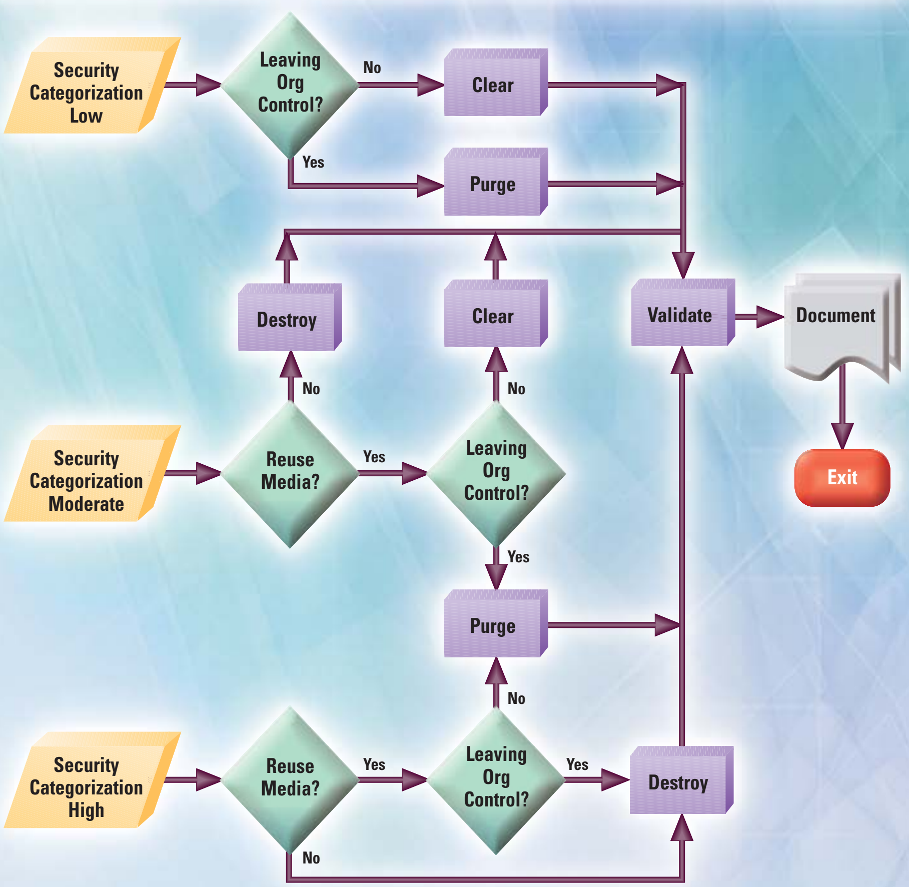
NIST SP 800-66 assists all agencies seeking further information on the security safeguards discussed in the HIPAA Security Rule, regardless of the particular structures, methodologies, and approaches used to address its requirements.

Media Sanitization

When storage media are transferred, become obsolete, or are no longer usable or required by an IT system, it is important to ensure that residual magnetic, optical, or electrical representation of data that has been deleted is not easily recoverable. Sanitization refers to the general process of removing data from storage media, such that there is reasonable assurance, in proportion to the sensitivity of the data, that the data may not be retrieved and reconstructed. Once the media are sanitized, it should be impossible or highly impractical to retrieve the data from those media.

The media sanitization guide—SP 800-88, *Media Sanitization Guide*—will assist organizations and system owners in making practical sanitization decisions based on the level of confidentiality of their information. This publication will also assist organizations in implementing a media sanitization program with proper and applicable techniques and controls for sanitization and disposal based on system categorization.

Media Sanitization Decision Flow Chart



Return on Security Investment

One of our goals is to develop modeling tools for the Federal community to help them select cost-effective strategies to achieve a level of computer security commensurate with the degree of risk and magnitude of likely harm. We are interested in doing some more research work on the subject of Return on Investment for security, and are assembling a meeting to talk to a sample of those in government who participate in the security investment process to gather more resource information, which will be valuable as we continue our analysis.

Contacts:
Ms. Joan Hash (Performance Metrics, HIPAA, ROSI)
(301) 975-5236
joan.hash@nist.gov

Ms. Pauline Bowen (Handbook, HIPAA)
(301) 975-2938
pauline.bowen@nist.gov

Ms. Elizabeth Chew (Performance Metrics, ROSI)
(301) 975-8897
elizabeth.chew@nist.gov

Dr. Alicia Clay (Performance Metrics, ROSI)
(301) 975-3641
alicia.clay@nist.gov

Mr. Arnold Johnson (HIPAA)
(301) 975-3247
arnold.Johnson@nist.gov

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

Mr. Matthew Scholl (Media Sanitization)
(301) 975-2941
matthew.scholl@nist.gov

SECURITY TESTING AND METRICS

STRATEGIC GOAL *The Computer Security Division (CSD) will provide Federal government agencies, industry and the public with a proven set of information technology (IT) security services based upon sound testing methodologies and test metrics. To this end, the CSD will engage in activities to develop, manage and promote security assessment tools, techniques and services, and will support programs for the testing, evaluation and validation of certain IT products. The CSD will also provide guidance to Federal agencies on the use of evaluated and tested products.*

OVERVIEW

Every IT product available makes a claim. 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 that require Federal agencies to use only tested and validated products.

Our testing-focused activities include the validation of cryptographic modules and cryptographic algorithm implementations, accreditation of 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. The 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 Office of Management and Budget, the Social Security Administration, the United States Postal Service, the Department of Veterans Affairs, the Federal Aviation Administration, and the 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.

REACHING OUR GOAL

LABORATORY ACCREDITATION

The goals of this project are to accredit fully-qualified Common Criteria Testing laboratories and Cryptographic Module Testing laboratories and to promote the technical competence of accredited and applicant laboratories. Vendors use independent, National Voluntary Laboratory Accreditation Program (NVLAP) accredited testing laboratories when having their products evaluated. This project develops new methods of proficiency testing for accreditation and periodic re-accreditation of these laboratories, as well as continuous training opportunities for laboratories. Laboratories being accredited leads to consistent evaluation and validations of products for use by Federal government agencies and the private sector. Going through this process also means accredited laboratories are highly qualified.

Currently there are twelve laboratories accredited to perform Cryptographic Module testing, including two in the United Kingdom, two in Canada and one in Germany. Currently there are nine Common Criteria testing laboratories.

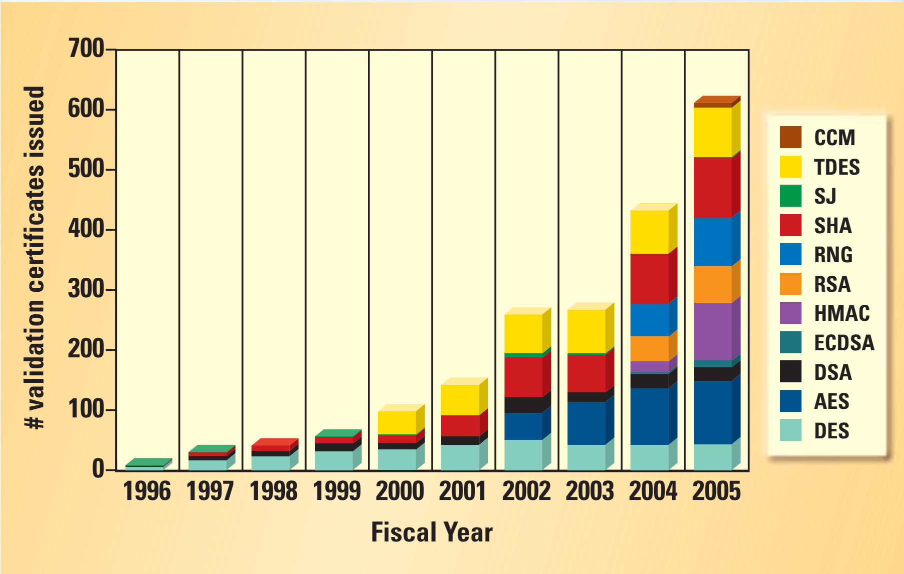
http://ts.nist.gov/ts/htdocs/210/214/214.htm
Contacts: Mr. Jeffrey Horlick
Standards Services Division
(301) 975-4020
jeffrey.horlick@nist.gov

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

CRYPTOGRAPHIC MODULE VALIDATION PROGRAM AND CRYPTOGRAPHIC ALGORITHM VALIDATION PROGRAM

Federal agencies, industry and the public now 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 are used in products and systems to provide security services such as confidentiality, integrity and authentication. Though 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 cryptographic algorithms against established standards is essential to provide security assurance.

The Progress of the CAVP



Vendors of cryptographic modules and algorithms use independent, private-sector testing laboratories accredited as Cryptographic Module Testing (CMT) laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP), to have their cryptographic modules tested by the Cryptographic Module Validation Program (CMVP) and their cryptographic algorithms validated by the Cryptographic Algorithm Validation Program (CAVP). The CMVP and the CAVP are collaborative programs involving NIST's Computer Security Division (CSD) and the Communication Security Establishment (CSE) of the Government of Canada that provide Federal agencies – in the U.S., Canada and the U.K. – 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 validates modules used in a wide variety of products including secure Internet browsers, secure radios, SmartCards, 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 a single or multiple 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 585 certificates have been issued, which represents almost 1,000 validated modules by the CMVP. These modules have been developed by over 125 international vendors. Approximately 110 of these certificates were issued during 2005. Likewise, approximately 1,944 certificates have been issued for validated cryptographic algorithms.

As the worldwide growth and use of cryptographic modules increases, demand to meet the testing needs for both algorithms and modules developed by vendors has also grown. NVLAP has received applications for the accreditation of CMT Laboratories, which has resulted in the accreditation of three new CMT Laboratories in 2005. One of these new laboratories is the first accredited CMT laboratory located in Germany. The other two new accredited CMT laboratories are located in the United States. This brings the current total number of accredited CMT Laboratories to twelve, spanning locations in the United States, Canada, the United Kingdom and Germany. A complete list can be found at: **http://csrc.nist.gov/cryptval/1401labs.htm.**

This fiscal year was the first year the CAVP provided validation testing for the following four algorithms: Random Number Generators (RNGs) (including three different RNGs), the RSA algorithm as specified in ANSI X9.31 (and the two signature schemes with appendix specified in the document PKCS #1 v2.1: RSA Cryptography Standard (June 14, 2002): RSASSA-PSS and RSASSA-PKCS1-v1_5), the Keyed-Hash Message Authentication Code (HMAC), and the Elliptic Curve Digital Signature Algorithm (ECDSA). As a result, there was a 41 percent increase in the number of algorithm validations issued this fiscal year as compared to last fiscal year; the CAVP issued 611 algorithm validation certificates in 2005 compared to 432 certificates issued in 2004.

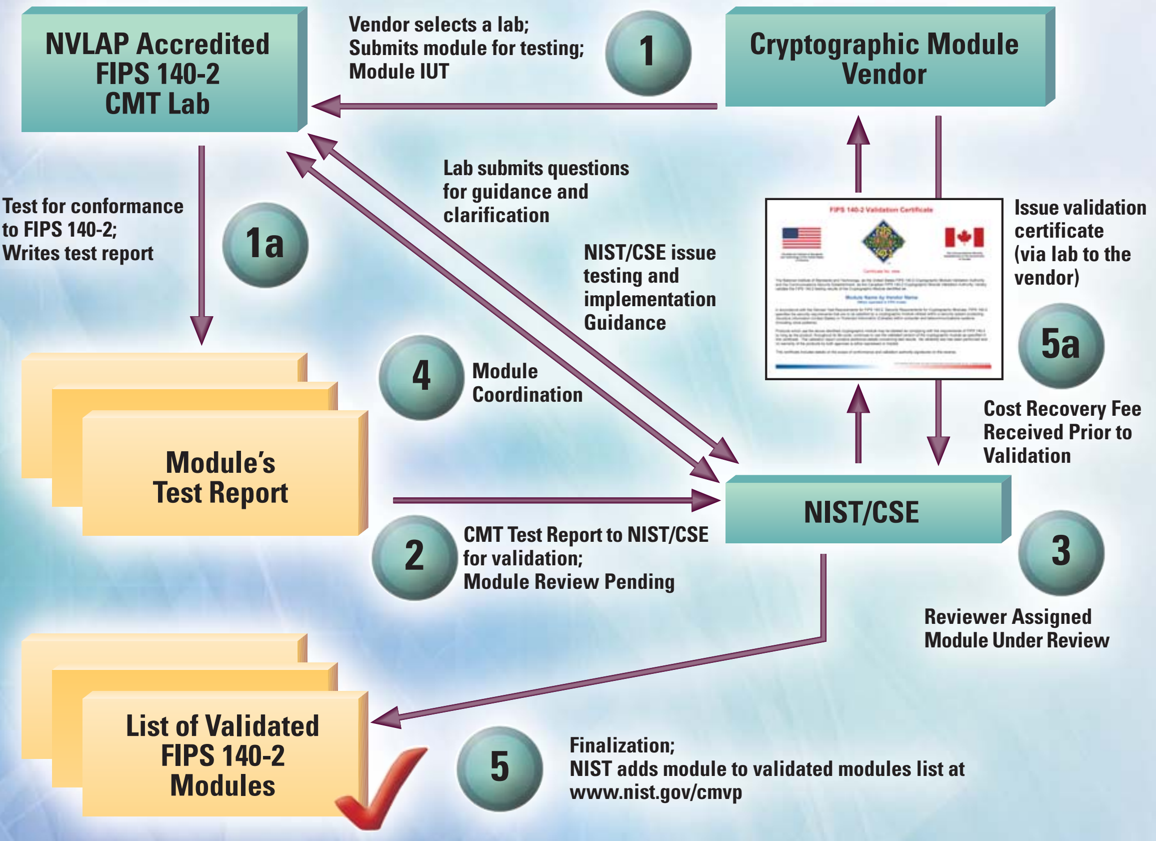
In addition to the above-mentioned cryptographic algorithms, the CAVP has developed a new test suite for the Secure Hash Algorithm-2 (SHA-2) and a new test suite for the CCM (Counter with CBC MAC) algorithm. SHA-2 contains the SHA-224, SHA-256, SHA-384 and SHA-512 sub-algorithms. SHA-1 could only produce a message digest (hash value) of 160 bits, providing no more than 80 bits of security against collision attacks. For the U.S. Advanced Encryption Standard (AES), which uses keys of 128, 192 or 256-bit size, the newer SHA-2 was proposed because it can produce hash sizes of 224, 256, 384 or 512-bits with collision protection levels of 112, 128, 192 and 256-bits respectively. This provides for a better balancing of the security of the hash algorithm with that of the encryption algorithm. The new mode of operation for AES – the CCM algorithm – is a combined confidentiality-authentication mode that was developed for the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard for wireless local area networks (LANs).

Work progressed during 2005 on the establishment of FIPS 140-2 as International Organization of Standardization (ISO) standard 19790. 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). The FDIS (or final draft) version of the draft has been officially issued for balloting with a deadline of December 31, 2005. Also in SC 27, a proposal has been approved for the development of a methodology for cryptographic module testing and evaluation. Mr. Randall Easter will be submitted as a candidate for nomination as an editor of this new project.

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

General Flow of FIPS 140-2 Testing and Validation


NVLAP Accredited FIPS 140-2 CMT Lab
Vendor selects a lab; Submits module for testing; Module IUT
1
Cryptographic Module Vendor
Test for conformance to FIPS 140-2; Writes test report
1a
Lab submits questions for guidance and clarification
NIST/CSE issue testing and implementation Guidance
Issue validation certificate (via lab to the vendor)
FIPS 140-2 Validation Certificate
5a
Cost Recovery Fee Received Prior to Validation
4
Module Coordination
Module's Test Report
NIST/CSE
2
CMT Test Report to NIST/CSE for validation; Module Review Pending
3
Reviewer Assigned Module Under Review
List of Validated FIPS 140-2 Modules
5
Finalization; NIST adds module to validated modules list at www.nist.gov/cmvp

AUTOMATED SECURITY TESTING AND TEST SUITE DEVELOPMENT

Each approved and recommended cryptographic algorithm has an associated reference called a Federal Information Processing Standard (FIPS) or a Special Publication. 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 will 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 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 Cryptographic Algorithm Validation Program (CAVP) encompasses validation testing for FIPS approved and CSD recommended cryptographic algorithms. Cryptographic algorithm validation is a prerequisite to the Cryptographic Module Validation Program (CMVP). The CAVP was established by NIST and the Communications Security Establishment (CSE) of the Government of Canada in July 1995. All of the tests under the CAVP are handled by third-party laboratories that are accredited as Cryptographic Module Testing (CMT) laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP). We develop and maintain a Cryptographic Algorithm Validation System (CAVS) tool which automates the validation testing for FIPS approved and CSD recommended cryptographic algorithms. 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 algorithms (RNG)
- The RSA algorithm
- The Keyed-Hash Message Authentication Code (HMAC)
- The Counter with Cipher Block Chaining-Message Authentication Code (CCM)
- The Elliptic Curve Digital Signature Algorithm (ECDSA).

This fiscal year was the first year the CAVP provided validation testing for the RNG, the RSA (including RSA, RSASSA-PSS, and RSASSA-PKCS1-v1_5), HMAC, ECDSA, SHA-224, SHA-256, SHA-384, SHA-512, and CCM algorithms. As a result, there was a 41 percent increase in the number of algorithm validations issued this fiscal year as compared to last fiscal year; the CAVP issued 611 algorithm validation certificates in FY 2005 compared to 432 certificates issued in FY 2004.

In FY 2006, the CAVP will be adding validation testing for the following algorithms:

- NIST Special Publication 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*
- FIPS PUB 186-3, *Digital Signature Standard (DSS)*—An updated DSS to accommodate for the increased SHA sizes and key sizes
- Draft Special Publication 800-56, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*
- Transport Layer Security (TLS) protocol
- 802.11i protocol.

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

FIPS 140 MAINTENANCE

Every five years, Federal Information Processing Standards (FIPS) are reviewed for currency and relevance. A Federal Register notice was issued in January 2005 soliciting comments regarding FIPS 140-2, *Security Requirements for Cryptographic Modules*, to support the development of the follow on FIPS 140-3. Many comments were received and reviewed. In the area of security and cryptographic module development, technology tends to be fast paced and highly innovative. There have been tremendous advances in technology since the issuance of FIPS 140-2 in May 2001. FIPS 140-3 will address new advances in technological developments, newly emerging security standards and lessons learned during the testing and validation of many modules against FIPS 140-2. Updating this type of document is a very lengthy process, so the work has begun in order to produce FIPS 140-3 before FIPS 140-2 loses its usefulness. The first public draft of FIPS 140-3 should be available in the second quarter of FY 2006. Additional public workshops will be scheduled for the review of the first draft.

In support of the development of the first draft of FIPS 140-3, the CMVP co-hosted a Physical Security Testing Workshop with the Information-Technology Promotion Agency, Japan (IPA), the Information Technology Research and Standardization Center, Japan (INSTAC), and the Japan Standards Association (JSA). Participating in the workshop were invited members of the vendor community who have developed cryptographic modules at the higher levels of physical security, the CMT Laboratories, and leaders in the many areas of physical security, incorporating both invasive and non-invasive attack techniques. Two days of presentations by speakers from the international community followed with two days of discussions on the issues and methods relative to physical security protection.

http://csrc.nist.gov/cryptval/
FIPS 140 Contact: Mr. Randall Easter
(301) 975-4641
randall.easter@nist.gov

RESEARCH ON TECHNICAL SECURITY METRICS

With an ever-growing dependency on information systems, system owners and system users look to answer the question "Is this system secure enough?"

Constantly changing technologies and threats prevent one from saying, "My system is completely secure." Still, there is a need to answer questions such as "How much is enough?"; "Am I closer to my security objectives today than I was yesterday?"; "Is that organization's system secure enough for me to allow an interconnection?" In order to answer these types of questions, metrics that speak to the security of information systems are needed—you can't improve what you cannot measure.

In SP 800-55, *Security Metrics for Information Technology Systems*, we defined security metrics as "Tools designed to facilitate decision-making and improve performance and accountability through data collection, analysis and reporting of relevant performance related data." Since the characteristics of information security are confidentiality, integrity, and availability, one can argue that security metrics may be viewed as standard measures of confidentiality, integrity, and availability. Though simplistically stated, this is a non-trivial concept that speaks to standard measures of system and organizational performance against defined specifications in the three security characteristics. Part of the challenge is gaining consensus on what "secure" means amidst a sea of systems with different functionalities and different missions. Though there is no clean break between system and organizational performance, this effort to develop technical security metrics is focused on the technology upon which the systems are based.

With this in mind, we have begun an effort to better define technical security metrics. We are looking to map the current state-of-the-art, understand the needs and objectives of practitioners asking the question "How secure?", and subsequently, design and implement a research program aimed at advancing knowledge in the field of security metrics. Next fiscal year we will host a workshop to explore these issues with leading researchers and practitioners.

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

SECURITY RESEARCH AND EMERGING TECHNOLOGIES

STRATEGIC GOAL ▸ *The Computer Security Division (CSD) will support and conduct research activities that will enhance information technology (IT) security for Federal agencies in the Executive Branch. The CSD will work to understand and enhance the security utility of new technologies through research. The identification and mitigation of vulnerabilities in IT technologies will be a piece of the research that will be undertaken.*

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 of 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 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 analyses. Our research helps 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 International Business Machines (IBM), Microsoft Corporation, Sun Microsystems, the Boeing Company, Intel Corporation, Lucent Technologies, Oracle Corporation, MITRE, the SANS Institute, the University of Maryland, Ohio State University, the University of Tulsa, George Mason University, Rutgers University, Purdue University, George Washington University, the University of West Florida, the University of California–San Diego, the University of Maryland-Baltimore County, the National Security Agency, the Department of Defense, the U.S. Naval Research Laboratory, the Defense Advanced Research Projects Agency, and the Department of Justice.

REACHING OUR GOAL

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 an almost daily basis and many ready-to-use exploits are widely available on the Internet. Because IT products are often intended for a wide variety of audiences, restrictive security controls are usually not enabled by default 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 yet effective tool is the security configuration checklist.

The goals of this program are—

- To facilitate the development and sharing of security configuration checklists by providing a framework for developers to submit checklists to us
- To assist developers in making checklists that conform to common baseline levels of security
- To assist developers and users by providing guidelines for making checklists better documented and more usable
- To provide a managed process for the review, update and maintenance of checklists
- To provide an easy-to-use repository of checklists.

This program also serves to assist vendors in the process of making their checklists available to users out-of-the-box. In such cases, it will still be advisable for product users to consult the checklist repository for updates to pre-installed checklists.

A security configuration checklist (sometimes called a lockdown, hardening guide, or benchmark) is in its simplest form 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 may be 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 (such as executables, security templates that modify settings, scripts)
- Documentation (for example, a text file) that guides the checklist user to manually configure software
- Documents that explain the recommended methods to securely install and configure a device
- 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 have created various checklists. However, these checklists may vary widely in terms of quality and usability and may have become outdated as software updates and upgrades have been released. Because there is no central checklist repository, they can be difficult to find. They may not be well documented with the result being that one checklist may differ significantly from another in terms of the level of security provided. It may be difficult to determine if the checklist is current, or how the checklist should be implemented. While many existing checklists are of high quality and quite usable, the majority of checklists aren't accessible or directly usable by most audiences.

Although the use of security configuration checklists can greatly improve overall levels of security in organizations, no checklist can make a system or a product 100 percent secure. However, use of checklists that emphasize hardening of systems against flaws or bugs inherent in software will typically result in greater levels of product security and protection from future threats.

We released the final version of Special Publication (SP) 800-70, *Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers* in May 2005. In conjunction with this, we introduced the NIST Beta Checklists repository in May 2005, which contains checklists and descriptions. Users can browse the repository by product category, vendor, and submitting organization to locate a particular checklist. The repository includes over 50 checklists covering database systems, DHCP servers, directory services, DNS servers, firewalls, multi-functional peripherals, network routers, network switches, operating systems, vulnerability management software, Web browsers, and Web servers.

A specific piece of this program has been the development of checklists for Windows operating systems. Since 2004, we have been working on guidance to help better secure Windows XP. SP 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, has been created to assist IT professionals, in particular Windows XP system administrators and information security personnel, in effectively securing Windows XP Professional Service Pack 2 (SP2) systems. The principal goal of the document is 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.

NIST TM
Security Configuration
CHECKLISTS
http://checklists.nist.gov
CSD

SP 800-68 discusses Windows XP and various application security settings in technical detail. The guide provides insight into the threats and security controls that are relevant for various operational environments, such as for a large enterprise or a home office. It describes the need to document, implement, and test security controls, as well as to monitor and maintain systems, on an ongoing basis. It presents an overview of the security components offered by Windows XP, and provides guidance on installing, backing up, and patching Windows XP systems. It discusses security policy configuration, provides an overview of the settings in the accompanying NIST security templates, and discusses how to apply additional security settings that are not included in the NIST security templates. It demonstrates securing popular office productivity applications, Web browsers, e-mail clients, personal firewalls, antivirus software, and spyware detection and removal utilities on Windows XP systems to provide protection against viruses, worms, Trojan horses, and other types of malicious code. This list is not intended to be a complete list of applications to install on Windows XP system, nor does it imply NIST's endorsement of particular commercial off-the-shelf (COTS) products. SP 800-68 will be finalized in November 2005.

This CSD program is in cooperation with checklist development activities at the Defense Information Systems Agency, the National Security Agency and the Center for Internet Security, and is in the process of establishing participation agreements with vendors and other checklist-producing organizations. We gratefully acknowledge sponsorship for this checklist program from the Department of Homeland Security.

http://checklists.nist.gov/
http://csrc.nist.gov/itsec/guidance_WinXP.html
Contacts: Mr. Tim Grance
(301) 975-3359
grance@nist.gov

Mr. Murugiah Souppaya
(301) 975-4758
murugiah.souppaya@nist.gov

SECURITY TECHNICAL IMPLEMENTATION GUIDES AND CHECKLISTS

Security technical implementation guides (STIGs) assist in securing IT products and systems. By using one of these guides, a product or system may be made more secure without an individual having to develop and test settings and specifications. After using a STIG, an accompanying checklist may be used to verify that the guide was correctly applied.

The Defense Information Systems Agency (DISA) issues STIGs and checklists for a variety of information technologies and hosts these on its Web site. Many of these resources deal with classified system requirements, and hence, access is restricted to military and government personnel only. Some of these resources, however, are suitable for non-classified system use. CSD, through an agreement with DISA, houses a repository of the STIGs and checklists that are suitable for non-classified systems so they may be accessed by contractors that handle Federal information systems. These guides and checklists are also available for voluntary adoption by others. DISA is working on having a publicly accessible site available in the near future. We will transition many of the STIGs to our IT Products Checklist Web page and maintain a small repository of STIGs on this site that do not fit the requirements for the checklist Web page.

http://csrc.nist.gov/pcig/cig.html
Contact: Mr. Richard Kissel
(301) 975-5017
richard.kissel@nist.gov

GOVERNMENT SMART CARD PROGRAM: INTERNATIONAL STANDARDS PROGRAM

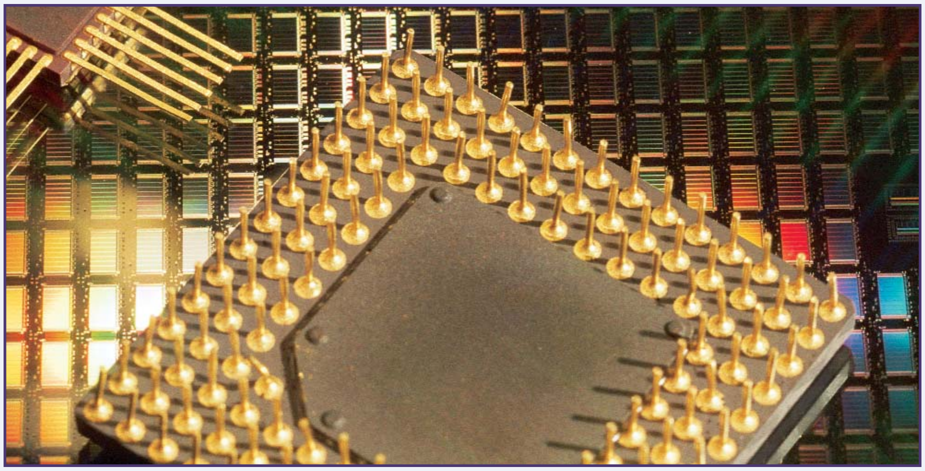
Many Federal agencies are interested in using smart cards because of their intrinsic portability and security. A smart card is able to store and actively process information, in particular, cryptographic keys and algorithms for providing digital signatures and for use with other cryptographic functions.

Our scientists have worked with Federal agencies and industry partners for the past several years to establish a Government Smart Card (GSC) program to facilitate widespread deployment of interoperable smart card systems. The Information Technology Laboratory (ITL) set out to build a framework for smart card interoperability, enabling broad adoption of this critical technology by the public and private sectors. The mechanism and technical foundation for this framework is the Government Smart Card Interoperability Specification (GSC-IS).

The GSC-IS established the framework for smart cards to work in an open environment. It defined an architectural model for interoperable smart card service provider modules, compatible with both file system cards and virtual machine cards, that allows smart card application developers to obtain various services (for example, encryption, authentication, and digital signatures) from GSC-compliant smart cards through a common, interoperable smart card services interface.

The GSC-IS framework and concepts were submitted to the International Organization for Standardization (ISO) for consideration as an international formal standard. The international ballot was approved with overwhelming success and NIST was selected as the convener of a dedicated task force for this new body of work, International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee 1 on Information Technology, Subcommittee 17 on Cards and Personal Identification, Work Group 4 on Integrated Circuit Cards with Contacts, Task Force 9 (ISO/IEC JTC1 SC 17/WG 4/Task Force 9).

The new suite of interoperability standards, ISO/IEC 24727: *Identification Cards – Integrated Circuit Card Programming Interfaces*, is under development in Task Force 9. ISO/IEC 24727 is a three part standard; Part 1 describes the frame-

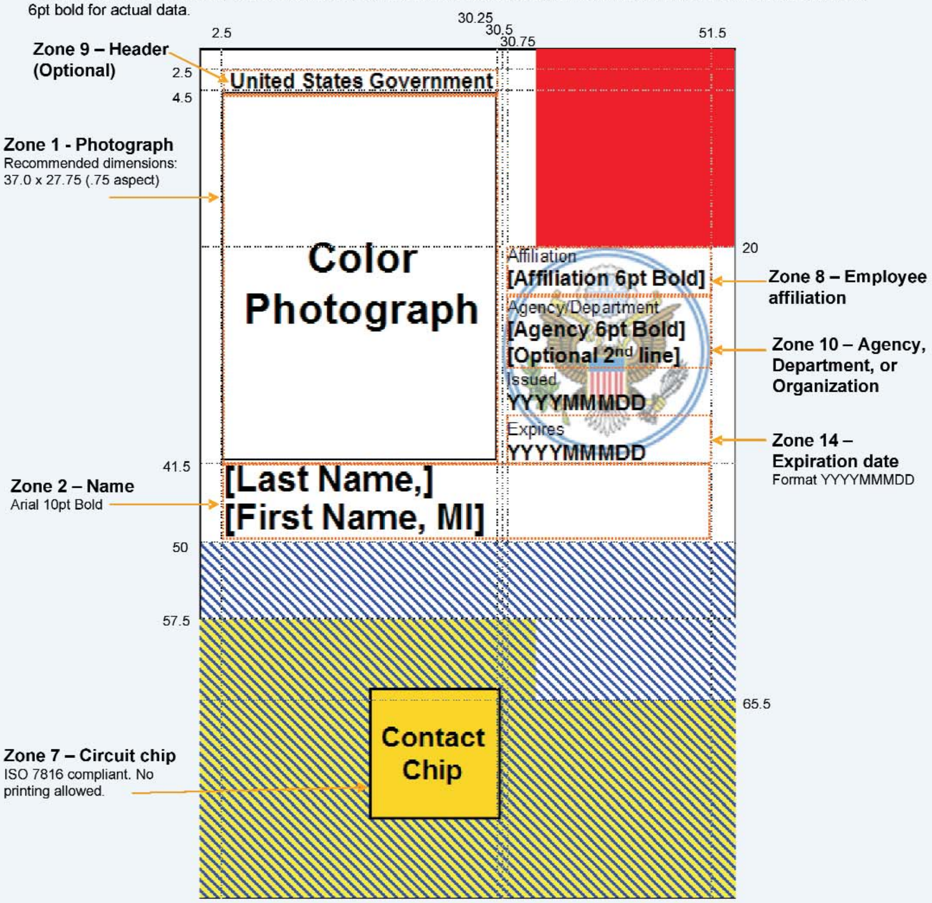


work, Part 2 describes the card-programming interface, and Part 3 describes the application-programming interface. The European Union has acknowledged their intent to use ISO/IEC 24727 for the European Union Citizen Card (EU CC) currently under development. Other countries have made plans to incorporate ISO/IEC 24727 interfaces with on-going smart card based projects. Formal completion of this work is anticipated in early 2007. Part 1 is in final committee draft stage, and Parts 2 and 3 are in committee draft stage. The ISO/IEC 24727 team of project editors was awarded an American National Standards Institute National award for their dedicated efforts.

We continue to champion smart card standardization work at the national and international level. NIST provides the Chair of a national task group under the direction of the InterNational Committee for Information Technology Standards/American National Standards Institute (INCITS/ANSI) B10, which is the U.S. Technical Advisory Group to ISO SC17.

PIV Card Front - Printable Areas

- All measurements around the figure are in millimeters and are from the top-left corner.
- All text is to be printed using the Arial font.
- Unless otherwise specified, the recommended font size is 5pt normal weight for data labels (also referred to as tags) and 6pt bold for actual data.



▨ Area for additional optional data. Agency-specific data may be printed in this area. See other examples for required placement of additional optional data elements. Note: In this example, Zone 9,11, and 13 are optional but shall be placed as depicted and therefore are not in the blue shaded area.

▨ Area likely to be needed by card manufacturer. Optional data may be printed in this area but may be subject to restrictions imposed by card and/or printer manufacturers.

🟥 Reserved area. No printing is permitted in this area unless verified as printable area by card and/or printer manufactuers.

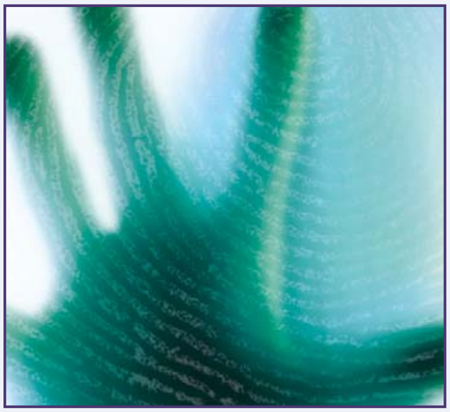
Continued collaboration with the International Aviation Civil Organization (ICAO), the United Nations organization responsible for travel documents, during the development of the next generation passport, which includes contactless technology, will ensure harmonization of selected protocols with U.S. mandates. Close collaboration with CSD's Personal Identity Verification (PIV) Program is maintained to ensure synchronization of policy, standardization, and technical activities of the Federal community as well as to ensure the interoperability and security mandates of Homeland Security Presidential Directive 12 (HSPD-12) are met.

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

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 is employed to authenticate identity, leveraging many different classes of identification identity credentials. For physical access, individual identity has traditionally been authenticated by use of paper credentials, such as driver's licenses and badges. Access to computers and data has traditionally been authenticated through user-selected passwords. More recently, cryptographic mechanisms and biometric techniques have been applied to physical and computer security, replacing or supplementing the traditional credentials. 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.

Homeland Security Presidential Directive 12 (HSPD-12), signed by the President on August 27, 2004, established the requirements for a common standard for identification issued by Federal departments and agencies to Federal employees and contractor employees for gaining physical access to Federally-controlled facilities and logical access to Federally-controlled information systems. HSPD-12 addressed the wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks. Limiting these variations will enhance security, increase government efficiency, reduce identity fraud and protect personal privacy by establishing a mandatory, government-wide standard for secure and reliable forms of identification issued by the Federal government to its employees.

In accordance with HSPD-12, we developed Federal Information Processing Standard (FIPS) 201, *Personal Identity Verification (PIV) for Federal Employees and Contractors*. FIPS 201 was issued in February 2005.

This standard defines the technical requirements for an identity credential that will be—

- Issued based on sound criteria for verifying an individual employee's identity
- Resistant to identity fraud, tampering, counterfeiting and terrorist exploitation
- Rapidly authenticated electronically
- Issued only by providers whose reliability has been established by an official accreditation process
- Applicable to all government organizations and contractors
- Used to grant access to Federally-controlled facilities and information systems
- Flexible enough for agencies to select the appropriate security level for each application by providing graduated criteria from least secure to most secure
- Not applicable to identification associated with national security systems
- Implemented in a manner that protects citizens' privacy.

The FIPS 201 standard establishes requirements for the following processes and the supporting infrastructure—

- Identity Token (ID card) Application by Person—this establishes the requirements for an application for the standardized identification.
- Identity Source Document Request by Organization—every Federal organization is different, but its security needs can be grouped into one of four assurance levels. Depending on which assurance level is needed, a given agency will require specific forms of documentation in order to verify the identity of the potential grantee of the ID Card.
- Identity Registration and ID Card Issuance by Issuer—after a person's legal identity has been authenticated that person needs to be registered with the PIV system and that person's card needs to be issued. The PIV standard provides specifications for this process.
- Access Control (determined by resource owner)—this refers to how users are granted access to Federal resources. The government agencies (resource owner) will determine if the person is granted access based on the security level of the card and the sensitivity level of the resource that is being accessed.
- Life Cycle Management—the information associated with a user's identity is subject to change. The user may change employers, gain new security clearances, leave an agency, or any one of a host of possibilities. This framework will recommend guidelines for managing these changes through the life cycle of both the card and the associated cardholder.

FIPS 201 was divided into two parts. Part 1 addressed the common identification, security, and privacy requirements for issuing organizations. Part 1 is to have been implemented by all Federal departments and agencies by October 27, 2005. Part 2 provided detailed technical specification of components and processes required for interoperability of PIV cards with the personal authentication, access control, and PIV card management systems across the government. The Office of Management and Budget (OMB) has directed that Part 2 be implemented by all Federal departments and agencies by October 27, 2006.

In addition to the FIPS 201 standard, we developed a reference implementation, designated an initial set of conformance test laboratories, and published several implementation guidelines. These guidelines included Special Publication (SP) 800-73, *Interfaces for Personal Identity Verification*; SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*; and SP 800-79, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*.

In the next year, we will complete a revision of FIPS 201 to accommodate policy changes mandated by OMB, provide management oversight of the conformance test program, and update reference implementations. We will also publish additional implementation guidelines—*PIV Middleware and PIV Card Application Conformance Test Guidelines, Codes for the Identification of Federal and Federally-Assisted Organizations*, and *Biometric Data Specification for Personal Identity Verification*.

Future plans include maintenance support activities such as implementation guidance, reference implementation, and conformance testing. Failure to accomplish these follow-on activities may result in a breakdown of interoperability among Federal government identity verification systems. Also, the proper authorities will be unable to validate implementations and upgrades due to the absence of conformance criteria and tests. Agencies may potentially fail to maintain security of their systems due to lack of the standard at other agencies. Some incompatibilities will also arise in Federal implementation of additional applications if the base system is not strong.

http://csrc.nist.gov/piv-program/
Contacts: Mr. Wm. Curt Barker
(301) 975-8443
william.barker@nist.gov

MOBILE AD HOC NETWORK AND WIRELESS SECURITY

The proliferation of wireless devices and the availability of new wireless applications and services raise new privacy and security concerns. Although network-layer anonymity protects the identities of the communication endpoints, the physical layer of many wireless communication protocols offers no such guarantee. The electromagnetic signal transmitted over an open communication medium can be monitored, captured, and analyzed in an effort to trace and identify users of wireless devices. In 2005, our division collaborated with the Boulder Electromagnetics Division to investigate the feasibility of identifying wireless nodes in a network by measuring distinctive electromagnetic characteristics, or "signatures," of Wireless Local Area Network (WLAN). This research was performed in a controlled laboratory environment, and research is under way to evaluate our approach in a real-world setting.

In 2005, our research team released an 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 five international conferences.

As part of a joint research effort with the University of Connecticut, we developed an open source implementation of an electronic coin-based wireless authentication protocol. This electronic coin-based protocol protects the privacy of the wireless user's identity and location, and is compatible with the IEEE 802.11 Extensible Authentication Protocol (EAP). The protocol enables privacy and security for the user and access control and billing for the wireless operator.

In 2006, we will develop a Secure Service Location Protocol (SSLP) for ad hoc networks. SSLP is a framework that allows ad hoc networking applications to advertise, manage, and discover the existence, location, and configuration of networked services. SSLP will allow participants in an open ad hoc network to advertise and discover networked services such as sensor base stations, Internet gateways, certificate authorities, and service directories. Our research group has also begun developing a sensor network test bed for measuring power consumption, memory use, communication cost, and computational power used by resource-constrained sensors. The sensor test bed will be used to measure the performance impact of various security mechanisms being developed for sensor networks. In addition, we are developing open source tools to enable mobile sensor base stations to access security services in hybrid ad hoc networks.

http://csrc.nist.gov/manet
Contacts: Dr. Tom Karygiannis
(301) 975-4728
karygiannis@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 quickly becoming more widespread in use. 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.

Work began during the past year on a new Special Publication (SP) dealing with wireless security issues. This report will provide readers with a detailed explanation of next generation 802.11 wireless security. It will describe the inherently flawed Wired Equivalent Privacy (WEP) and explain 802.11i's 2-step approach (interim and long-term) to providing effective wireless security. It will also include guidance on best practices for establishing secure wireless networks using the emerging Wi-Fi technology, as well as several sample scenarios. This SP will be published in FY 2006.

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

NATIONAL VULNERABILITY DATABASE

In July 2005, we released a new vulnerability management product called 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 approximately 1.5 million times each month 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, you can find all publicly available U.S. government vulnerability resources and references to industry resources. It contains over 13,000 NVD vulnerability summaries with 13 new vulnerabilities added each day.

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)
- 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 300 security products and services to uniquely identify vulnerabilities.

NVD is based on and replaces the NIST ICAT vulnerability meta-base product.

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

AUTHORIZATION MANAGEMENT AND ADVANCED ACCESS CONTROL MODELS

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 on building upon these core features by specifying advanced features to include enforcement of safety invariants, static separation of duty, and multi-state policies (also referred to as history-based 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
- Increased cooperation among organizations through the potential for the coordination, exchange, and interoperability of access control data.

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

REFERENCE IMPLEMENTATIONS FOR AUTOMATED TEST GENERATION TOOLKIT

The automated test generation framework and the associated toolkit were originally applied to develop software code for testing security functions of a commercial database management system (DBMS). The test generation framework uses a model to generate the DBMS areas to be tested and it has been found that this approach provides adequate testing to cover the multiple ways a DBMS can be used as well as to test the functional ability of the systems. This approach could also be used to generate test cases to validate a DBMS's ability to operate with other systems and to confirm other needed functionality of the system.

Based on the above findings, the automated test generation toolkit was utilized to generate conformance tests for testing the interoperability functions of Government Smart Card Interoperability Specification (GSC-IS v2.1). The motivation behind the reference implementation was to determine the feasibility of using the automated test generation toolkit for testing products with complex interfaces as well as to augment tests generated using other approaches. The actual formal verification model used between client application and Smart Card middleware resulted in over 400 requirements that were tested and testing of 390 different ways the system can be used. These tests together with the verification model and middleware access environmental information were used in a test code generator to generate usable software containing 390 tests.

We applied this methodology to generate conformance tests for testing all the interface requirements for Smart Cards to be used across the Federal government for Personal Identity Verification (PIV). We found that the methodology generated good quality tests with sufficient path coverage in a very efficient manner. These interface requirements are specified in SP 800-73, *Integrated Circuit Card for Personal Identity Verification*. The test conditions and test cases that pertain to the generated tests are described in SP 800-85, *PIV Middleware and PIV Card Application Conformance Test Guidelines*.

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

QUANTUM CRYPTOGRAPHY AND INFORMATION SYSTEMS

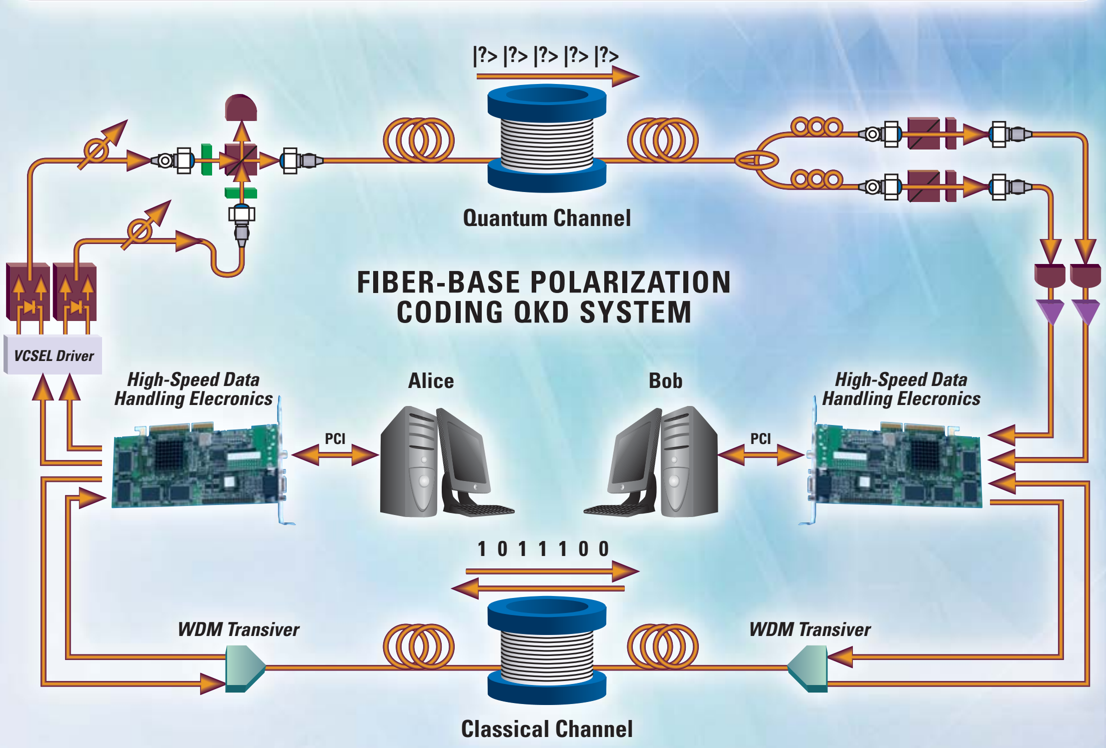
Quantum mechanics, the strange behavior of matter on the atomic scale, provides entirely new and uniquely powerful tools for computing and communications. This field could revolutionize many aspects of computing and secure communications, and could have enormous impacts on homeland security. Whereas 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 nano-seconds 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 particular 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 prop-

Experimental Setup OF NIST fiber QKD system



erties 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 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 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) that 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, they 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 will be published in late 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.

http://math.nist.gov/quantum/
Contacts: Mr. D. Richard Kuhn
(301) 975-3337
kuhn@nist.gov

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

PROTOCOL SECURITY

As the Internet becomes an essential part of day-to-day business and government operations, security, stability, and availability of Internet services are critical issues to the health of our Nation's economy. Expediting the development and deployment of standardized Internet infrastructure protection technologies has been one of ITL's major focus areas in networking, involving the Advanced Network Technologies Division (ANTD) and the Computer Security Division (CSD). We are helping develop public specifications to secure the Internet naming infrastructure through the Domain Name System Security (DNSSEC) project. Another effort is the development of standards for the protection of both content and resources in the Internet routing infrastructure, in particular, the Border Gateway Protocol (BGP). Our work on Internet Protocol Security (IPSec) has also progressed.

Contact: Mr. Tim Grance
(301) 975-3359
grance@nist.gov

DOMAIN NAME SYSTEM SECURITY EXTENSIONS

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) address 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.

There are several distinct classes of threats to the DNS. Most of these are DNS-related instances of more general problems, but a few of these are specific to peculiarities of the DNS protocol. DNSSEC (short for DNS Security Extensions) adds security to the Domain Name System. It is a set of extensions to DNS, which provide (1) origin authentication of DNS data, (2) data integrity, and (3) authenticated denial of existence. DNSSEC was designed to protect the Internet from certain attacks.

We are developing public specifications to secure the Internet naming infrastructure through our DNSSEC project. ITL leads the Internet Engineering Task Force (IETF) DNSSEC editors' team in the completion and progression of all core DNSSEC specifications. We also work with industry and the Department of Homeland Security to expedite the deployment of these new standards.

In 2005, we made further progress in the development of commercial standards and adoption of tools and best practices for securing DNS. As leader of the IETF DNSSEC editors' team, we made the necessary efforts to promote three DNSSEC documents to RFC (Request for Comments) status. We continued our active participation in the U.S. Government DNSSEC Deployment Team. Public comments we received on the draft of Special Publication (SP) 800-81, *Secure Domain Name System Deployment Guide*, were incorporated into a final document. We will be posting this document soon on our Web site. Our paper, "An Integrity Verification Scheme for DNS Zone File Based on Security Impact Analysis," has been accepted for publication in the proceedings of the 21st Annual Computer Security Applications Conference to be held in December 2005.

We have added an online monitoring capability to our Secure Zone Integrity Checker tool. We have also developed tools for DNS traffic capture and replay. Finally, we are coordinating with the General Services Administration (GSA) and associated contractors to finalize plans for securing the **.gov** domain when the maintenance contract is up for renewal. We will work with the contract awardee to facilitate development, procurement and deployment of tools that are required to configure and administer a secure (DNSSEC-based) **.gov** domain.

Contact: Dr. Ramaswamy Chandramouli
(301) 975-5013
chandramouli@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 (ISP).

The BGP project was kicked off in February 2004. The project aims to help industry 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
- Provide deployment and policy guidance for emerging BGP security technologies.

In the past year, we completed 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 will be released to assist industry and government.

The focus of our 2006 activities will be to extend the modeling and analysis tools to incorporate significantly larger and more realistic topologies In fiscal year 2006, 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. D. Richard Kuhn
(301) 975-3337
kuhn@nist.gov

INTERNET PROTOCOL SECURITY

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 is a network-layer control with several components. IPsec has two security protocols—Authentication Header (AH) and Encapsulating Security Payload (ESP). AH can provide integrity protection for packet headers and data. ESP can provide encryption and integrity protection for packets, but cannot protect the outermost IP header, as AH can. The capability for integrity protection was added to the second version of ESP, which is used by most current IPsec implementations; accordingly, the use of AH has significantly declined. 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 can also use the IP Payload Compression Protocol (IPComp) to compress packet payloads before encrypting them.

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.

To expedite the development of this crucial technology, Information Technology Laboratory (ITL) staff designed and developed Cerberus, a reference implementation of the IPsec specifications, and PlutoPlus, a reference implementation of the IKE key negotiation and management specifications. Numerous organizations from all segments of the Internet industry have acquired these implementations as a platform for ongoing research on advanced issues in IPsec technology.

To answer an industry call for more frequent and accessible interoperability testing for emerging commercial implementations of IPsec technology, ITL developed the NIST IPsec WWW-based Interoperability Tester (IPsec-WIT), which is built around the Cerberus and PlutoPlus prototype implementations. IPsec-WIT also serves as an experiment in test system architectures and technologies. The novel use of WWW technology allows IPsec-WIT to provide interoperability testing services anytime and anywhere without requiring any distribution of test system software or relocation of the systems under test. ITL staff also collaborated with key industry representatives to co-author protocol specifications and resolve technical impasses that threatened the progress of the IPsec design and standardization process.

During the past year, we completed Special Publication (SP) 800-77, *Guide to IPsec VPNs*. This document describes the three primary models for VPN architectures: gateway-to-gateway, host-to-gateway and host-to-host. These models can be used, respectively, to connect two secured networks (such as a branch office and headquarters) over the Internet, to protect communications for hosts on unsecured networks (such as traveling employees), or to secure direct communications between two computers that require extra protection.

The guide describes the components of IPsec. It also presents a phased approach to IPsec planning and implementation that can help in achieving successful IPsec deployments. The five phases of the approach are—

- Identify needs
- Design the solution
- Implement and test a prototype
- Deploy the solution, and
- Manage the solution.

Special considerations affecting configuration and deployment are analyzed and three test cases are presented to illustrate the process of planning and implementing IPsec VPNs. SP 800-77 will be published in FY 2006.

http://csrc.nist.gov/ipsec/
Contact: Ms. Sheila Frankel
(301) 975-3297
sheila.frankel@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 SMS (Short Message Service) messaging, Multi-Media Messaging Service (MMS) messaging, IM (Instant Messaging), electronic mail exchange, Web browsing, PIM (Personal Information Management) maintenance (e.g., address book, task list, and calendar schedule), and even the reading, editing, and production of digital documents. When used over time, they 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 Special Publication (SP) 800-72, *Guidelines on PDA Forensics*, intended to provide suggestions on procedures and highlight key principles associated with the handling and examination of electronic evidence contained on PDAs. NIST Interagency Report (IR) 7250, *Cell Phone Forensic Tools: An Overview and Analysis*, is scheduled for release in late 2005. The report gives 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. The NIST IR will be followed by a companion publication entitled *Guidelines on Cell Phone Forensics*.

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.

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

Mr. Richard Ayers
(301) 975-4971
richard.ayers@nist.gov

INTERNET PROTOCOL VERSION 6

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 standard 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 was 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 header, improved mobility and security, and quality of service controls.

The Office of Management and Budget (OMB) has mandated that Government agencies will incorporate IPv6 capability into their backbone (routers, gateways, etc.) by 2008.

We are planning a guidance document on IPv6. 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. We are also planning research on the challenges posed to intrusion detection systems (IDSs) and firewalls by adding IPv6 to the network.

http://csrc.nist.gov/ipsec/
Contacts: Mr. Douglas Montgomery (ANTD)
(301) 975-3630
dougm@nist.gov

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

MOBILE DEVICE SECURITY

Handheld devices such as personal digital assistants are becoming indispensable tools for today's highly mobile workforce. Small and relatively inexpensive, these devices can be used for many functions, including sending and receiving e-mail, storing documents, delivering presentations, and remotely accessing data. Though their small size can be an advantage, it can also be a disadvantage since handheld devices can be easier to misplace or to steal than a desktop or notebook computer. If they do fall into the wrong hands, gaining access to the information they store can be relatively easy.

User authentication is the first line of defense against this threat and an important aspect of mobile device security. We recently issued two reports aimed at making it harder for unauthorized users to access information from these devices through innovations in authentication.

Many organizations have put in place smart card infrastructures for security. However, conventional-size cards, the approximate size of a credit card, require a card reader that can be nearly as large as the handheld device. NIST Interagency Report (IT) 7206, *Smart Cards and Mobile Device Authentication*, describes two types of smart cards that function the same as conventional-size cards, but use standard interfaces supported by handheld devices to eliminate the use of cumbersome readers.

NIST IR 7200, *Proximity Beacons and Mobile Device Authentication*, describes how two different kinds of location-based authentication mechanisms that use signals from wireless beacons can be used to authenticate handheld device users. If the user is in an unauthorized location or a location outside a defined boundary, access will be denied or an additional authentication mechanism must be satisfied before gaining access.

Both reports describe these innovative authentication mechanisms and provide details on their design and implementation.

In earlier work, we devised a general-purpose knowledge-based mechanism for authenticating a user to a mobile device using a visual login technique called Picture Password. The mechanism uses image recall as an easy and natural way for users to authenticate, in lieu of alphanumeric passwords. Features of Picture Password include style dependent image selection, password reuse, and embedded salting, which overcome a number of problems with knowledge-based authentication for handheld devices. More information can be found in NIST IR 7030, *Picture Password: A Visual Login Technique for Mobile Devices*. All of these reports are available in the Publications section of the CSD Web site (CSRC).

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

INDUSTRIAL CONTROL SYSTEMS SECURITY

Industrial control systems (ICS) 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 and DCS systems, which are used in the electric, water, oil and gas, chemical, 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 relays, collecting data from sensor systems, and monitoring the local environment for alarm conditions.

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

Most ICS 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 include basic error detection and correction capabilities, but nothing that guarantees secure communications. The need for cyber security measures within these systems was not anticipated, and, at the time, security for ICS 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 ICS changed to incorporate the latest technologies. Internet-based technologies started making their way into ICS designs in the late 1990s. These changes to ICS 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 SCADA and ICS security, which will be published as NIST Special Publication (SP) 800-82. The purpose of this document is to provide guidance for establishing secure SCADA and other industrial control systems. The document provides an overview of industrial control systems and typical system topologies, identifies typical vulnerabilities and threats to these systems, and provides recommended security countermeasures to mitigate the associated risks. A public draft of SP 800-82 will be available in early 2006 with a final document complete by late 2006. 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 will undergo 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 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 Electronics and Electrical Engineering Laboratory (EEEL). ISD leadership of the PCSRF was recognized with a U.S. Department of Commerce Gold Medal during 2005.

http://www.isd.mel.nist.gov/projects/processcontrol/
Contacts: Mr. Keith Stouffer
Intelligent Systems Division, MEL
(301) 975-3877
keith.stouffer@nist.gov

Mr. Tim Grance
(301) 975-3359
grance@nist.gov

DEDICATED SHORT-RANGE COMMUNICATIONS SECURITY

Dedicated Short Range Communications (DSRC) is a wireless technology that offers the potential to support short to medium range, very high data rate, wireless communications between vehicles, and between vehicles and roadside signs. The goal of this project is to enhance vehicle-based crash prevention performance by using information that could be wirelessly transmitted to vehicles from the roadside and to and from other vehicles. Wireless technologies in vehicles can be used to reduce traffic accidents, resulting in lower direct and indirect financial costs, fewer injuries and fatalities, and reduced traffic congestion. Wireless technologies in vehicle-to-vehicle applications, however, raise a number of serious security concerns. We collaborated with the Department of Transportation and the Vehicular Safety Communication Consortium to define and evaluate the architecture and the security requirements for vehicle-to-vehicle and infrastructure-to-vehicle wireless communication. The Vehicle Safety Communications Consortium (VSCC) consists of seven original equipment manufacturers (OEMs): BMW, DaimlerChrysler, Ford, General Motors, Nissan, Toyota, and Volkswagen. Our efforts included a review of the security architecture, a simulation of network applications in various critical and non-critical scenarios, and the development of a reference implementation of the Vehicular Safety Communication (VSC) Security Protocol.

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

AUTOMATED SOFTWARE TESTING USING COVERING ARRAYS

Software testing is inordinately expensive, typically consuming 50 percent or more of software development budgets. Except for the most critical cases, software products are inadequately tested. One of the main reasons for this is the time and expense for rigorous testing. For example, testing an avionics application with 20,000 lines of code to high assurance levels might require 7 calendar weeks simply to run tests, and much longer to produce test cases. Typical consumer software contains millions of lines of code, so testing to the same level of assurance would require many years, effectively pricing the software out of the market. A recent CSD study of failures in software for medical devices, browsers, servers, and NASA database systems showed that all failures were triggered by interactions among six or fewer input parameters. This suggests that if individual failures involve six or fewer parameters, then test suites designed to exercise from two-way up to six-way interactions will lead to very high confidence that most faults have been found. As a result, techniques and tools for developing test suites that efficiently provide from two-way to six-way coverage could dramatically improve software testing practice, providing better testing at significantly reduced cost. In August 2005, the Information Technology Laboratory (ITL) initiated a new project to incorporate these ideas into prototype testing tools.

The project is using combinatorial mathematics to develop one or more algorithms to produce a test suite with anywhere from two-way to six-way coverage. Algorithms are being implemented in tools for automatic generation of test suites for real-world systems. These are uncharted territories. Some software tools claim to provide multi-way coverage, but they do not seem to work beyond small-scale problems. Generation of complete test cases is also a significant technical challenge. Although test data can be produced easily, tools that can determine the expected result to go with test data are barely out of the laboratory stage. This project is incorporating combinatorial testing algorithms into tools that use formal specifications and model checkers to generate test cases.

ITL researchers are working with faculty from George Mason University and the University of Texas at Arlington. The project team has developed some initial results on optimal test generation strategies, selected two example applications to use in evaluating the prototype, and will begin development of the prototype in fiscal year 2006. During FY 2006, the team will develop the prototype test generator and conduct an experiment on error detection rate for the generated tests using fault injection methods. Theoretical insights on optimal test generation strategies will be further developed and incorporated into tool development as appropriate.

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

Dr. Ramaswamy Chandramouli
(301) 975-5013
chandramouli@nist.gov

Dr. Raghu Kacker (MCSD)
(301) 975-2109
raghu.kacker@nist.gov

Cryptographic Standards and Applications

STRATEGIC GOAL ▸ *The Computer Security Division (CSD) will develop and improve cryptographic methods for protecting the integrity, confidentiality and authenticity of Federal agency information resources in the Executive Branch. We will work to enable government and industry to be able to build secure, interoperable applications with high-assurance products that implement needed cryptographic security functionality. This will include the ongoing development of cryptographic standards and testing methods, developing methods for securing government applications with cryptography, further developing key management guidelines and schemes and the updating and creation of new modes of operation for use with cryptographic algorithms.*

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. In the previous 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 included 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.

This area of work involves collaboration with a number of entities, both from Federal agencies and industry. Some of the Federal agencies include the Department of Treasury, agencies participating in the Federal PKI Steering Committee and Bridge CA Project, the Federal Deposit Insurance Corporation (FDIC), and the National Security Agency (NSA). We have worked recently with the American National Standards Institute's (ANSI's) X9 Committee that develops standards for the financial industry, as well as with the Internet Engineering Task Force's (IETF's) PKIX Working Group. Industry collaborators for these projects have included RSA Security Entrust Technologies, International Business Machines (IBM), Mastercard, Visa, Verizon, VeriSign, and Microsoft Corporation.

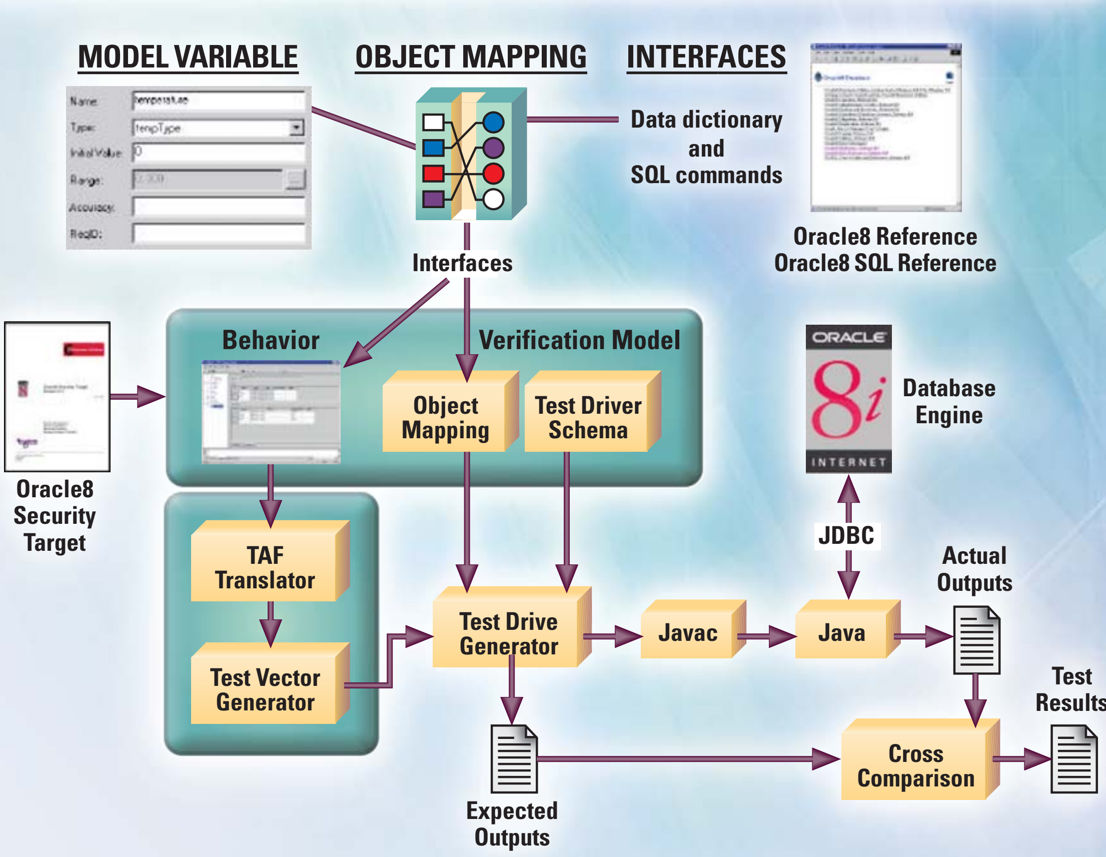
REACHING OUR GOAL

CRYPTOGRAPHIC STANDARDS TOOLKIT

The aim of the Cryptographic Standards Toolkit (CToolkit) project is to enable U.S. governmental agencies and others to select cryptographic security components and functionality for protecting their data, communications, and operations. The CToolkit helps to ensure that there is worldwide government and industry use of strong cryptography and that secure interoperability is achieved through standard algorithms. The CToolkit also provides guidance and education in the use of cryptography. It currently includes a wide variety of cryptographic algorithms and techniques for encryption, authentication, non-repudiation, key establishment and random number generation. The CToolkit is a collection of standards and guidance, and does not include any actual software implementations of the algorithms.

A great deal of work has been made on the CToolkit during FY 2005. Parts 1 and 2 of Special Publication (SP) 800-57, *Recommendation on Key Management*, have been completed; Part 3 will be posted for a public comment period in early 2006. SP 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, has also been completed. NIST SP 800-56, *Recommendation on Key Establishment Schemes*, and a revision of SP 800-21, *Guideline for Implementing Cryptography*, were posted for public comment and will be completed in late 2005. The Data Encryption Standard (DES), which was initially adopted in 1977, was withdrawn as a Federal Information Processing Standard.

Application of TAF-SFT toolkit for DBMS Security Functional Testing



In response to a recently identified vulnerability in a FIPS-approved cryptographic hash algorithm, Secure Hash Algorithm-1 (SHA-1), we are beginning a multi-year effort analyze other currently approved hash functions and develop new hash functions. To initiate the effort, a public Cryptographic Hash Workshop was conducted in the fall of 2005. A second workshop is planned for summer 2006.

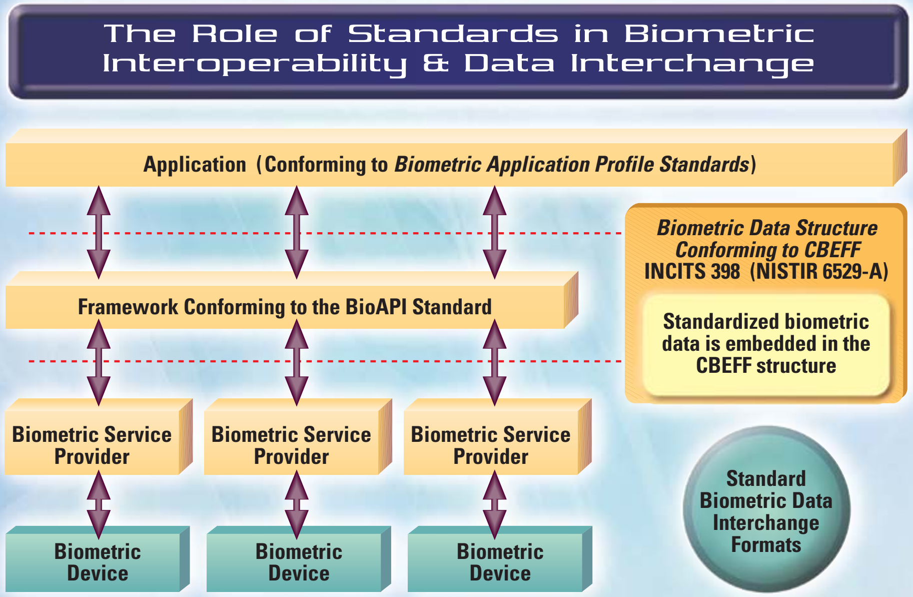
Other plans for 2006 include the completion of a revision of the Digital Signature Standard (DSS), a recommendation for obtaining the required assurances for generating and verifying digital signatures, and a recommendation that specifies Deterministic Random Bit Generators (DRBGs). The DRBG recommendation is one part of the multi-year, multi-part development of a American National Standard for random number generation.

Validation tests were begun at the validation laboratories for compliance with American National Standard Institute (ANSI) X9.31, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*. Validation tests on DES were halted because of the withdrawal of the standard.

http://csrc.nist.gov/CryptoToolkit/index.html
Contact: Ms. Elaine Barker
(301) 975-2911
elaine.barker@nist.gov

BIOMETRIC STANDARDS PROGRAM AND SECURITY

Biometric technologies consist of automated methods of identifying a person or verifying the identity of a person based upon recognition of a physiological or a behavioral characteristic. Consumers need biometric-based high-performance, interoperable (standards-based) systems developed in a timely fashion. In the absence of timely open systems standards developments, migration from proprietary systems to open-systems standard-based solutions is usually more difficult and expensive. Therefore, standards are the cornerstone of our biometrics program. Deploying new information tech-



The Role of Standards in Biometric Interoperability & Data Interchange

Application (Conforming to *Biometric Application Profile Standards*)
Framework Conforming to the BioAPI Standard
Biometric Service Provider
Biometric Service Provider
Biometric Service Provider
Biometric Device
Biometric Device
Biometric Device
Biometric Data Structure Conforming to CBEFF
INCITS 398 (NISTIR 6529-A)
Standardized biometric data is embedded in the CBEFF structure
Standard Biometric Data Interchange Formats

nology systems for homeland security and for preventing ID theft require both national and international consensus standards for biometrics. 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.

These standards and associated conformity assessments need further development in order to help deploy significantly better, open-systems security solutions. We have identified the critical tasks that will help power the development of these standards so that the deployment of such systems may be accelerated. Consequently, 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. 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 the national (INCITS Technical Committee M1 on Biometrics) and the international (ISO/IEC JTC 1/SC 37-Biometrics) biometric standards developments

- Providing expert technical leaders for critical standards projects

- Acting as an advisor to other Federal government agencies, including the Department of Homeland Security (DHS), the National Security Agency (NSA) and the Department of Defense (DoD) Biometric Management Office

- Supporting required administrative infrastructures (for example, the ISO/IEC JTC 1/SC 37 Secretariat)

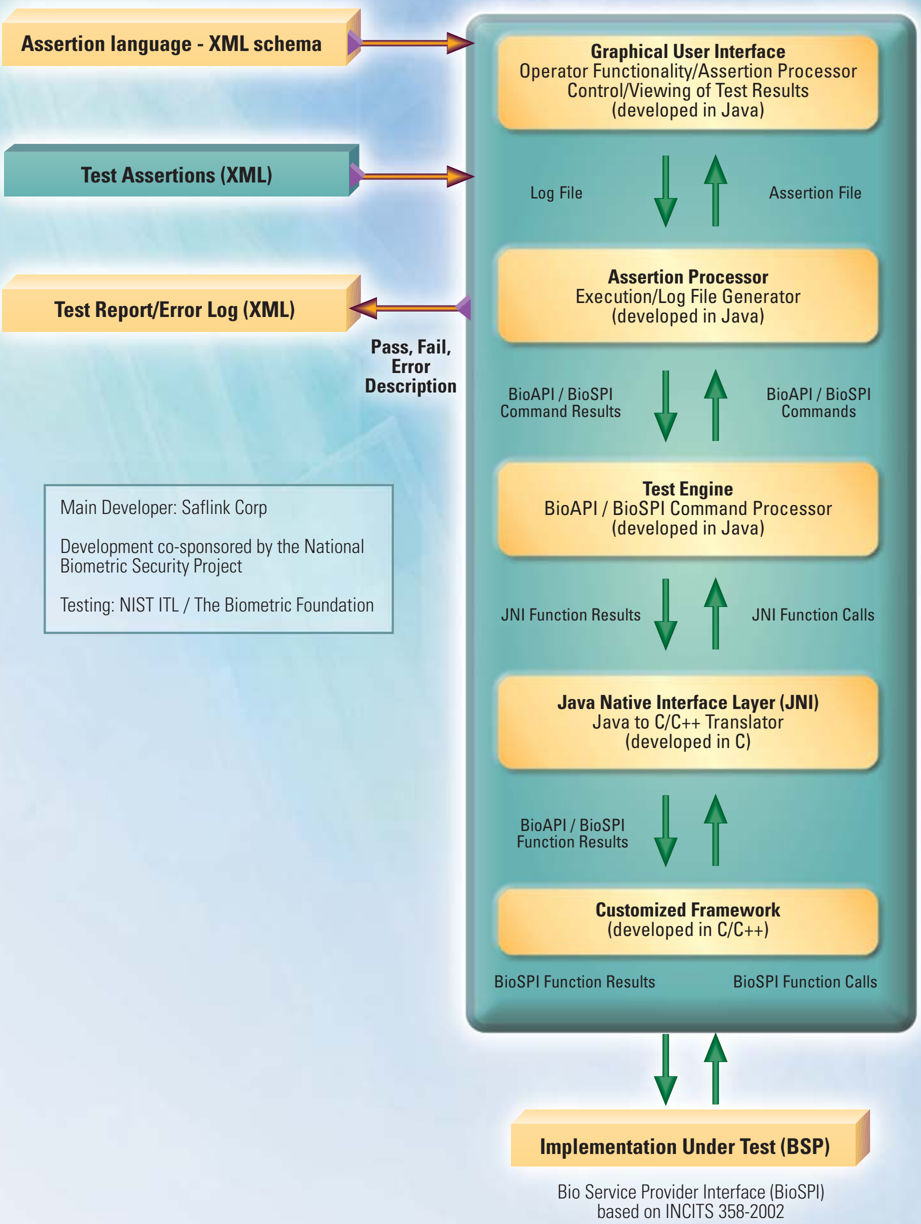
- Working through biometric standards "incubators" (such as the Biometric Consortium and the BioAPI Consortium)

- Promoting fast processing of consortia specifications into national/international standards

- Initiating development of technical implementations and software development for conformity assessment and interoperability tests to Application Profiles as required.

Nationally, NIST's Information Technology Laboratory's (ITL's) biometric standards program helped to establish Technical Committee M1 under the InterNational Committee for Information Technology Standards (INCITS). The purpose of INCITS M1 is to ensure a high-priority, focused and comprehensive approach in the U.S. 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. NIST is an active technical contributor to this standards development body and has sponsored several of their standards development projects. The program experts from CSD work in close collaboration with ITL's Information Access Division's (IAD's) biometric experts. During 2004 and 2005, 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). INCITS M1 is currently developing conformance testing methodology standards for a number of these biometric data interchange formats. In 2005 INCITS M1 completed the development of three parts of a multipart standard that specifies biometric performance testing and reporting. INCITS M1 also approved two biometric application profiles: Verification & Identification of Transportation Workers and Biometric-Based Personal Identification for Border Management. In addition to the development of conformance testing methodologies for biometric data interchange formats, NIST co-sponsored with other INCITS M1 members, the development of a conformance testing methodology standard for the BioAPI specification. INCITS M1 is currently 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 are very active in these standards developments.

NIST ITL BioAPI CTS Architecture


Assertion language - XML schema
Test Assertions (XML)
Test Report/Error Log (XML)
Pass, Fail, Error Description
Graphical User Interface
Operator Functionality/Assertion Processor
Control/Viewing of Test Results
(developed in Java)
Log File
Assertion File
Assertion Processor
Execution/Log File Generator
(developed in Java)
BioAPI / BioSPI Command Results
BioAPI / BioSPI Commands
Test Engine
BioAPI / BioSPI Command Processor
(developed in Java)
JNI Function Results
JNI Function Calls
Java Native Interface Layer (JNI)
Java to C/C++ Translator
(developed in C)
BioAPI / BioSPI Function Results
Customized Framework
(developed in C/C++)
BioSPI Function Results
BioSPI Function Calls
Implementation Under Test (BSP)
Bio Service Provider Interface (BioSPI) based on INCITS 358-2002
Main Developer: Saflink Corp
Development co-sponsored by the National Biometric Security Project
Testing: NIST ITL / The Biometric Foundation

Internationally, we successfully supported the establishment of the International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee 1 Subcommittee 37-Biometrics (ISO/IEC JTC 1/SC 37-Biometrics). INCITS M1 is the national Technical Committee responsible for representing the U.S. in JTC1/SC 37. We provide the chairperson for these two standards bodies and manage their standards programs. We provide the chair of the national standards development efforts on biometric profiles (the Convener of the JTC 1/SC 37 Working Group responsible for the international biometric profile projects is provided by ITL). A large number of the projects within JTC 1 SC 37's program of work were initiated by the U.S. (through INCITS M1). During 2005, JTC 1/SC 37 approved four of these standards. They specify biometric data interchange standard formats for face recognition (face image), finger minutiae, finger image and iris recognition (iris image). ISO published these standards also during 2005. Six additional standards are scheduled to be approved by JTC 1/SC 37 in the first quarter of 2006. 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.

Biometric standards under development in INCITS M1 and JTC 1/SC 37 support interoperability and data interchange. Biometric Service Providers conforming to one of the biometric data interchange formats (any one of the biometric modalities) can develop and interpret a data structure that conforms to one of these standards. A requirement for conformance is embedding the biometric data that conforms to one of the biometric data format interchange standards within a data structure that conforms to CBEFF (Common Biometric Exchange Formats

Framework). BioAPI defines a generic way of interfacing to a broad range of biometric technologies. The data structure defined in BioAPI is an instantiation of CBEFF. BSPs are expected to conform to BioAPI. Applications are expected to conform to BioAPI, CBEFF and one of the biometric profiles under development.

In 2004, the International Civil Aviation Administration (ICAO) adopted a global, harmonized blueprint for the integration of biometric identification information into passports. The biometric requirements include the use of facial recognition as the globally interoperable biometric for travel documents; the use of fingerprint in its several differing technical formulations; and the use of iris as well. ICAO directly adopted the SC 37 standards for its applications. The ICAO community has also committed conformance to and adoption of CBEFF as the data structure for the utilization of biometrics for global interoperability and standardization. ICAO requires conformance to the standards developed by JTC 1/SC 37 for these biometric data interchange standard formats and CBEFF.

The International Labour Office of the United Nations (ILO) has approved Convention 185, which defines a Seafarers Identity Document (SID) containing fingerprint templates in a barcode. In March 2004, the ILO governing body approved a Technical Report that specifies the use of several JTC1/SC 37 draft standards. The specific JTC 1/SC 37 data interchange standards being specified as normative by the ILO are the finger minutiae and finger image data interchange formats. This represents the first time an external agency to ISO has specifically mandated the use of JTC 1/SC 37 standards in an international treaty.

Nationally, in October 2004, DHS adopted the face recognition standard developed by INCITS M1 in order to extract portions of this standard to provide guidelines for specific DHS users including project managers, software and system developers, photographers and subjects, and to develop best practices for producing uniform photographs (posters). In addition, Phase III—Prototype Phase of DHS's Transportation Worker Identification Credential (TWIC) Program (a system-wide common credential to be used for all personnel requiring unescorted physical and/or logical access), includes requirements to the INCITS M1 standards, as applicable, including the Biometric profile—Verification & Identification of Transportation Workers. A sub-pilot of the DHS/TSA registered Traveler Program administered by the Greater Orlando Aviation Authority (GOAA) requires two INCITS M1 interface standards, the BioAPI Specification, and the CBEFF, and some of the biometric data interchange standards developed by INCITS M1. CBEFF was originally published as NIST IR 6529-A under the leadership of CSD experts and the National Security Agency (NSA). Draft Special Publication (SP) 800-76, *Biometric Data Specification for Personal Identity Verification,* requires wrapping the biometric data specified in the draft SP in a CBEFF structure.

We have also participated 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 over 900 members representing over 60 agencies, industry and academe. NIST co-chairs the BC with NSA. The BC sponsors an annual conference, technical workshops and biometrics technical developments. The NIST/BC Biometric Working Group, sponsored by NIST and the BC has been working in the last few years with government users and industry developing biometric specifications. In the past it approved and provided to formal standards bodies three specifications for further processing as national and international standards, including (1) Biometric Data Protection and Usage, (2) Biometric Application Programming Interface for Java Card, and (3) an augmented version of CBEFF. An international version of CBEFF is being developed within JTC 1/SC 37. CBEFF is a requirement for conformance for the national and international data interchange standards under development within INCITS M1 and JTC 1/SC 37.

NIST is also a member of the BioAPI Consortium and its Steering Committee. BioAPI Consortium's membership consists of over 100 organizations, including biometric vendors, end-users, system developers and original equipment manufacturers (OEMs). This consortium developed the BioAPI specification, which was approved as INCITS 358-2002. The BioAPI specification and related standards are under development in JTC 1/SC 37. BioAPI is an International Organization of Standardization (ISO) standard candidate. It is expected to be approved as an ISO standard during the 1st Quarter of 2006.

During 2005 NIST has led an effort to develop an implementation of a conformance testing suite (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, DoD Biometrics Management Office (BMO), 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. The initial CTS implementation was co-sponsored by NBSP and developed by Saflink Corporation. In coordination with NIST/ITL/CSD, DoD BMO has been independently developing a similar implementation of the BioAPI CTS. These test tools are being developed in support of users within Government Agencies already requiring, or interested in requiring in the near future, that Biometric Service Providers (BSPs) conform to the BioAPI standard; the possible establishment of conformity assessment programs to validate conformance to the BioAPI standard and other emerging standards; and product developers interested in developing products conforming to voluntary consensus biometric standards by using the same test tools available to users. NIST and DoD BMO are currently performing intensive testing of the initial versions of these CTSs in order to cross - validate the test results using a number of vendor BSPs claiming conformance to the BioAPI standard before anticipated release of these tools to the public. Our tests are performed in cooperation with experts from The Biometric Foundation (also co-sponsored by NBSP). We are planning to extend conformance test suite development efforts during 2006 in support of other documentary standards and specifications. CTSs to test implementation of biometric data structures conforming to CBEFF are planned.

Mr. Fernando Podio leads the national and international voluntary biometric standards programs.

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

e-AUTHENTICATION

The Office of Management and Budget (OMB) has identified the remote identification of users, or e-authentication, as a crosscutting impediment to the provision of Internet-based government services. To fully realize the benefits of electronic government, government agencies require e-authentication policies and corresponding technical guidance tailored to the protection of government systems and data. This project establishes a policy structure for e-authentication within the U.S. government, promoting consistent implementation of e-authentication across Federal agencies. This consistency will in turn help to enhance government efficiency by securing electronic processes needed to conduct more transactions through e-government applications.

OMB released memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, in December 2003. This OMB policy memorandum defined four levels of authentication – Levels 1 to 4 – in terms of the assurance that an asserted identity is valid. The OMB guidance requires agencies to perform a risk assessment to determine the appropriate authentication level for an application based on the likely consequences of an authentication error. This means a system using Level 4 authentication – a system that allows a user access to more sensitive, personal information for example – has a much higher assurance that a user's identity is what it is claimed it to be. After completing a risk assessment and mapping the identified risks to the required assurance level, OMB guidance directs agencies to identify and implement appropriate authentication mechanisms based on NIST technical guidance.

In 2004, our e-authentication technical guidance was published as SP 800-63, *Recommendation for Electronic Authentication*. This recommendation provides technical guidance to agencies implementing electronic authentication on how to allow an individual person to remotely authenticate his or her identity to a Federal IT system. SP 800-63 states specific technical requirements for each of the four levels of assurance in the areas of identity proofing and registration, tokens, remote authentication mechanisms and assertion mechanisms. It only addresses authentication mechanisms that work by making the individual demonstrate possession and control of a secret, such as a cryptographic key or a password.

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. To meet these challenges, we developed a white paper that defines a generic KBA model and identifies the KBA technical requirements state satisfy OMB assurances Levels 1 and 2. In 2006, we will incorporate this guidance into the SP 800-63. Biometric methods are widely used to authenticate individuals who are physically present at the authentication point, for example, for entry into buildings. Biometrics do not constitute secrets suitable for use in the conventional remote authentication protocols addressed in SP 800-63. In the local authentication case, the claimant uses a capture device controlled by the verifier, so authentication does not require that biometrics be kept secret. In 2005, we held a workshop to examine remote authentication protocols and biometrics. Based on the results of the workshop, CSD, in collaboration with industry, helped 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 will provide a technical report on its findings in 2006.

In this project, we are collaborating with Federal agencies and industry partners. Federal agencies include the Office of Management and Budget, Government Services Administration and the Federal Identity and Credentialing Committee. Industry partners include Financial Service Technology Consortium, Electronic Authentication Partnership, Fidelity, Wells Fargo Bank, Electrosoft, VeriSign and RSA.

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

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

INFRASTRUCTURE AND APPLICATIONS

Individual government agencies implementing electronic authentication techniques would incur prohibitive costs if they were to implement separate techniques for each application instead of an umbrella infrastructure that could span numerous agencies and applications. There is also a burden on the public in interacting with the government by having to maintain multiple credentials and not being able to access the services they need using those credentials. It is clear that a cross-agency interoperable infrastructure approach is a better alternative.

Pursuant to its responsibilities under the Electronic Government Act of 2002, OMB has determined that beginning in fiscal year 2006 Federal agencies that intend to use Public Key Infrastructure (PKI) services will be buying them from qualified managed service providers – Shared Service Providers (SSPs) – operating under the Federal Common Policy Framework rather than establishing their own internal PKI. The Common Policy Framework is a suite of uniform policies developed by us in 2004.

Agencies with PKI operations that are cross-certified with the Federal Bridge Certification Authority will not be required to migrate to these new managed service providers, but as time goes on it may become desirable to migrate to these new providers. This two-step process will result in cost savings to both industry and government; first by insuring that PKI services are developed to meet a common policy, rather than having each agency developing its own idiosyncratic policy, and secondly by having a common contract against which task and delivery orders may be placed by Federal agencies (and other authorized users of the General Services Administration (GSA) Schedules).

We continue to support the development and deployment of the Federal PKI. We provide the vice-chair of the Federal PKI Policy Authority, which manages the suite of Federal PKI Certificate Policies and the operations of the Federal Bridge Certification Authority. We also co-chair the Internet Engineering Task Force (IETF) PKI Working Group and is managing the related Path Validation Testing. These activities advance interoperable infrastructures for all Internet users.

We play a leading role on the Federal Identity Credential Committee's SSP Subcommittee. We provide the technical knowledge and expertise that drive the FICC and the SSP Program. We also provide several members of the SSP Subcommittee and have contributed heavily to the development of the Subcommittee's library of documents.

Potential SSPs must meet the requirements established in the Common Policy Framework and satisfy the Federal certification and accreditation requirements. Vendors of PKI services wishing to be an SSP must meet an objective list of requirements established by the SSP Subcommittee. The SSP Subcommittee used this list of requirements to evaluate vendors' operational procedures, review third-party audits and assess operational compliance demonstrations when establishing the initial list of three approved PKI providers.

CSD, as part of the SSP Subcommittee, has developed the Shared Service Provider Roadmap. The Shared Service Provider Roadmap is intended to identify the background information, phases and activities related to the selection process for prospective PKI managed service providers. This document identifies the process by which a vendor qualifies for inclusion on the Qualified Bidders List. The document also describes requirements that must be met to maintain qualification, as well as contracting considerations.

We are also assisting GSA in the development of an online e-authentication credential validation infrastructure. The GSA e-Authentication Gateway mediates between government applications and non-government CSPs, permitting applications to accept a variety of identification credentials. For example, individuals may be able to leverage authentication mechanisms, such as passwords, established with their banks to access government applications. The GSA E-Authentication Gateway architecture relies on SAML, TLS, and PKI to exchange authentication information with CSPs and government applications. CSD assisted GSA by developing PKI architecture and PKI policies supporting TLS-protected transmission of authentication information between the E-Authentication Gateway, CSPs and government applications.

We are collaborating with many entities, including the Army Corps of Engineers, Federal PKI Policy Authority, GSA, the U.S. Department of Agriculture (USDA), the National Finance Center, the Department of Defense, the Office of Management and Budget, the Department of Treasury, the Department of Energy, the Department of Homeland Security, Cybertrust, Entrust, Identrus, Microsoft, Orion, VeriSign, the States of Illinois and Washington, and EduCause, which includes 1,800 universities, colleges and educational institutions.

Contacts: Mr. Wm. Tim Polk
(301) 975-3348
william.polk@nist.gov

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

VOTING SYSTEM STANDARD DEVELOPMENT

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 the National Institute of Standards and Technology (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). We support the activities of the EAC, TGDC, and STS related to voting equipment security.

In the past year, the Voluntary Voting System Guidelines (VVSG) were updated with new sections covering secure software distribution, setup validation, voter verified paper audit trail (VVPAT), and secure use of wireless technology. The concept of Independent Dual Verification (IDV) was introduced in the updated VVSG where the objective is the production of ballot records whose correctness can be audited to very high levels of precision.

Plans for 2006 include holding a threat analysis workshop for voting systems, hosting the TGDC plenary meetings, supporting STS activities, working with the EAC and TGDC to substantially revise and restructure the VVSG, engaging the voting system vendor, state election official, and academic communities to explore ways to increase voting system security and transparency.

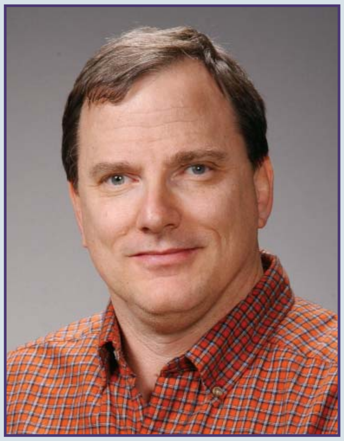
http://vote.nist.gov/
Contact: Dr. Nelson Hastings
(301) 975-5237
nelson.hastings@nist.gov

HONORS AND AWARDS

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY BRONZE MEDAL FOR SUPERIOR FEDERAL SERVICE

The Bronze Medal Award is the highest honorary recognition available for Institute presentation. The award, approved by the Director, recognizes work that has resulted in more effective and efficient management systems as well as the demonstration of unusual initiative or creative ability in the development and improvement of methods and procedures. It also is given for significant contribution affecting major programs, scientific accomplishment within the Institute, and superior performance of assigned tasks for at least five consecutive years.

Mr. Timothy Grance and **Ms. Joan Hash** are recognized for their efforts in providing standards and guidelines in support of Federal Information Security Programs and improving the management and technical processes that are essential to successful information security program implementation. Their work has been key in advancing overall security management and implementation strategy government-wide, nationally, and internationally, resulting in increased protection of information assets and supporting information technology infrastructures needed to provide critical public service.



THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS HARADEN PRATT AWARD 2005

The IEEE Haraden Pratt Award was established in 1971 in honor of Haraden Pratt, who was Director Emeritus of the IEEE and who had given dedicated and distinguished service to the Institute. As President, Treasurer, and then Secretary for 23 consecutive years, his service on the Board of Directors, including that of Director Emeritus, totaled 31 years. The purpose of this award is to recognize individuals who have rendered outstanding service to the Institute.

Mr. Daniel R. Benigni has made significant contributions toward shaping today's IEEE. He is a selfless volunteer and passionate supporter of the organization, demonstrated by the critical roles he has served on more than 25 committees and boards, including the IEEE Board of Directors, Executive Committee, Regional Activities Board, IEEE-USA Board, and Publication Services and Products Board. He was instrumental in transforming the U.S. Activities Board into the IEEE-USA.

As general chairman of the IEEE 2002 Section Congress in Washington, D.C., he helped to influence the IEEE Foundation's financial support for the well-received core leadership educational program. He also created the operating and finance committees of the Regional Activities Board, thus establishing clear responsibilities in these areas.

DEPARTMENT OF COMMERCE CHIEF INFORMATION OFFICER BRONZE MEDAL

This award is the highest honorary award granted by the Chief Information Officer for superior performance characterized by outstanding or significant contributions that have increased the efficiency and effectiveness of the management of information technology within the Department. To warrant a Bronze Medal, a contribution must focus on qualitative and quantitative performance measures reflected in the Department's Strategic Plan.

Representing NIST, **Mr. Daniel Benigni** served as a member and contributed significantly to the Department’s Capital Planning and Investment Control Leadership Group and its efforts to develop and implement processes and policies to make the Department of Commerce a leader in Government in managing information technology capital investments. The Group successfully implemented increasingly rigorous Office of Management and Budget requirements while developing and institutionalizing processes and policies directly supporting the President’s Management Agenda goals on managing information technology capital investments.

COMPUTER SECURITY DIVISION PUBLICATIONS – 2005

NIST SPECIAL PUBLICATIONS

SP 800-79	Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations	July 2005
SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identity Verification	April 2005
SP 800-72	Guidelines on PDA Forensics	November 2004
SP 800-70	Security Configuration Checklists Program for IT Products	May 2005
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule	March 2005
SP 800-65	Integrating Security into the Capital Planning and Investment Control Process	January 2005
SP 800-58	Security Considerations for Voice Over IP Systems	January 2005
SP 800-53	Security Controls for Federal Information Systems	February 2005
SP 800-52	Guidelines on the Selection and Use of Transport Layer Security	June 2005
SP 800-38B	Recommendation for Block Cipher Modes of Operation: The RMAC Authentication Mode	May 2005

NIST DRAFT SPECIAL PUBLICATIONS

SP 800-87	Codes for the Identification of Federal and Federally-Assisted Organizations	August 2005
SP 800-86	Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response	August 2005
SP 800-85	PIV Middleware and PIV Card Application Conformance Test Guidelines	August 2005
SP 800-84	Guide to Single-Organization IT Exercises	August 2005
SP 800-83	Guide to Malware Incident Prevention and Handling	August 2005
SP 800-81	Secure Domain Name System (DNS) Deployment Guide	August 2005
SP 800-77	Guide to IPsec VPNs	January 2005
SP 800-76	Biometric Data Specification for Personal Identity Verification	January 2005
SP 800-73	Integrated Circuit Card for Personal Identification Verification	November 2005
SP 800-57	Recommendation on Key Management	April 2005
SP 800-56	Recommendation on Key Establishment Schemes	July 2005
SP 800-53A	Guide for Assessing the Security Controls in Federal Information Systems	July 2005

FEDERAL INFORMATION PROCESSING STANDARDS

FIPS 201	Personal Identity Verification for Federal Employees and Contractors	February 2005
FIPS 200	Minimum Security Requirements for Federal Information and Information Systems	Draft

NIST INTERAGENCY REPORTS

NIST IR 7219	Computer Security Division – 2004 Annual Report	April 2005
NIST IR 7206	Smart Cards and Mobile Device Authentication: An Overview and Implementation	July 2005
NIST IR 7200	Proximity Beacons and Mobile Handheld Devices: Overview and Implementation	June 2005
NIST IR 7224	4th Annual PKI R&D Workshop: Multiple Paths to Trust—Proceedings	August 2005

INFORMATION TECHNOLOGY LABORATORY BULLETINS WRITTEN BY THE CSD

September 2005	Biometric Technologies: Helping to Protect Information and Automated Transactions in Information Technology Systems
August 2005	Implementation of FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors
July 2005	Protecting Sensitive Information that is Transmitted Across Networks: NIST Guidance for Selecting and Using Transport Layer Security Implementations
June 2005	NIST's Security Configuration Checklists Program for IT Products
May 2005	Recommended Security Controls for Federal Information Systems: Guidance for Selecting Cost-Effective Controls Using a Risk-Based Process
April 2005	Implementing The Health Insurance Portability and Accountability Act (HIPAA) Security Rule
March 2005	Personal Identity Verification (PIV) of Federal Employees and Contractors: Federal Information Processing Standard (FIPS) 201
January 2005	Integrating IT Security into the Capital Planning and Investment Control Process
November 2004	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
October 2004	Securing Voice Over Internet Protocol (IP) Networks

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 Ms. Joan Hash, (301) 975-5236, joan.hash@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 Ms. Joan Hash, (301) 975-5236, joan.hash@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, academic 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 two 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.

Tanya Brewer, *Editor*
Matthew Scholl, *Editor*

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

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

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

NIST IR 7285
February 2006

Disclaimer: Any mention of commercial products is for information only; it does not imply NIST recommendation or endorsement, nor does it imply that the products mentioned are necessarily the best available for the purpose.

Michael James, *Design/Production*
The DesignPond

SECURITY
mail
e
Verification
AUTHORIZATION
SYSTEMS
FINAN