

Computer Security Division



Annual
Report



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

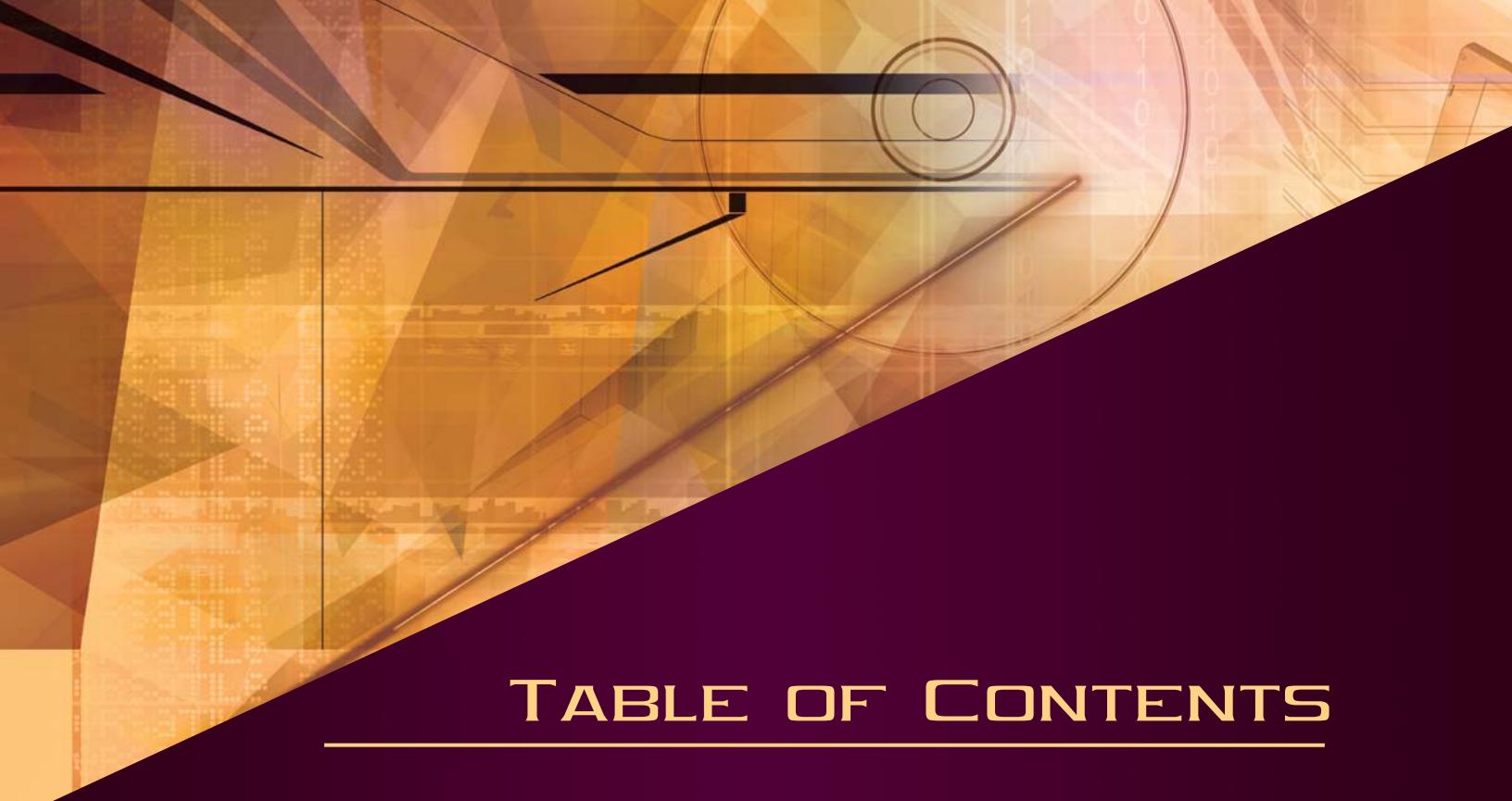


TABLE OF CONTENTS

Welcome Letter	1
Division Organization	2
The Computer Security Division Responds to the Federal Information Security Management Act of 2002	3
Outreach, Awareness and Education	4
Security Management and Guidance	9
Security Testing and Metrics	20
Security Research and Emerging Technologies	23
Cryptographic Standards and Applications	39
Honors and Awards	44
Computer Security Division Publications – 2004	46
Ways to Engage Our Division and NIST	48

Welcome

This year can best be characterized as one of significant challenges. Advances in technology further supported reduced paperwork, streamlined processes, improved control of assets, better communications, more accurately verified identity, more appropriate control of access to information and improved government-business-consumer-taxpayer interchange. New and increasingly complex security concerns accompanied these benefits. The Computer Security Division played a key role in addressing these issues.

Among the highlights of our work in 2004 was a challenge from the President, issued in Homeland Security Presidential Directive #12, to develop a new standard for identification and verification of Federal employees and contractors. We continued making progress in fulfilling the mandates of the Federal Information Security Management Act of 2002 which resulted in Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, and NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*. In addressing the President's challenge, we drew heavily upon our ongoing smart card, biometric and cryptographic work. As such, we made great strides towards a framework for protecting Federal facilities, systems and the employees who have access to them. The long-term benefit of using FIPS 199, SP 800-53 and a standards-based approach to system security in general is more targeted, cost-effective, consistent and improved security.

While the interconnection of information systems often increases the risk to an organization's operations and assets, FIPS 199 and our associated suite of standards and guidelines provide a common way to express information security requirements. This in turn promotes greater consistency across diverse organizations in managing risks.

Scientists in the Computer Security Division have been working with our partners for the past several years to establish a Government Smart Card (GSC) program to facilitate widespread deployment of interoperable smart card systems. In recognition of this work, the NIST Smart Card Team received the Department of Commerce's 2004 Gold Medal Award for the development of a framework and specification that dramatically advanced interoperability among smart card applications, coalesced U.S. government requirements and forged alliances with the world's foremost authorities on smart cards.

The Division has had many other accomplishments this past year, including advancing development of our cryptographic standards toolkit, further e-authentication work, expansion of our Cryptographic Module Validation Program, development of an IT product security configuration checklist program and more work with digital forensics tools and methods. We have begun new work, as well as continuing previous work, on several key Internet security protocols – IPSec, BGP and DNSSEC. We have also provided technical expertise to several U.S. government groups on the security implications of spam e-mail and phishing attacks.

These are just some of the highlights of our work this year. We invite you to read more about our work – and to work with us – as we address these and future challenges. Our extraordinarily talented and knowledgeable experts are recognized as leaders in their fields. Many have come to us from the private sector and other agencies, bringing with them a diverse set of perspectives and expertise and a solid commitment to public service. We are proud to highlight their achievements in this report and to note the honors and awards that were received this year celebrating their achievements.

As you browse this report of the Division's activities for 2004, we hope you will want to learn more. We invite you to visit the CSRC Web site, <http://csrc.nist.gov>, or to contact any of the Division experts noted in this report.

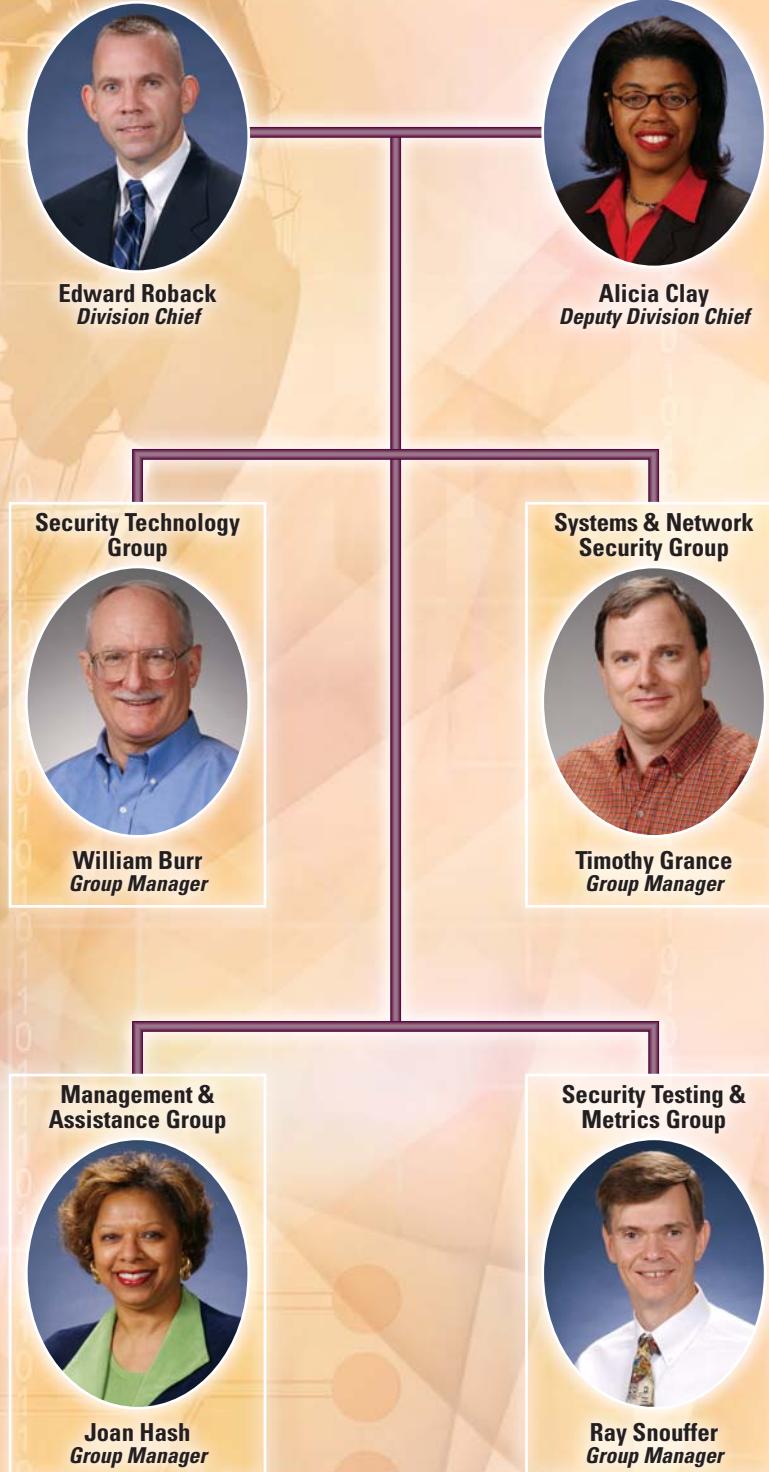
Edward Roback
Division Chief



Alicia A. Clay
Deputy Division Chief



Division Organization



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

The E-Government Act (Public Law 107-347) passed by the 107th Congress and signed into law by the President in December 2002 recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act of 2002 (FISMA), included duties and responsibilities for the Computer Security Division in Section 303 "National Institute of Standards and Technology." In 2004, we addressed these assignments as follows:

- ◆ **Standards to be used by Federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels** – Developed Special Publication (SP) 800-37, *Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems* (final version issued May 2004)
- ◆ **Guidelines recommending the types of information and information systems to be included in each category** – Developed and issued FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* (final version issued February 2004)
- ◆ **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* (first public draft issued October 2003), and continued work on SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (first public draft to be issued January 2005)
- ◆ **Incident detection and handling guidelines** – Developed SP 800-61, *Computer Security Incident Handling Guide* (final version issued January 2004)
- ◆ **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 reimbursable 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. CSD, in conjunction with the Government of Canada's Communications Security Establishment, also 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.
- ◆ **Identification of national security systems guidelines** – Developed SP 800-59, *Guideline for Identifying an Information System as a National Security System* (final version issued August 2003)
- ◆ **Solicit recommendations of the Information Security and Privacy Advisory Board on draft standards and guidelines** – Solicit recommendations of the Board regularly at quarterly meetings
- ◆ **Annual NIST reporting requirement** – Produce an annual report as a NIST Interagency Report (IR). The 2003 Annual Report was issued as NIST IR 7111 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

The CSD provides IT security standards and guidelines to Federal government agencies in the Executive Branch. One of our constant challenges is to provide useful and timely materials to these agencies. When developing and producing our products, we engage in consensus-building with the IT industry, academia and Federal agencies in order to keep the quality of these products and services as high as possible. As part of this consensus-building process, every Federal Information Processing Standard (FIPS) and Special Publication (SP) produced by the CSD 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, the CSD provides materials, information and services useful from the Federal agency level to the home-user level.

The Division houses 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. The Division also hosts several organizations that address specific portions of government and industry. These organizations are discussed in greater detail later in this report.

In 2004, CSD greatly expanded its outreach efforts with the private sector, especially the healthcare community. We formed new coalitions to support small business outreach, made significant enhancements to the Computer Security Resource Center (CSRC) and continued utilizing the Security Managers Forum 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 2005, 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 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 CSD's 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 at the December 2003 meeting (l to r): Sallie McDonald, Elaine Frye, Rebecca Leng, Leslie Reis, Morris Hymes, Howard Schmidt, Steven Lipner, Charisse Castagnoli, Marilyn Bruneau, John Sabo, Susan Landau, Richard Guida, Joan Hash, Franklin Reeder, and Bruce Brody.

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, the civil service, the 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 (two Board members are attorneys), 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 reviews of proposed standards and guidelines developed by NIST
- ◆ 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.

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 report issued in June 2004, "The National Institute for [sic] Standards and Technology Computer Security Division: The Case for Adequate Funding." This paper reflects the results of a year-long review by the Board with input from government and industry. One of the main findings of the paper:

"While funding for the CSD program in real terms has grown modestly over time, it has not kept pace with the growing demand for cyber security guidelines and standards as a result of the government's and the nation's growing reliance of information technology, the growth and diversity of the technologies on which we have come to depend, and the increased threat both from acts of negligence and inadvertence and from those who seek to disrupt or disable the nation's vital systems."

The paper is publicly available at <http://csrc.nist.gov/ispab/board-recommendations.html>.

The Board also expressed its findings and recommendations to the Director of the Office of Management and Budget on the issue of agencies using Web-based transactions to provide e-government services to members of the public.

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 Accountability Office's (GAO's) Report on the Privacy Act, an overview of the Department of Veterans Affairs' (VA's) cyber security program, privacy challenges being faced by the Department of Homeland Security (DHS), updates on the review being conducted of the National Information Assurance Partnership, results of the first Privacy Trust Survey of the U.S. government, customer relations management in the U.S. Postal Service (USPS), specifications and implementations of the Trusted Computing Group's Secure Platform and security issues with voice over IP (VoIP).

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, insuring the authenticity of government Web sites, NIST's outreach and partnering approach and cyber security leadership in the Executive Branch.

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

Ms. Elaine Frye
(301) 975-2819
elaine.frye@nist.gov

FEDERAL INFORMATION SYSTEMS SECURITY EDUCATORS ASSOCIATION

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

Membership is open to information systems security professionals, trainers, educators and managers who are responsible for information systems security training programs in Federal agencies, as well as contractors of these agencies and faculty members of accredited educational institutions. There are no membership fees for FISSEA; all that is required is a willingness to share products, information and experiences. Business is administered by a twelve-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. There is also a contest for computer 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. CSD assists FISSEA with its operations by providing staff support for several of its activities and by being FISSEA's host agency.

FISSEA membership in 2004 spanned Federal agencies, industry, military, contractors, state governments, academia, the press and foreign organizations to reach 1083 members in a total of fourteen countries. The 635 Federal agency members represent 88 agencies from the Executive and Congressional Branches of government. The Educator of the Year Award for 2003 was presented to Jeff Recor, Walsh College, at the FISSEA Annual Conference in March 2004.

FISSEA hosted its second free workshop, "Developing Role-Based Training and Classroom



FISSEA Board Members for 2004-05 – Pictured left to right: Jeffrey Seeman (NSA), Peggy Himes (NIST), Louis Numkin (NRC), Barbara Cuffie (retired SSA), Mary Ann Strawn (LOC, back), Tanetta Isler (HUD) and Lewis Baskerville (SBA). Not pictured: LTC Curt Carver (USMA), Thomas Foss (UNC), Gretchen Morris (NASA), LTC Will Suchan (USMA), Marvelle Towns (NSA) and Mark Wilson (NIST).

Demonstrations," in May 2004. The workshop was presented by the U.S. Department of State's Diplomatic Security Training Center for Information Assurance training team. Attendees were invited to participate in this interactive workshop on the process of designing information assurance training programs to meet Federal guidelines. The workshop began with an overview of the NIST Special Publication (SP) 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*. Next, discussion provided attendees with an overview of three primary information assurance (IA) training categories: Management Controls, Operational Controls and Technical Controls. Based on these categories, attendees generated a list of topics, learning objectives, presentation modes, learning activities and learning measurement strategies for three specific IA roles – Managers, System Administrators and Information System Security Officers (ISSOs). This gave the attendees realistic training that would transfer to their agency's awareness and training program.

FISSEA will also be holding several free workshops during late 2004 and early 2005 to assist Federal employees in gaining a better understanding of how to implement NIST SP 800-16 in their agencies. These workshops will be conducted by Mark Wilson, editor of SP 800-16 and a FISSEA Executive Board Member.

The 2005 FISSEA Conference will be held in March 2005 at the Bethesda North Marriott Hotel and Conference Center in Bethesda, Maryland. This two-day two-track conference will provide an excellent opportunity to network with other security professionals. Further information regarding the conference is available on the FISSEA Web site.

<http://csrc.nist.gov/fisseal/>
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. The CSD uses 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 information. It serves as a vital link to the various groups we wish to reach.

In the last year the CSRC had over 26.1 million requests – an average of over 2.1 million requests per month. Every document released for public comment or published through the Division has been posted to the CSRC. In the summer of 2003 CSD conducted an evaluation and analysis project of CSRC in order to allow the Division to deal with issues of scale, organization and volume. The past year has seen a great deal of work to make the changes and improvements identified in the evaluation and analysis report. The site has been streamlined and simplified to make items easier to find and an extensive site map has been developed.

The CSRC will continue to grow and be updated in 2005. There is a survey under way in order to obtain 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.

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

Mr. Patrick O'Reilly
(301) 975-4751
patrick.oreilly@nist.gov Ms. Elaine Frye
(301) 975-2819
elaine.frye@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 other than the owner and employees of that business. However, over 95 percent of all U.S. businesses – over 20 million – 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 organizations is to identify needed security mechanisms and training that are practical and cost-effective. Such organizations also need to become more educated consumers 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 IT security for small businesses. The purpose of the meetings is to have individuals knowledgeable in IT 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 third 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 first year we were invited to conduct a conference presentation detailing the program and it was received very well with a large number of attendees.

In 2005 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 determine new avenues for this outreach project.

A CSD representative will attend planning meetings hosted by the State Department's office on the Asia-Pacific Economic Cooperation (APEC). A focus of these meetings is an information security education outreach for SMBs to be held during APEC's Spring 2005 meeting in Lima, Peru. Others attending these working meetings are representatives from the Carnegie Mellon Software Engineering Institute, the Internet Security Alliance, SBA and the Department of Justice.

CSD will also reach out through the U.S. Chamber of Commerce and the National Cyber Security Alliance (NCSA) to conduct a small and medium business information security workshop in Fairfax, Virginia.

<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

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)]. A CSD staff person serves as the Chairperson of the Forum. CSD also serves 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.

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, build upon the experiences of other programs and reduce possible duplication of effort. It provides an organizational mechanism for CSD to exchange information directly with Federal agency information security program managers in fulfillment of its leadership mandate under the Federal Information Security Management Act of 2002 (FISMA). It assists CSD in establishing and maintaining relationships with other individuals or organizations that are actively addressing information security issues within the Federal government. Finally, it helps CSD 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

Topics of discussion at Forum meetings in the last year have included briefings on certification and accreditation, protecting critical infrastructure information, Project Matrix, Microsoft Windows XP SP2, status reports on the NIST FISMA Project, and a full-day workshop on automated data collection and reporting tools. This year's annual off-site meeting featured updates on the computer security activities of the Government Accountability Office, the National Institute of Standards and Technology, Office of Management and Budget and the activities of the Department of Homeland Security. Briefings were also provided on e-authentication, privacy issues and the Department of Defense vulnerability assessment and patching program.

In the next year there are plans to have a half-day workshop on the revised security planning guidance and briefings on agency implementation of their certification and accreditation programs and minimum security controls.

<http://csrc.nist.gov/organizations/cspmf.html>

Contact: Ms. Marianne Swanson

(301) 975-3293

marianne.swanson@nist.gov

Ms. Elaine Frye

(301) 975-2819

elaine.frye@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

FISMA places significant requirements on Federal agencies, including NIST, for the protection of information and information systems. In response to this important legislation, CSD is leading the development of key information system security standards and guidelines as part of its FISMA Implementation Project. This high-priority project includes the development of security categorization standards and standards and guidelines for the specification, selection and testing of security controls for information systems.

Publications that are specifically called for by FISMA include Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*; FIPS 200, *Minimum Security Controls for Federal Information Systems*; NIST Special Publication (SP) 800-59, *Guideline for Identifying an Information System as a National Security System*; and SP 800-60,

Guide for Mapping Types of Information and Information Systems to Security Categories. Additional security guidance documents are being developed in support of the project that are not called out directly in the FISMA legislation, including SP 800-37, *Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems*; SP 800-53, *Recommended Security Controls for Federal Information Systems*; and SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*. It should be noted that CSD continues to produce other security standards and guidelines in support of FISMA, which may be found in the CSD Web site's publication section.

To gauge the impact of this project on the massive inventory of Federal information systems, one must first understand how the world of information technology has changed over the past two decades. Not long ago, the information systems that populated Federal enterprises consisted of large, expensive, standalone mainframes, taking up a significant amount of physical space in the facilities and consuming substantial portions of organizational budgets. Information systems were viewed as "big ticket items" requiring specialized policies and procedures to effectively manage.

Today, information systems are more powerful, less costly (for the equivalent computational capability), networked and ubiquitous. The systems, in most cases, are viewed by agencies as commodity items, although items coupled more tightly than ever to the accomplishment of agency missions. However, as the technology raced ahead and brought a new generation of information systems into the Federal government with new access methods and a growing community of users, some of the policies, procedures and approaches employed to ensure the protection of those systems did not keep pace.

The administrative and technological costs of offering a high degree of protection for all Federal information systems at all times would be prohibitive, especially in times of tight governmental budgets. Achieving adequate, cost-effective infor-

mation system security (as defined in Office of Management and Budget Circular A-130, Appendix III) in an era where information technology is a commodity requires some fundamental changes in how the protection problem is addressed. Information systems must be assessed to establish priorities based on the importance of those systems to agency missions.

There is clearly a criticality and sensitivity continuum with regard to agency information systems that affects the ultimate prioritization of those systems. At one end of the continuum, there are high-priority information systems performing very sensitive, mission-critical operations, perhaps as part of the critical information infrastructure. At the other end of the continuum, there are low-priority information systems performing routine agency operations. The application of safeguards and countermeasures (specifically, security controls) to all these information systems should be tailored to the individual systems based on established agency priorities (where the systems fall on the continuum of criticality/sensitivity with regard to supporting the agency's missions). The level of effort dedicated to testing and evaluating the security controls in Federal information systems and the determination and acceptance of risk to the mission in operating those systems (security certification and accreditation) should also be based on the same agency priorities.

Until recently, there were a limited number of standards and guidelines available to help agencies implement a more granular approach to establishing security priorities for their information systems. As a result, many agencies would end up expending too many resources (both administratively and technologically) to protect information systems of lesser criticality/sensitivity and not enough resources to protect systems of greater criticality/sensitivity. Some "load balancing" was needed.

The vision of the FISMA Implementation Project is that the standards and guidelines developed to support FISMA will lead to:

- ◆ More consistent, comparable and repeatable evaluations of security controls applied to information systems
- ◆ A better understanding of enterprise-wide mission risks resulting from the operation of information systems
- ◆ More complete, reliable and trustworthy information for authorizing officials, facilitating more informed security accreditation decisions
- ◆ More secure information systems within the Federal government including the critical infrastructure of the United States

More information about the project, including a schedule and links to publications, may be found at the project's Web site.

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

Mr. Ray Snouffer
(301) 975-4293
stanley.snouffer@nist.gov

SECURITY CERTIFICATION AND ACCREDITATION (C&A)

It is essential that agency officials have the most complete and accurate information possible on the security status of their information systems in order to make credible, risk-based decisions on whether to authorize operation of those systems. Security evaluations are detailed and comprehensive assessments of the technical and non-technical aspects of information systems and networks in operational environments by security professionals. These provide senior executives with the necessary information to authorize the secure operation of those systems and networks. The management responsibilities required by law of executive agencies presume that responsible agency officials understand the risks and other

factors that could adversely affect their missions. Moreover, these officials must understand the current status of their security programs and the security controls planned or in place to protect their information and information systems in order to make informed judgments and investments that appropriately mitigate risk to an acceptable level. The ultimate objective is to conduct the day-to-day operations of the agency and to accomplish the agency's stated missions with what the Office of Management and Budget (OMB) Circular A-130 defines as *adequate security*, or security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

Security accreditation is the official management decision to authorize operation of an information system. This authorization, given by a senior agency official, is applicable to a particular environment of operation and explicitly accepts the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, remaining after the implementation of an agreed upon set of security controls. By accrediting an information system, the agency official is not only responsible for the security of the system but is also accountable for adverse impacts to the agency if a breach of security occurs. Security accreditation, which is required under OMB Circular A-130, provides a form of quality control and challenges managers and technical staff at all levels to implement the most effective security controls and techniques, given technical constraints, operational constraints, cost and schedule constraints and mission requirements.

In addition to risk assessments and security plans, security evaluation also plays an important role in the security accreditation process. It is essential that agency officials have the most complete, accurate and trustworthy information possible on the security status of their information systems in order to make credible, risk-based decisions on whether to authorize operation of those systems. This information and supporting evidence for

system authorization is often developed during a detailed security review of the information system, typically referred to as *security certification*. Security certification is the comprehensive evaluation of the management, operational and technical security controls in an information system. This evaluation, made in support of the security accreditation process, determines the effectiveness of these security controls in a particular environment of operation and the vulnerabilities in the information system after the implementation of such controls.

The results of the security certification are used to reassess the risks and update the security plan for the information system, thus providing the factual basis for the authorizing official to render the security accreditation decision. By accrediting the information system, the agency official accepts the risk associated with it and the implications on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Formalization of the security accreditation process ensures that information systems will be operated with appropriate management review, that there is ongoing monitoring of security controls and that reaccreditation occurs periodically and whenever there is a significant change to the system or its environment.

While the initial goal of this effort, a piece of the FISMA Implementation Project, was to develop a methodology/approach for use by Federal, State and Local governments, significant effort was made to obtain input and consensus from the commercial sector to achieve an additional goal that the methodology/approach become an industry-wide standard for the assessment of a system's IT security (for example, it could potentially be used by commercial sector organizations, adopted by cyber-insurance companies and used as the basis of issuing cyber-insurance policies).

The final version of Special Publication (SP) 800-37, *Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems*, was published in May 2004. This guideline is proposed in the context

of a broader security framework for categorizing the criticality of an IT system and for selecting and assessing/verifying the effectiveness of a system's security controls on a continuing basis.

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

Contacts: Dr. Ron Ross
(301) 975-5390
rross@nist.gov

SECURITY CATEGORIZATION OF INFORMATION AND INFORMATION SYSTEMS

Having a standard way to categorize information and information systems provides a common framework and understanding for expressing security that for the Federal government promotes: 1) effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security and law enforcement communities; and 2) consistent reporting to OMB and Congress on the adequacy and effectiveness of information security policies, procedures and practices. Such a standard is called for in the Federal Information Security Management Act of 2002 (FISMA), and in Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*. This standard, approved by the U.S. Secretary of Commerce, is mandatory for Federal agencies.

FIPS 199 provides the first step toward bringing some order and discipline to the challenge of protecting the large number of information systems supporting the operations and assets of the Federal government. The standard is predicated on a simple and well-established concept – determining appropriate priorities for agency information systems and subsequently applying appropriate measures to adequately protect those systems. The security controls applied to a particular information system should be commensurate with the system's criticality and

sensitivity. FIPS 199 assigns this level of criticality and sensitivity based on the potential impact on agency operations (mission, functions, image, or reputation), agency assets, or individuals should there be a breach in security due to the loss of confidentiality (Unauthorized disclosure of information), integrity (Unauthorized modification of information), or availability (denial of service). FIPS 199 establishes security categories based on the magnitude of harm that can be expected to result from compromises rather than on the results of an assessment that includes an attempt to determine the probability of compromise. FIPS 199 requires Federal agencies to do a "triage" on all of their information types and systems, categorizing each as low, moderate, or high impact for the three security objectives of confidentiality, integrity (including authenticity and non-repudiation) and availability.

While FIPS 199 defines the security categories, security objectives, and impact levels, SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, is designed to assist agencies in mapping their information to these categories. Appendixes to SP 800-60 recommend provisional impact levels for specific information types. They also provide

some rationale for these recommended provisional levels and discuss some of the circumstances that might result in assignment of impact levels higher or lower than the recommended provisional levels.

The basis employed in SP 800-60 for the identification of information types is the Office of Management and Budget's Federal Enterprise Architecture Program Management Office June 2003 publication, *The Business Reference Model Version 2.0* (BRM). The BRM describes functions relating to the purpose of government (missions, or *services to citizens*), the mechanisms the government uses to achieve its purpose (*modes of delivery*), the support functions necessary to conduct government (*support services*), and the resource management functions that support all areas of the government's business (*management of resources*). The information types associated with support services and management of resources functions are treated as management and support types. Some additional information types have been added at the request of Federal agencies.

The long-term effect of employing a FIPS 199 standards-based approach is more targeted,

more cost-effective and improved security for Federal information and information systems. While the interconnection of information systems often increases the risk to an agency's operations and assets, FIPS 199 and the associated suite of standards and guidelines provide a common framework and understanding for expressing information security, and thus, promote greater consistency across diverse organizations in managing that risk. Agencies will determine which information systems are the most important to accomplishing assigned missions based on the security categorization of those systems and will protect the systems appropriately. Agencies will also determine which systems are the least important to their missions and will not allocate excessive resources for the protection of those systems.

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

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

Mr. Wm. Curt Barker (301) 975-8443 william.barker@nist.gov	Ms. Annabelle Lee (301) 975-2941 annabelle.lee@nist.gov
--	---

POTENTIAL IMPACT DEFINITIONS FOR SECURITY OBJECTIVES			
SECURITY OBJECTIVE	POTENTIAL IMPACT		
	Low	Moderate	High
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

SECURITY CONTROLS FOR FEDERAL INFORMATION SYSTEMS

The selection 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. Security controls are the management, operational and technical safeguards and counter-measures prescribed for an information system which, taken together, adequately protect the confidentiality, integrity and availability of the system and its information. There are three important questions that should be answered by organization officials when addressing the security considerations for their information and information systems:

- ◆ What security controls are needed to adequately protect the information and information system that supports the operations and assets of the organization in order to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions and protect individuals?
- ◆ Have the selected security controls been implemented or is there a realistic plan for their implementation?
- ◆ What is the desired or required level of assurance (for example, what would be the grounds for confidence) that the selected security controls, as implemented, are effective in their application?

The answers to these questions cannot be given in isolation but rather in the context of an information security program for the organization that identifies, controls and mitigates risks to its information and information systems.

During the last two years we have worked to create a list of security controls to be recommended for use by organizations in protecting

their information systems in conjunction with, and as part of, a well-defined information security program. In an attempt to create the most technically sound and broadly applicable set of security controls for information systems, a variety of sources were considered during the development of Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*. The sources included security controls from the defense, audit, financial, healthcare and intelligence communities as well as controls defined by national and international standards organizations. The objective of SP 800-53 is to provide a sufficiently rich set of security controls that satisfies the breadth and depth of security requirements for information systems and that are consistent with and complementary to other established security standards.

The catalog of security controls provided in SP 800-53 can be effectively used to demonstrate compliance with a variety of governmental, organizational, or institutional security requirements. It is the responsibility of organizations to select the appropriate security controls, to implement the controls correctly and to demonstrate the effectiveness of the controls in satisfying their stated security requirements. The security controls in the catalog facilitate the development of assessment methods and procedures that can be used to demonstrate control effectiveness in a consistent and repeatable manner, thus contributing to the organization's confidence that there is ongoing compliance with its stated security requirements.

Organizations should use FIPS 199 to define security categories for their information systems. SP 800-53 associates recommended minimum security controls with the FIPS 199 low-, moderate- and high-impact security categories. The recommendations for minimum security controls from SP 800-53 can subsequently be used as a starting point for and input to the organization's risk assessment process. The risk assessment process refines the initial

set of minimum security controls with the resulting set of agreed-upon controls documented in the development of security plans for those information systems. While the FIPS 199 security categorization associates the operation of the information system with the potential impact on an organization's operations and assets, the incorporation of refined threat and vulnerability information during the risk assessment process facilitates the tailoring of the baseline security controls to address organizational needs and tolerance for risk. Deviations from the recommended baseline security controls should be made in accordance with the scoping guidance provided in SP 800-53 and documented with appropriate justification and supporting rationale in the security plan for the information system. The use of security controls from SP 800-53 and the incorporation of baseline (minimum) controls as a starting point in the control selection process facilitate a more consistent level of security in an organizational information system. It also offers the needed flexibility to tailor the controls based on specific organizational policy and requirements documents, particular conditions and circumstances, known threat and vulnerability information, or tolerance for risk to the organization's operations and assets.

FIPS 199 was finished during the last year and was published in February 2004. Work has continued on SP 800-53 this past year and this document will be issued early in 2005.

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

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

ORGANIZATIONAL ACCREDITATION PROGRAM

The second phase 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 the application of the NIST security standards and guidelines associated with the security certification and accreditation of 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 SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.

- ◆ Development of detailed and comprehensive assessment methods and procedures for security controls in SP 800-53, *Recommended Security Controls for Federal Information Systems*.

- ◆ 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.
- ◆ 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 SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, and a public review of the implementation strategy for the accreditation program.

The earliest initial planning for this phase of the FISMA Implementation Project will begin in the coming year. The methodology for this project will be developed following the production of SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, and Federal Information Processing Standard (FIPS) 200, *Minimum Security Controls for Federal Information Systems*. FIPS 200 will be issued, in conformance with legislative requirements, in December 2005. SP 800-53A will be issued in early 2006.

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

Mr. Ray Snouffer
 (301) 975-4293
 stanley.snouffer@nist.gov

Ms. Joan Hash
 (301) 975-5236
 joan.hash@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. CSD is 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. CSD was 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 CIO 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 information technology (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, eleven practices and examples were added to the collection bringing the total to 126.

CSD also invites public and private organizations to submit their information security practices for consideration to be included in the list of practices maintained on the Web site. Policies and procedures may be submitted to NIST 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. Current participants include Computer Associates, the Internet Security Task Force, Microsoft, the SANS Institute, the Carnegie Mellon University CERT Coordination Center, the American Bankers Association, Ars Technica and EDUCAUSE. This area added twelve practices in the past year bringing the total number of listings to twenty.

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

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

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

PROGRAM REVIEW FOR INFORMATION SECURITY MANAGEMENT ASSISTANCE

The NIST Program Review for Information Security Management Assistance (PRISMA) is a new capability that builds upon NIST's former Computer Security Expert Assistance Team (CSEAT) function and has been revised to include more review options and incorporate guidance contained in Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*. The PRISMA is

based upon existing Federal directives including the Federal Information Security Management Act of 2002 (FISMA), NIST guidance and other proven techniques and recognized best practices in the area of information security.

A base set of criteria has been developed by CSD to support PRISMA activity and is updated as lessons are learned and feedback is received at the conclusion of each review.

PRISMA has three primary objectives:

- ◆ To assist agencies in improving their information security programs
- ◆ To support Critical Infrastructure Protection (CIP) Planning
- ◆ To facilitate exchange of effective security practices within the Federal community

PRISMA provides an independent review of the maturity of an agency's IT security program. The review is based upon a combination of proven techniques and best practices, and results in an action plan that provides a Federal agency with a business case-based roadmap to cost-effectively enhance the protection of their information system assets. The PRISMA review, which is not an audit or an inspection, begins with an assessment of the maturity of the agency's IT security program. This includes the agency's IT security policies, procedures and security controls implementation and integration across all business areas. The PRISMA team performs a comparable review of the agency's organizational structure, culture and business mission. After the assessment is performed, the PRISMA team documents issues identified during the assessment phase, and provides corrective actions associated with each issue. These corrective actions are then provided as a prioritized action plan for the agency to use to improve its computer security program. The resulting action plan is weighted to provide the agency the greatest improvements most cost-effectively.

TA	Management, Operational, and Technical Areas	Policy	Procedures	Implemented	Tested	Integrated
1	Information Security Management & Culture	0.63	0.60	0.30		
2	Information Security Planning	0.20	0.20			
3	Security Awareness, Training, and Education			0.40		
4	Budget and Resources			0.60		
5	Life Cycle Management					
6	Certification and Accreditation	0.80	0.30			
7	Critical Infrastructure Protection		0.60	0.30		
8	Incident and Emergency Response	0.80	0.50			
9	Security Controls	0.80	0.60	0.60		

Sample maturity level review results by topic area – The color indicates the level of compliancy with requirements. Green is compliant, yellow is partially compliant and red is non-compliant.

The corrective actions the PRISMA team identifies include the time frame for implementation and the projected resource impact. The action plan can readily be used to develop scopes of work for quick "bootstrapping" of a cyber security program.

PRISMA focuses on nine primary review areas, each of which was derived from a combination of SP 800-26, *Self-Assessment Guide for Information Technology Systems*, as supplemented by other criteria from requirements and guidance found in SP 800-53. Agencies may choose one of two pre-defined review options or work with the PRISMA team to further tailor their reviews.

The PRISMA review is based upon five levels of maturity: policy, procedures, implementation, test and integration. The PRISMA team assesses the maturity level for each of the review criteria. A higher maturity level can only be attained if the previous maturity level is attained. Therefore, if there is an implementation, but there is not a policy for a specific criteria, none of the maturity levels are attained for the specific criteria.

Information from self-assessments generated by using SP 800-26 can be used as inputs to the PRISMA review process as they are self-assessments of individual systems. However, limited

value can be obtained from any self-assessment. PRISMA requires evidence of policies, procedures, implementation, testing and integration of each of the PRISMA criteria. This evidence can be provided in the form of policy and procedure documents, independent assessments of systems, etc.

A PRISMA review is available in two versions. Option One of a PRISMA review focuses on the **strategic aspects** of the overall information security program. This review identifies the level of maturity of the information security program and the agency's ability to comply with existing requirements in eight areas. Option Two focuses on the **strategic aspects** and the **technical aspects** of the overall information security program. This option identifies the level of maturity of the information security program and the agency's ability to comply with existing requirements in nine areas. This review includes all of the criteria in Option One and one additional area of security controls.

Agencies may request a review by the PRISMA team via email at: prisma@nist.gov. Agencies being reviewed will need to provide a liaison knowledgeable about computer security and systems included in the review in order to work with the PRISMA team and collect and organize information received.

Future plans include publication of the review methodology to enable agencies and Inspector Generals (IGs) to employ it as a supplement to other tools.

<http://prisma.nist.gov>
Contacts: Ms. Joan Hash
(301) 975-5236
prisma@nist.gov

Ms. Pauline Bowen (301) 975-2938 prisma@nist.gov	Mr. Richard Kissel (301) 975-5017 prisma@nist.gov
---	--

INFORMATION SECURITY WITHIN THE SYSTEM DEVELOPMENT LIFE CYCLE

Many methods exist that can be used by an organization to effectively develop an information system. A traditional system development life cycle (SDLC) is called a linear sequential model, which assumes that the system will be delivered near the end of the life cycle. Another SDLC method uses the prototyping model, which is often used to develop an understanding of system requirements without developing a final operational system. More complex models have been developed and successfully used to address the evolving complexity of advanced and large information system designs. The SDLC model is

embedded in any of the major system developmental approaches: spiral, incremental development, evolutionary and waterfall.

The expected size and complexity of the system, development schedule and length of a system's life will affect the choice of which SDLC model to use. In most cases, the choice of SDLC model will be defined by an organization's acquisition policy. Including security early in the SDLC typically results in less expensive and more effective security than adding security to an operational system.

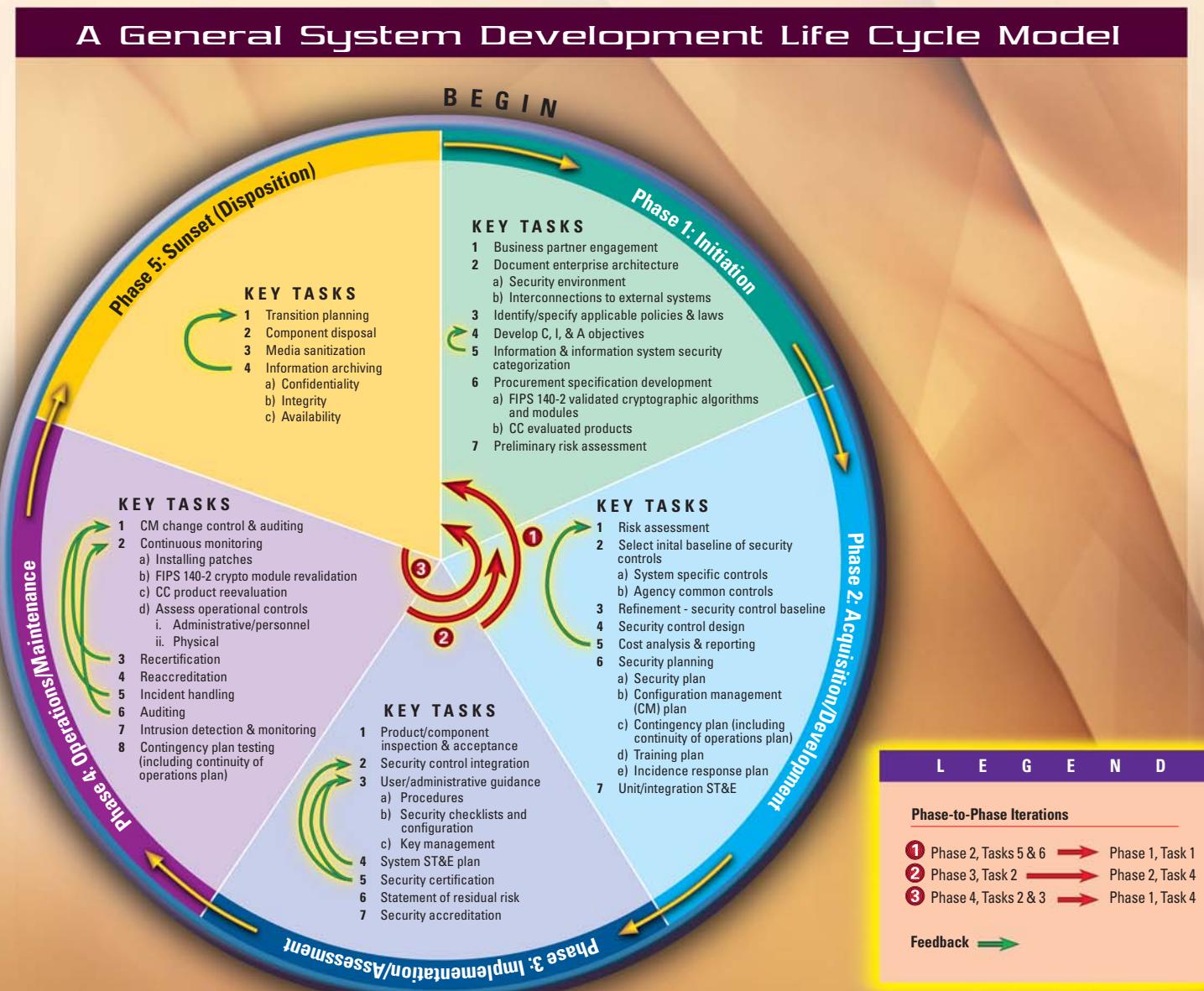
The following questions are some high-level starting points that should be addressed in determining the security controls/countermeasures that will be required for a system:

- ◆ How critical is the system in meeting the organization's mission?
- ◆ What are the security objectives required by the system, such as integrity, confidentiality and availability?
- ◆ What regulations and policies are applicable in determining what is to be protected?

◆ What are the threats that are applicable in the environment where the system will be operational?

◆ Who selects the protection mechanisms that are to be implemented in the system?

Security should be incorporated into all phases of an SDLC model. A general SDLC includes five phases. Each of the five phases – initiation, acquisition/development, implementation, operations/maintenance and disposition – includes a minimum set of information security tasks needed to effectively incorporate security into a



system during its development. There are several NIST documents that are applicable to every phase of the SDLC, including Special Publication (SP) 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, and SP 800-64, *Security Considerations in the Information System Development Life Cycle*.

During the past year, CSD developed and published SP 800-64, *Security Considerations in the Information System Development Life Cycle*. CSD also developed and produced several documents that identify the NIST publications that are applicable in each phase of a general SDLC model. These documents include a brochure with a list of the major publications and a poster with a full listing of all primary and secondary reference materials. The brochure and poster have been widely distributed to Federal agencies and are available on the CSD Web site. Finally, CSD issued an Information Technology Laboratory Bulletin in September 2004 with a full-text version of the information listed on the poster.

<http://csrc.nist.gov/SDLCinfosec>
Contacts: Ms. Annabelle Lee
(301) 975-2941
SDLCinfosec@nist.gov

Ms. Tanya Brewer
(301) 975-4534
SDLCinfosec@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 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, will be released in December 2004. A new user's manual will be issued at this time as NIST Interagency Report (IR) 6885, *Automated Security Self-Evaluation Tool User Manual 2004 Edition*. This manual is intended to help users of ASSET-System 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

Today unsolicited bulk e-mail, or spam, is often used to deliver viruses or initiate fraudulent activity. Spammers have begun to use viruses to take control of insufficiently protected computers in order to route their messages through these machines, or even to have the controlled computer, or "zombie," send the messages with virtually no further control or effort needed. Virus makers have begun to use spammer techniques to deliver their cyber payloads to large numbers of recipients. This combination of techniques is commonly known as a "blended threat."

In addition to blended threats, another new development in the use of spam is quickly becoming a greater security threat. "Phishing," also called "carding," is a high-tech scam that uses spam to send fraudulent e-mail messages in order to deceive consumers into disclosing their credit card numbers, bank account information, Social Security numbers, passwords and other sensitive information. Phishers have recently become even more aggressive and have

begun using a combination of DNS poisoning and domain hijacking to cause users who type a legitimate URL into their browser to be redirected to a criminal Web site that is set up to capture sensitive personal information.

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.

In February 2004, CSD and the Advanced Network Technologies Division (ANTD) sponsored a Spam Technology Workshop, which was attended by 120 people from industry, non-profit organizations and government agencies. The purpose of the workshop was to discuss

technological methods used to address spam, to identify major issues associated with spam detection and reduction, to solicit input from standards bodies on activities related to this area, to get input from Internet service providers on current and future plans in this area and to hear from government and private entities on internal processes being used to address the issue. Finally, the workshop was to assist NIST in developing ideas for criteria and procedures for improving effectiveness of spam controls.

In the past year, CSD has contributed a staff member to the U.S. Delegation to the Organisation for Economic Co-Operation and Development (OECD) Working Party on Information Security and Privacy (WPISP). We have also contributed a staff member as a member of the newly created OECD Task Force on Spam. The Task Force is a joint effort between the OECD Committee for Information, Computer and Communications Policy (ICCP), the WPISP and the OECD Committee on Consumer Policy (CCP), and was established in

order to enhance co-ordination of all work on spam within the OECD.

We will continue to participate in broader U.S. government initiatives to combat spam, including a conference to be held in Winter 2004 in conjunction with the Federal Trade Commission and participation in OECD activities. CSD will also consider ways it can further assist agencies or conduct relevant, useful research on 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

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.

The CSD's testing-focused activities include the validation of cryptographic modules and cryptographic algorithm implementations, assisting with Common Criteria (CC) evaluation and validation programs, facilitation of and participation in international recognition arrangements, 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 CSD 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, AMEX, 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, 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 Accreditation Laboratory Accreditation Program (NVLAP) accredited testing laboratories when having their products evaluated. This project develops new methods of proficiency testing for accreditation and re-accreditation of these laboratories, as well as continuous training opportunities for laboratories. This leads to consistent evaluation and validations of products for use by Federal government agencies and the private sector, as well as to highly-qualified accredited laboratories.

In 2004, one Common Criteria testing laboratory and two Cryptographic Module testing laboratories were re-accredited. Two new laboratories were accredited for Cryptographic Module

Testing and three new accreditations were issued for Common Criteria testing. This past year was also a transitional period. Beginning in fiscal year 2005, the National Security Agency (NSA) and NVLAP will be handling all Common Criteria testing laboratory accreditation.

Currently there are nine laboratories accredited to perform Cryptographic Module testing: five in the United States, two in Canada and two in the United Kingdom. Seven laboratories are to be re-accredited in 2005 and three or more new laboratories should complete accreditation. 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 regularly 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 crypto-



graphic algorithms against established standards is essential to provide security assurance.

Vendors of cryptographic modules and algorithms use independent, private-sector testing laboratories accredited as Cryptographic Module Testing (CMT) laboratories by 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 CSD and the Communication Security Establishment (CSE) of the Canadian Government that provide Federal agencies – in the U.S., Canada and the U.K. – with confidence that a validated cryptographic product 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, 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% of the cryptographic modules and 27% 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 460 certificates have been issued for validated products by the CMVP, representing over 120 vendors. Over 110 of these certificates were issued during 2004. Likewise, over 1,312 certificates have been issued for validated cryptographic algorithms. Over 336 of these certificates were issued in 2004.

The CMVP Symposium, "FIPS 140-2: Where Security Starts," was held in Rockville, Maryland, in September 2004. The CMVP symposium included presentations and discussions on FIPS 140-2, *Security Requirements for Cryptographic Modules*, supporting documents such as the Derived Test Requirements and Implementation Guidance, cryptographic algorithm testing suites, expectations, future direction, panel discussions from Federal and user agencies and laboratory panel discussions. The symposium was planned to be useful for security IT developers (hardware and software), security IT users, cryptographic module/algorithm vendors, procurement specialists, testing laboratories and IT managers.

One of the topics discussed at the Symposium is the work that will begin in 2005 to draft and issue FIPS 140-3. This FIPS will be an update to the current FIPS 140-2. There have been tremendous advances in technology since the

issuance of FIPS 140-2 in May 2001. FIPS 140-2 is becoming more difficult to generically apply to new technologies. Updating this type of document is a very lengthy process, so the work will begin in order to produce FIPS 140-3 before FIPS 140-2 loses its usefulness. Current plans are to begin a public comment period in January 2005 to gain input on the possibility of using FIPS 140-2 as a starting point for FIPS 140-3. Work on the first draft is planned to begin in April 2005 with the first draft being made available for public comment in October 2005. It is thought that the final FIPS 140-3 will become effective in November 2006.

This past year has seen a number of new algorithm validation tests developed in the CAVP. Some of these tests now allow for testing of a number of "legacy algorithms," including Random Number Generators (RNGs), the RSA, the Keyed-Hash Message Authentication Code (HMAC) and the Elliptic Curve Digital Signature Algorithm (ECDSA). These legacy algorithms are cryptographic algorithms that were accepted for use in the CMVP, but did not have validation tests developed in the CAVP. Modules using these legacy algorithms were previously issued certificates based on the general trust of the inherent security of the algorithm and with a

distinction that showed that the implementation of the algorithm was being affirmed as correct by the vendor. All modules using these algorithms from this point forward will be required to go through the full cryptographic algorithm validation testing. This new level of testing will significantly raise the trust and confidence in these modules.

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 2004 with the establishment of FIPS 140-2 as International Organization of Standardization (ISO) standard 19790. The draft of the standard is a new project 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). It is expected that the draft will see progress in the SC's process in the early part of 2005. Also in SC 27, a proposal has been made to devote six months to a study of the development of a methodology for cryptographic module evaluation. A CSD staff member will lead this study.

<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

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

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

To keep pace with the rate of change in emerging technologies we conduct a large amount of research into existing and emerging technologies. 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, recently including 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, University of California-San Diego, 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 Cyber Security Research and Development Act of 2002 (Public Law 107-305) tasks NIST to "develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to, become widely used within the Federal Government." In addition, the Common Configuration Working Group Report of the Technical Standards and Common Criteria Task Force, formed at the Department of Homeland Security's (DHS's) first National Cyber Security Summit in 2003, recommended government promotion of the use of a NIST central repository for IT security configuration checklists. In response, NIST, with sponsorship

from DHS, has created the Security Configuration Checklists Program for IT Products to facilitate the development and dissemination of security configuration checklists so that organizations and individual users can better secure their IT products.

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 NIST
- ◆ 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 the 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.

Some of the benefits that organizations and individuals can achieve by using checklists are:

- ◆ Providing a baseline level of security to protect against common and dangerous local and remote threats and a consistent approach to securing systems
- ◆ Significantly reducing the time required to research and develop appropriate security configurations for installed IT products
- ◆ Allowing smaller organizations to leverage outside resources to implement recommended practice security configurations
- ◆ Preventing public loss of confidence or embarrassment due to compromise of publicly accessible systems

While 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% 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.

CSD will begin to maintain a checklist repository in Winter 2005 containing checklists and descriptions, which will be located at <http://checklists.nist.gov>. Users will be able to search on the descriptions to locate a particular checklist using a variety of different fields, including the product name, vendor name and operational environment/category.

We recognize that checklists are significantly more useful when they follow common security baselines. This program identifies several broad and specialized operational environments, any one of which should be common to most audiences. By identifying and describing these environments, developers can better target their checklists to the general security baselines associated with the environments and users can better select the checklists that are most appropriate for



their operating environments. The operational environments are:

- ◆ Standalone (or Small Office/Home Office - SOHO) describes small computer installations that are used for home or business purposes. Standalone encompasses a variety of small-scale environments and devices, ranging from laptops, mobile devices, or home computers, to telecommuting systems, to small businesses and small branch offices
- ◆ Managed (or Enterprise) are typically centrally-managed environments with defined, organized suites of hardware and software configurations, usually consisting of centrally-managed workstations and servers protected from the Internet by firewalls and other network security devices
- ◆ Specialized Security-Limited Functionality are systems and networks at high risk of attack or data exposure, with security taking precedence over functionality. It assumes systems have limited or specialized (not general-purpose workstations or systems) functionality in a highly threatened environment – such as an outward facing firewall or public Web server – or whose data content or mission purpose is of such value that aggressive trade-offs in favor of security outweigh the potential negative consequences to other useful system attributes such as legacy applications or interoperability with other systems. Checklists for this environment are not recommended for home users or for large-scale, general-purpose systems. This environment could be a subset of other environments
- ◆ Custom environments contain specialized systems in which the functionality and degree of security do not fit the other environments. Legacy is a typical Custom environment. A legacy environment contains older systems or applications that may use older, less-secure communication mecha-

nisms. A Custom environment could be a subset of other environments

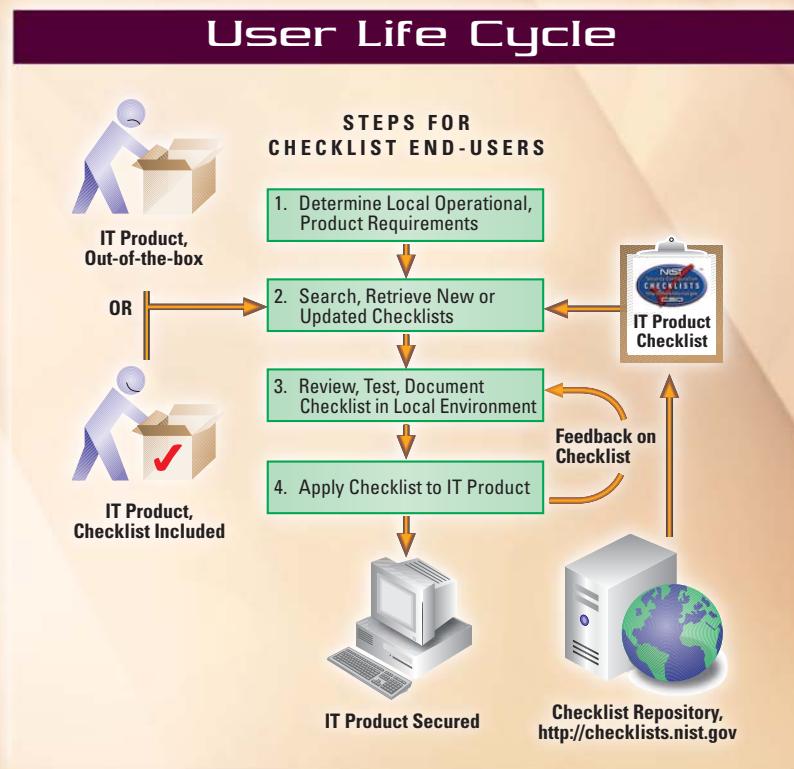
The NIST Security Configuration Checklists Program for IT Products provides a process and guidance for developing and using checklists in a consistent fashion. For checklist users, steps include gathering local requirements, researching and retrieving checklists that match the user's operational environment and security requirements, modifying and documenting the checklist as necessary to take into account local policies and needs, testing the checklist and providing any feedback to NIST and the checklist developers. The final step involves preparation for applying the checklist, such as making configuration or data backups, and then applying the checklist in production.

For checklist developers, steps include the initial development of the checklist, checklist testing, documenting the checklist according to the guidelines of the program and submitting a checklist package to NIST. We will screen the checklist

submission in accordance with the program requirements prior to a public review of the checklist. After the public review period and any subsequent issue resolution, it will be listed on the checklist repository with a detailed description. We will periodically ask checklist developers to review their checklists and provide updates as necessary. Checklists will be retired or archived as they become outdated or incorrect.

The NIST 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. CSD gratefully acknowledges sponsorship for its checklist program from the Department of Homeland Security.

<http://checklists.nist.gov/>
Contact: Mr. John Wack
(301) 975-3411
john.wack@nist.gov



WINDOWS XP SYSTEMS ADMINISTRATION GUIDANCE

When an IT security configuration checklist (also known as a hardening or lockdown guide) is applied to a system in combination with trained system administrators and a sound and effective security program, a substantial reduction in vulnerability exposure can be achieved. During the past year, CSD has produced the draft of Special Publication (SP) 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, in order to assist personnel responsible for the administration and security of Windows XP systems. This guide contains information that can be used to secure desktop Windows XP workstations, mobile computers and telecommuter systems more effectively in a variety of environments, including small offices, home offices (SOHO) and managed enterprise environments. This guidance should only be applied throughout an enterprise by trained and experienced system administrators.

This guide provides detailed information about the security of Windows XP, security configuration guidelines for popular applications and security

configuration guidelines for the Windows XP operating system. 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 in four types of environments: SOHO, Enterprise, Specialized Security-Limited Functionality and Legacy.

This guide includes security templates that will enable system administrators to apply the security recommendations rapidly. The NIST Windows XP Security Templates are text-based configuration files that specify values for security-relevant system settings. The security templates modify several key policy areas of a Windows XP system, including password policy, account lockout policy, auditing policy, user rights assignment, system security options, event log policy, system service settings and file permissions. The templates are based on security templates previously developed by the National Security Agency (NSA), Defense Information Systems Agency (DISA) and Microsoft. Most of the settings in the templates represent consensus recommendations as proposed by various security experts from the Department of

Homeland Security (DHS), Center for Internet Security (CIS), DISA, NSA, Microsoft and NIST.

The NIST templates and additional settings described in SP 800-68 have been applied to test systems and tested according to detailed functional and security test plans. The functionality of common office productivity tools, Web browsers, e-mail clients, personal firewalls, anti-virus software and spyware detection and removal utilities was also tested against the NIST templates and additional settings to identify potential conflicts. By implementing the recommendations described throughout this publication, in addition to the NIST Windows XP security templates themselves and general prescriptive recommendations, organizations should be able to meet a secure common configuration baseline for operating a Windows XP system.

Although the guidance presented in SP 800-68 has undergone considerable testing, every system and environment is unique, so system administrators should perform their own testing. The development of the NIST Windows XP Security Templates was driven by the need to create more secure Windows XP workstation configurations. Because some settings in the templates may reduce the functionality or usability of the system, caution should be used when applying the baseline security templates. Specific settings in the templates should be modified as needed so that the settings conform to local policies and support required system functionality. NIST strongly recommends that organizations fully test the templates on representative systems before widespread deployment. Some settings may inadvertently interfere with applications, particularly legacy applications that may require a less restrictive security profile.

SP 800-68 is due to be finalized early in 2005.

http://csrc.nist.gov/itsec/guidance_WinXP.html
 Contacts: Mr. Murugiah Souppaya
 (301) 975-4758
 murugiah.souppaya@nist.gov



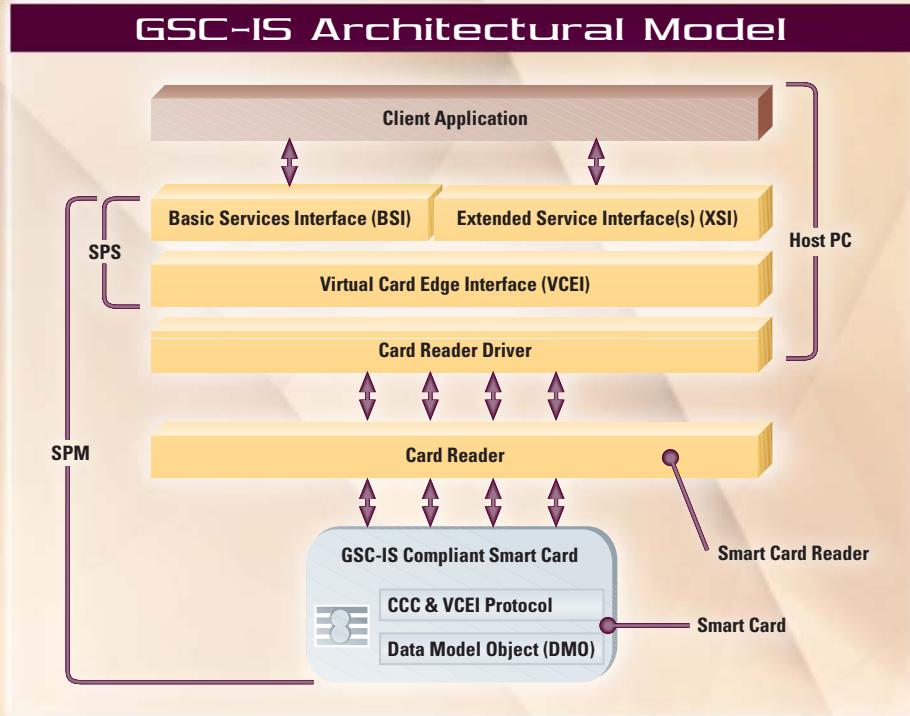
GOVERNMENT SMART CARD PROGRAM

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.

Scientists in CSD have been working 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 version 2.1 was published in July of 2003.

The GSC-IS lays the groundwork for smart cards to work in an open environment. It defines 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.

Homeland Security Presidential Directive #12 (HSPD-12) mandated the Secretary of Commerce to develop a Federal standard for government-wide secure and reliable forms of identification and a smart card is the chosen technology. The Federal government has embraced smart card technology because of the inherent security features and versatility of this technology. For example, a single smart card



could be used as an identification card, to provide access to secure buildings, to securely logon to computer systems and to make small purchases. Approximately 30 to 40 million smart cards are due to be issued within the next few years for government purposes.

The Government Smart Card Inter-Agency Advisory Board (IAB) established the Technical Working Group (TWG), which consists of representatives from the Federal agencies and industry partners. The TWG is co-chaired by NIST and chartered to develop technical solutions for identified government requirements. The IAB and TWG fall under the purview of the Federal Identity Credential Committee (FICC), a committee under the Chief Information Officers (CIO) Council e-Authentication activity.

NIST represents the GSC program in industry, government and formal standards organizations. NIST is also charged with developing a comprehensive GSC conformance test program. CSD has partnered with the Software Diagnostics and Conformance Testing Division (SDCT) for the work of this program.

The fundamental framework of GSC-IS v2.1 was submitted for consideration as an international formal standard. The international ballot was approved with overwhelming success and NIST now provides the Convener of the 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.

A new suite of interoperability standards, ISO/IEC 24727, is under development. In the coming year, NIST will work with ISO and the International Committee for Information Technology Standards/American National Standards Institute (INCITS/ANSI) B10, the U.S. Technical Advisory Group to ISO SC17, on these formal standardization efforts. Continued collaboration with the International Civil Aviation 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 GSC-IS. Finally, close collaboration with the FICC will continue to ensure synchronization of policy, standardization and technical activities of the Federal community.

<http://smartcard.nist.gov/>
 Contacts: Mr. James Dray, technical lead
 (301) 975-3356
 james.dray@nist.gov

Ms. Teresa Schwarzhoff, ANSI/INCITS and ISO Chair,
 standards lead
 (301) 975-5727
 teresa.schwarzhoff@nist.gov

GOVERNMENT-WIDE 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.

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 contractors (including 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 and contractors (including contractor employees).

In accordance with HSPD-12, CSD has begun work on Federal Information Processing Standard (FIPS) 201, *Personal Identity Verification (PIV) for Federal Employees and Contractors*. FIPS 201 will be signed by the Secretary of Commerce by February 25, 2005, in order to comply with the deadlines set out in HSPD-12.

This standard will define 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 will establish 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.

Upon completion of the FIPS 201 standard, CSD will begin Phases II and III of the PIV project.

Under Phase II, we will provide additional specifications for the issuer software and implementation guidance for interoperability among government agencies. The consequences of not accomplishing activities of Phase II will result in lack of early operational interoperability due to varying implementations of the standard. Also, the proper authorities will be unable to validate initial implementations due to the absence of conformance criteria and tests. For some agencies, lack of

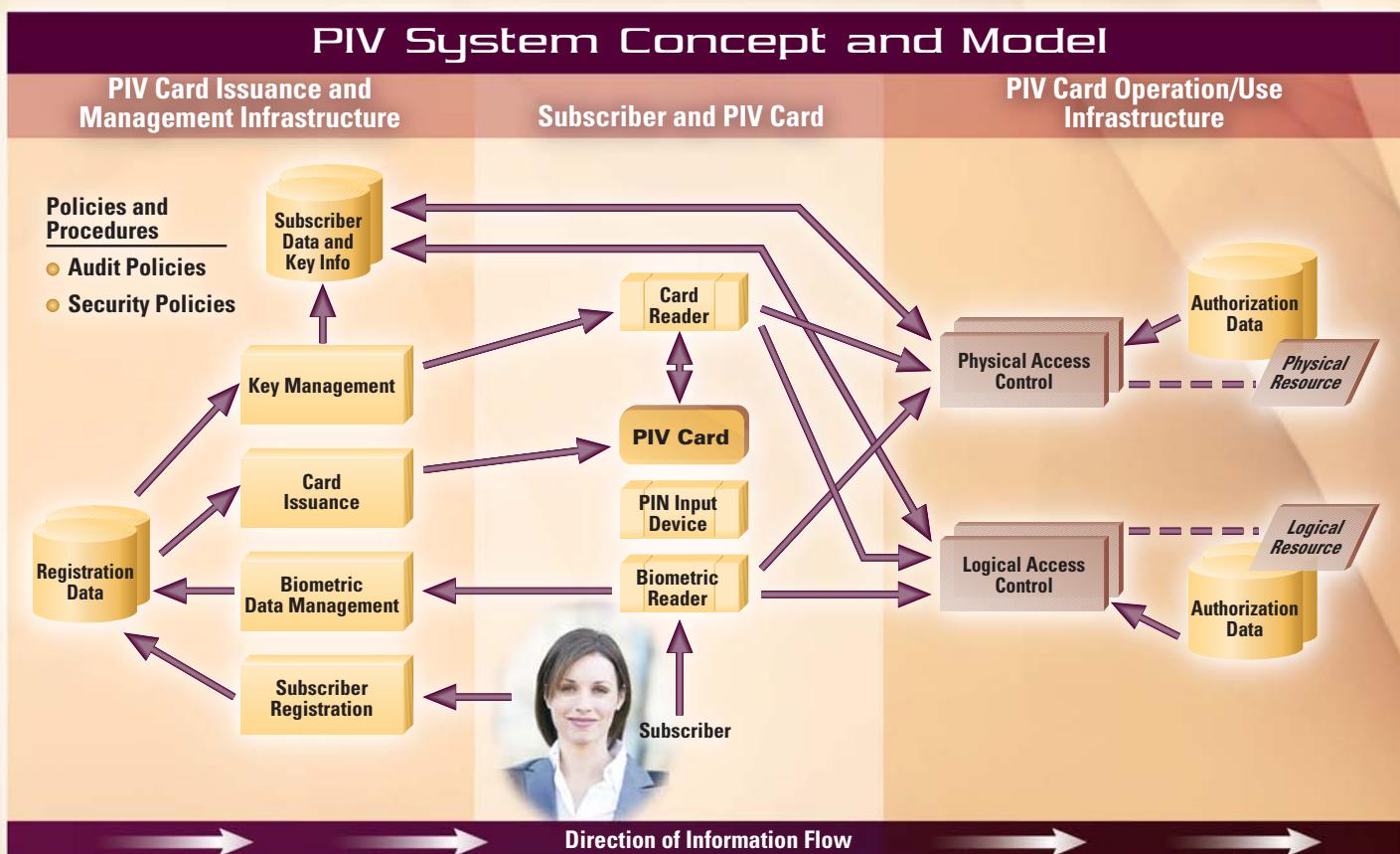
Phase II support may result in delayed implementation of the FIPS 201 standard.

Upon completion of Phase II activities, CSD will begin Phase III of the PIV project. Phase III will entail maintenance support activities such as implementation guidance, reference implementation and conformance testing. Failure to accomplish activities of Phase III may result in 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-project/>
Contacts: Mr. Wm. Curt Barker
(301) 975-8443
william.barker@nist.gov

MOBILE AD HOC NETWORK SECURITY

Ad hoc networks are well suited for sensor networks comprised of small wireless electronic devices that can measure and monitor events and physical properties such as temperature, movement, pressure and location. These sensors can be used to provide visual and audio feedback in environments not easily accessible by humans. Inexpensive wireless sensors can be used to monitor bridges, factories, highways and buildings, for example, to help improve public safety. Mobile handheld devices such as personal digital assistants (PDAs) and laptops can be used by first responders and by today's emerging mobile workforce to easily and quickly set up networks to communicate with their peers. The goal of this research is to develop and test security mechanisms that support secure routing, communication and intrusion detection within small-scale wireless mobile ad-hoc networks (MANET).



The majority of the routing protocols proposed in the literature assume non-hostile environments. Due to their dynamically changing topologies, open environment and lack of centralized security infrastructure, MANETs are susceptible to routing attacks by malicious nodes. NIST has developed a proof-of-concept implementation of a secure ad hoc routing algorithm that provides on-demand trust establishment among the nodes that are collaborating to detect malicious activities. A trust relationship is established based on a dynamic evaluation of the sender's "secure IP address" and of signed evidence. This routing protocol enables the source and destination nodes to establish a secure communication channel between them based on a concept of "statistically unique and cryptographically verifiable" (SUCV) identifiers which ensure a secure binding between IP addresses and keys without assuming the availability of any trusted certification authority (CA) or key distribution center (KDC). This is a joint research project between the University of Maryland and NIST.

MANETs present a number of unique problems for Intrusion Detection Systems (IDS). Differentiating between malicious network activity and spurious, but typical, problems associated with an ad hoc networking environment is a challenging task. In an ad hoc network, malicious nodes may enter and leave the immediate radio transmission range at random intervals or may collude with other malicious nodes to disrupt network activity and avoid detection. Malicious nodes may behave maliciously only intermittently, further complicating their detection. A node that sends out false routing information could be the one that has been compromised or merely one that has a temporarily stale routing table due to volatile physical conditions. Dynamic topologies make it difficult to obtain a global view of the network and any approximation can become quickly outdated. Traffic monitoring in wired networks is usually performed at switches, routers and gateways, but an ad hoc network does not have these types of network elements where the IDS can collect audit data for the entire

network. Network traffic can be monitored on a wired network segment, but ad hoc nodes or sensors can only monitor network traffic within its observable radio transmission range.

In 2004, NIST and the University of Maryland-Baltimore County (UMBC) developed a MANET IDS for ad hoc networks running Ad hoc On Demand Distance Vector (AODV) over IPv6. This MANET IDS is capable of detecting malicious nodes that are dropping or modifying packets as well as nodes that masquerade as other nodes within the network.

In 2005 we will take the lessons learned from our previous work and develop a MANET IDS test bed that will emulate the logical movement of nodes and changes in signal strength of the nodes. This test bed will be able to be used to evaluate different IDS technologies for their ability to detect malicious activity. We will also work on building a collaborative MANET IDS, adding optimization features to the secure routing algorithm we implemented, publishing our results and releasing new versions of the open source code to the research community.

<http://csrc.nist.gov/manet>
 Contacts: Dr. Tom Karygiannis
 (301) 975-4728
 tom.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 802.11'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 2005.

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

ICAT

The ICAT Metabase is a NIST-maintained searchable index of computer vulnerabilities. ICAT provides users with links to a variety of publicly available vulnerability databases and patch sites, thus enabling one to find and fix the vulnerabilities existing on their systems more easily. ICAT allows users to search at a fine granularity, a feature unavailable with most vulnerability databases, by characterizing each vulnerability using over 21 attributes, including software name and version number. ICAT indexes the information available in Computer Emergency Response Team (CERT) advisories, Internet Security Systems X-Force (ISS X-Force), Security Focus, NTBugtraq, Bugtraq and a variety of vendor security and patch bulletins. This system complements publicly available vulnerability databases as a search engine with pointers for users to other sites. ICAT uses, and is completely based on, the industry standard Common Vulnerabilities and Exposures (CVE) naming standard.

Many different types of people use ICAT for a variety of purposes. System administrators and computer security officers use ICAT to identify the known vulnerabilities (and patch information) associated with the software on critical systems. Law enforcement can use ICAT in forensics activities to determine the set of possible vulnerabilities that a hacker might have used to penetrate a system. Computer security researchers use ICAT to identify sets of vulnerabilities that have particular characteristics of interest. Auditors can use ICAT to check to see if particular vulnerabilities have been patched in audited systems.

The last year included a substantial amount of updating and use of ICAT. Over 800 new vulnerabilities were added to the database. The ICAT Web site was highly utilized, totaling some 1.54 million hits.

Work on ICAT over the next year will focus largely on updating and improving an already successful project. We will continue analysis of feedback

from users, using this feedback to improve the Web site. We plan on improving the frequency of the database updates, as well as improving the administrator interface. Finally, we plan to continue updating the vulnerability listings within the database.

<http://icat.nist.gov/>

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

AUTHORIZATION MANAGEMENT AND ADVANCED ACCESS CONTROL MODELS

Access control is the administrative and automated process of defining and limiting which system users can perform which system operations on which system resources. These limitations are based on business rules or policies of a specific host organization. The ability to enforce policy can be of great economic and mission importance to an organization. Although often specified in terms of protection, the ability of an organization to enforce policy enables the sharing of greater volumes of data and resources to a greater and more diverse user community. Access control policies are enforced through a mechanism consisting of access control functions and access control data that together map a user's access request to a decision whether to grant or deny access.

Today access control mechanisms come in a wide variety of forms, each with distinct policy advantages and disadvantages. Although each may meet specific access needs, the resulting technology has disappointed the marketplace. This is due to the reality that a given access control mechanism may meet the policy requirements within a particular market domain, while being completely inappropriate in another. The reality is that access control policies can be as diverse as the business applications that need to enforce

them. This rigidity creates a problem when the protection required of an application/organization/agency is different from the policy(ies) built into the mechanism at hand. This problem is exacerbated when there is a mission need to share and coordinate information among operational units.

The ability of an organization to enforce its access control policies directly impacts its ability to execute its mission – by determining the degree to which its volumes of resources may be protected and shared among its user community. Whether in regard to the Government's war on terror or a company's formation of a strategic partnership, the focus on sharing information is becoming increasingly acute. Unfortunately, when it comes to access control mechanisms, one size does not fit all.

At the request and support of the Department of Homeland Security (DHS), CSD has initiated a project in pursuit of a standardized access control mechanism that is general enough to configure and enforce any attribute-based access control policy, referred to as the Policy Machine (PM). A core feature is the PM's ability to configure and enforce arbitrary attribute-based access control policies and its ability to protect resources under multiple instances of these policies. It is not our intent to devise a completely new access control mechanism, but instead to redefine, implement and transfer to industry an access control mechanism that we believe includes abstractions, properties and functions common to most if not all access control mechanisms.

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

- ◆ Increased user productivity through the increased sharing of resources
- ◆ Decreased insider crime through the ability to enforce organization-specific access control policies

- ◆ Increased administrator productivity through better interfaces in configuring access control policy
- ◆ Increased cooperation among organizations through the potential for the coordination and exchange of interoperability of access control data

Development of the PM has been ongoing during the last year and will continue in the coming year.

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

VOICE OVER INTERNET PROTOCOL SECURITY ISSUES

Voice over IP (VoIP) – the transmission of voice over packet-switched IP networks – is one of the most important emerging trends in telecommunications. As with many new technologies, VoIP introduces both security risks and opportunities. For several years VoIP was a technology prospect, something on the horizon for the "future

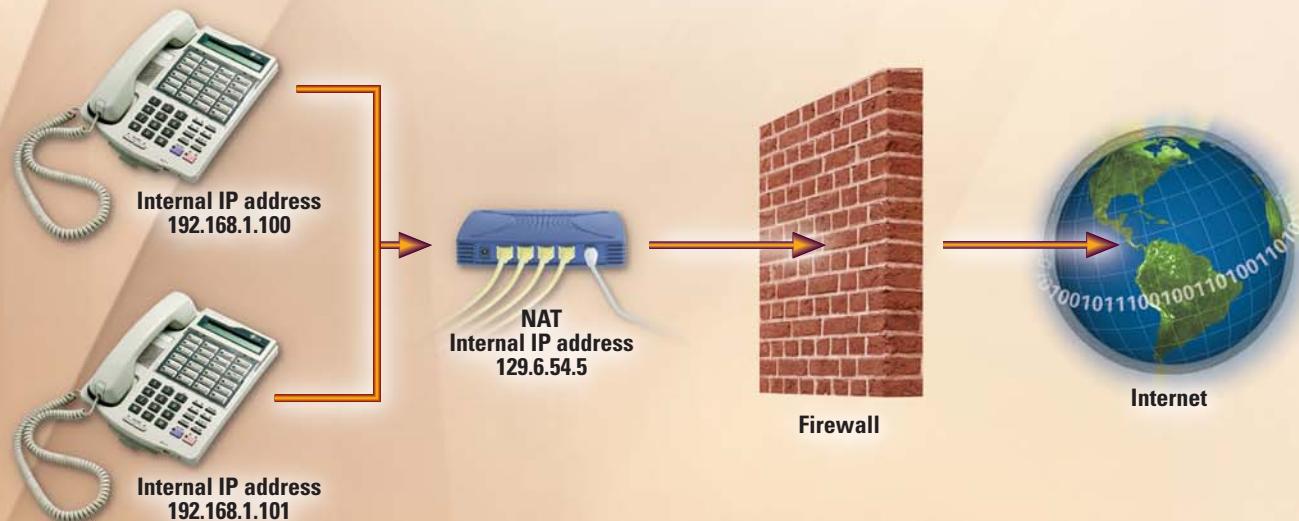
"works" segment of telephony and networking papers. Now, however, telecommunications companies and other organizations have already, or are in the process of, moving their telephony infrastructure to their data networks. The VoIP solution provides a cheaper and clearer alternative to traditional public switched telephone network (PSTN) phone lines. Although its implementation is widespread, the technology is still developing. It is growing rapidly throughout North America and Europe, but it sometimes can be difficult to integrate with existing systems. Nevertheless, VoIP will capture a significant portion of the telephony market given the fiscal savings and flexibility that it can provide.

VoIP systems take a wide variety of forms, including traditional telephone handsets, conferencing units and mobile units. In addition to end-user equipment, VoIP systems include a variety of other components, including call processors/call managers, gateways, routers, firewalls and protocols. Most of these components have counterparts used in data networks, but the performance demands of VoIP mean that ordinary network software and hardware must be supplemented with special VoIP components. Not only does VoIP require higher performance than most data

systems, critical services, such as Emergency 911, must be accommodated. One of the main sources of confusion for those new to VoIP is the (natural) assumption that because digitized voice travels in packets just like other data, existing network architectures and tools can be used without change. However, VoIP adds a number of complications to existing network technology, and these problems are magnified by security considerations.

Quality of Service (QoS) is fundamental to the operation of a VoIP network that meets users' quality expectations. However, the implementation of various security measures can cause a marked deterioration in QoS unless VoIP-specific equipment and architectures are used. These complications range from firewalls delaying or blocking call setups to encryption-produced latency and delay variation (jitter). Because of the time-critical nature of VoIP and its low tolerance for disruption and packet loss, many security measures implemented in traditional data networks are simply not applicable to VoIP in their current form; firewalls, intrusion detection systems and other components must be specialized for VoIP. Most current VoIP systems use one of two standards – H.323 or the Session Initiation

IP Telephone Security



IP Telephones behind Name Address Translator (NAT) and Firewall

Protocol (SIP). Although SIP seems to be gaining in popularity, neither of these protocols has become dominant in the market yet, so it often makes sense to incorporate components that can support both.

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

The current Internet architecture does not provide the same physical wire security as the phone lines. The key to securing VoIP is to use the security mechanisms like those deployed in data networks

(firewalls, encryption, etc.) to emulate the security level currently enjoyed by PSTN network users.

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

During the past year, the CSD has considered the security implications of VoIP and worked to produce guidance for Federal agencies to use when developing and deploying VoIP systems. Special Publication (SP) 800-58, *Security Considerations for Voice Over IP Systems*, was released as a draft for public comment in May 2004. This publication investigates the attacks and defenses relevant to VoIP and explores ways to provide appropriate levels of security for VoIP networks at reasonable cost. The document is due to be finalized in early 2005.

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

REFERENCE IMPLEMENTATIONS FOR AUTOMATED TEST GENERATION TOOLKIT

The automated test generation framework and the associated toolkit were originally applied to develop executable test code for testing the security functions of a commercial database management system (DBMS) product. The test generation framework makes use of formal verification models to generate test vectors. It has been found that test vectors generated using this approach provide adequate path coverage as well as traceability of tests to func-

tional requirements. It was also found that this approach could be used to generate conformance tests for other types of functional requirements such as the Interoperability requirements.

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 formal verification model of the 23 interoperability functions between client application and Smart Card middleware resulted in 419 requirement threads and 390 test vectors. These test vectors together with the verification model and middleware access environmental information were used in a test code generator to generate executable Java code containing 390 tests.

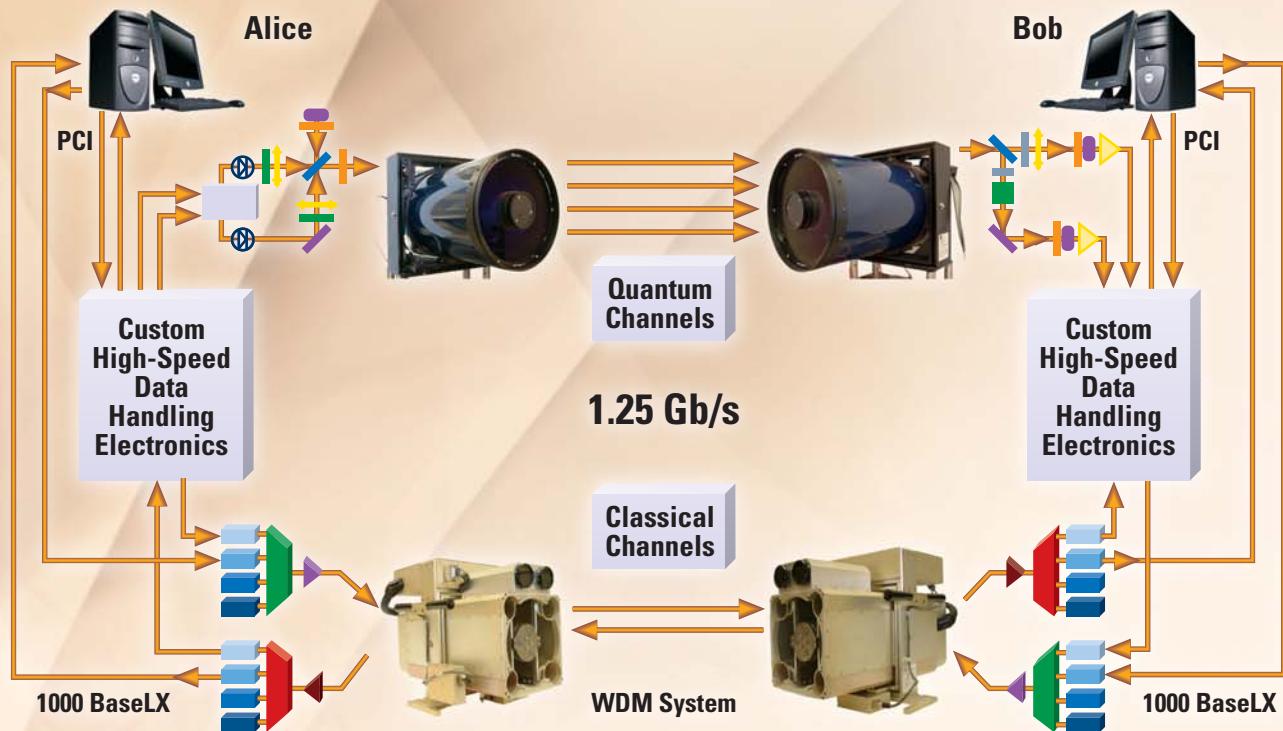
We plan to apply this methodology to generate conformance tests for testing all the interface requirements for Smart Cards to be used across the Federal government for Personal Identity Verification. These interface requirements are specified in SP 800-73, *Integrated Circuit Card for Personal Identity Verification*.

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

Quantum Key Distribution



Quantum Key Distribution with 1.25 Gbs Clock Synchronization Demonstrated

communications, and could have enormous impacts on homeland security. Whereas current computers calculate linearly, quantum computers will be able to calculate enormous number of variables simultaneously. This capability is particularly useful in modeling complex situations with many variables (weather modeling, for example) and in solving extremely difficult equations (processing tasks that would literally take billions of years on conventional computers).

Exploiting quantum properties would be particularly valuable in cryptography, making codes that would be unbreakable by the best supercomputers of tomorrow or breaking codes in nanoseconds that could not be cracked in millions of years by the most powerful binary computers. Quantum information also can be used for remarkably secure communications. In this 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; 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 shown to be secure if implementations preserve assumptions regarding physical properties of the system. Many varieties of the BB84 scheme have been developed and other forms of quantum key distribution have been proposed as well.

Quantum cryptography offers the potential for stronger security, but as with any information technology, QKD must be designed and implemented properly to provide 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 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 system that represents a major increase in the attainable rate of quantum key generation, over 100 times faster than previously reported results. 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 investigate applications of quantum cryptography to the problem of secure routing.

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

Contact: 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 and the Computer Security Division. 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 IPsec has also continued.

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. To the user and application process this translation is a service provided either by the local host or from a remote host via the Internet. The DNS server may communicate with other Internet DNS servers if it cannot translate the address itself.

There are several distinct classes of threats to the DNS, most of which are DNS-related instances of more general problems, but a few of which 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 (a) origin

authentication of DNS data, (b) data integrity and (c) 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 2004, NIST achieved several significant milestones towards its goal of expediting commercial standards and test and measurement tools for DNSSEC. In addition to leading the IETF DNSSEC editors' team, we actively participated in the U.S. government DNSSEC Deployment team. We initiated efforts to develop operational plans for the secure operation of .gov and subordinate domains. An initial prototype of the Secure Zone Integrity Tester (SZIT) was completed and put online for diagnosing configuration and operation errors in operational DNSSEC-enabled servers. A NIST Special Publication (SP) 800 Series document, *Secure Domain Name*

System Deployment Guide, was drafted and is being completed by the DNSSEC team. This draft guidance document defines the DNS security problem space, outlines best current practices for securing DNS operations and provides deployment guidance for DNSSEC technologies. Development of an open DNSSEC benchmark framework consisting of measured and cataloged data sets, standard reference models and test scenarios, open source benchmark tools and agreed upon metrics was begun. Development of a DNS zone anonymizer and statistical analysis tools was completed. We collected and statistically analyzed over 2000 DNS zones, developed clustering techniques to facilitate cataloging of zone models and began development of DNS traffic analysis tools.

The focus of our 2005 activities will be to continue the development of the DNSSEC benchmark framework, to prototype and put online persistent DNSSEC monitoring tools, to publish and promote the SP 800 guidance document and to lead the development of operational plans for securing the .gov domain.

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

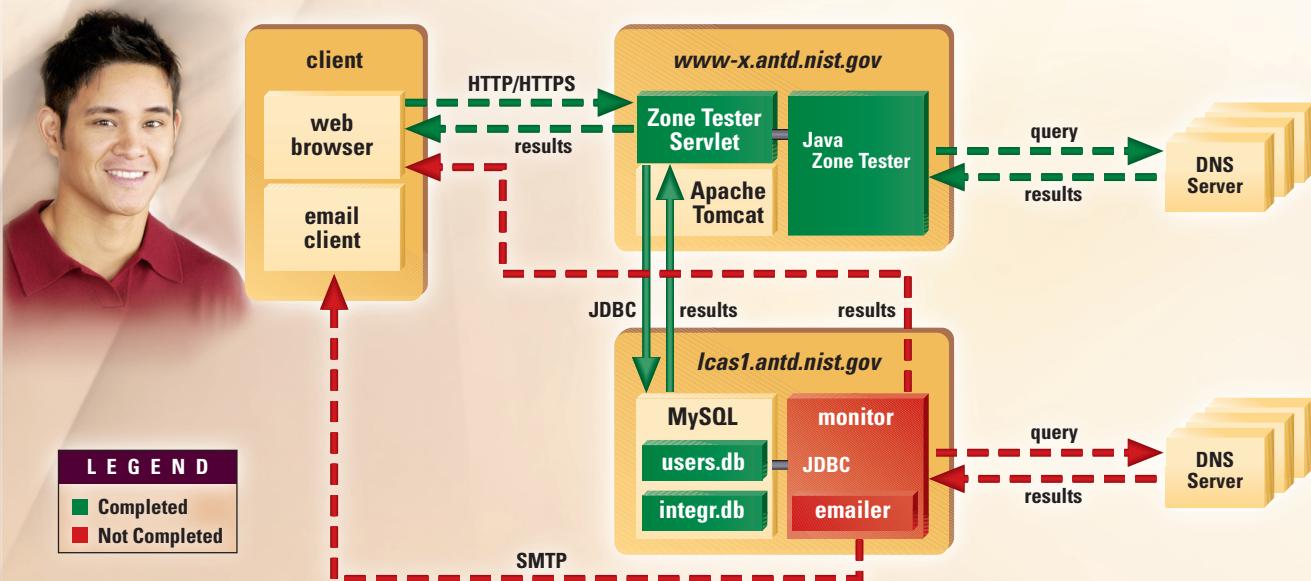
BORDER GATEWAY PROTOCOL

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). Previously there was a lack of awareness and knowledge in the IT sector of the potential threats, risks, mitigation techniques and their cost.

The BGP project was kicked off in February 2004. The project aims to help the 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 IETF community. The project also seeks to expedite convergence towards standardized, implemented and deployed BGP security solutions.

NIST 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

Global DNSSEC Monitoring Tool (GDMT) Architecture



of focused BGP attacks and analytical models of threat versus countermeasure effectiveness. NIST is 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 made a number of accomplishments. In the attack-modeling framework, we extended the Scalable Simulation Framework (SSF)/Dartmouth BGP discrete event simulation tools with the ability to generate arbitrary focused attacks on BGP infrastructures. We designed a general framework for modeling attacks on BGP protocols. We designed metrics and analysis/visualization tools to characterize the effect of simulated successful BGP attacks, including routing quality metrics, BGP protocol metrics and measured attack properties.

In addition to these accomplishments we developed the Attack Vs. Countermeasure Effectiveness (ACE) modeling tool. ACE includes details of attack trees and allows mapping of components of solution space (countermeasures) to components of problem space (atomic attack goals).

The focus of our 2005 activities will be to complete remaining features of the modeling and analysis tools developed in 2004 and to extensively use these tools to generate meaningful contributions to the on-going industry deliberation on the requirements for and design of BGP security solutions. In fiscal year 2005 we plan to make active contributions to the IETF RPSec working group and to issue the first draft of our NIST BGP security guidance document. We expect to expand our collaborations with the DETER/EMIST routing team in the areas of

attack models, analysis techniques and coordinated experimentation.

<http://www.antd.nist.gov/iipp.shtml>
Contact: Mr. D. Richard Kuhn
(301) 975-3337
kuhn@nist.gov

transmitted between networks. Although VPNs can reduce the risks of networking, they cannot eliminate it. For example, a VPN implementation may have flaws in algorithms or software, or insecure configuration settings and values that attackers can exploit.

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 protection.

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

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 have begun work on Special Publication (SP) 800-77, *Guide to IPSec VPNs*. This document will describe 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

Gateway-to-Gateway VPN for Remote Office Connectivity



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 will describe the components of IPsec. It also will present a phased approach to IPsec planning and implementation that can help in achieving successful IPsec deployments. The five phases of the approach are to identify needs, design the solution, implement and test a prototype, deploy the solution and manage the solution. Special considerations affecting configuration and deployment will be analyzed and three test cases will be presented to illustrate the process of planning and implementing IPsec VPNs. SP 800-77 will be published in 2005.

<http://csrc.nist.gov/ipsec/>
 Contact: Ms. Sheila Frankel
 (301) 975-3297
 sheila.frankel@nist.gov

DIGITAL FORENSICS

The digital forensic community faces a constant challenge to stay on top of the latest technologies that may be used to reveal relevant clues in an investigation. Personal digital assistants (PDAs) and cellular telephones are commonplace in today's society, used by many individuals for both personal and professional purposes. Handheld device technologies are changing rapidly with new products and features being introduced regularly.

When a PDA or cellular phone is encountered during an investigation, many questions arise: What should be done about maintaining power? How should the device 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 the hardware and software characteristics of PDAs. Developing an understanding of the components and inner workings of these devices (such as memory organization and use) is a prerequisite to understanding the criticalities involved when

dealing with digital devices. PDA memory (that is, RAM) is volatile and requires power to maintain data unlike a personal computer's hard disk.

CSD has worked this past year to produce SP 800-72, *Guidelines on PDA Forensics*, which was released as a public draft in August 2004. The intended audience is varied and ranges 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. The practices recommended in this guide are designed to highlight key principles associated with the handling and examination of electronic evidence, in general, and PDAs in particular.

SP 800-72 will be finalized in Winter 2005. We will continue to work on digital forensics in the coming year, particularly in the area of cellular phones. We will also be working with the NIST Office of Law Enforcement Standards on digital forensic issues.

Contact: Mr. Richard Ayers
 (301) 975-4971
 richard.ayers@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. CSD 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 begun in this area. A few examples of the impact this work will have in the near future include changes to Federal employee identification methods, how users authenticate their identity when needing government services online and the technical aspects of passports issued to U.S. citizens.

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). CSD has 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 makes guidance and education available 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. Many of the projects discussed in this area of work are combined to form the CToolkit.

The past year has seen a great deal of work go into the CToolkit. Final drafts of the NIST Special Publication (SP) 800-56, *Recommendation on Key Establishment Schemes*, and Parts 1 and 2 of SP 800-57, *Recommendation on Key Management*, will be posted for public review in Spring 2005. Drafts for public review and comment will also be posted for SP 800-38B, *Recommendation for Block Cipher Modes of Operation: The RMAC Authentication Mode* (RMAC – Randomized Message Authentication Code), and a revision of SP 800-21, *Guideline for Implementing Cryptography*.

Plans for 2005 also include completion of a revision of the Digital Signature Standard (DSS), a recommendation specifying deterministic random bit generators and a recommendation for the use of cryptographic algorithms and key sizes.

Validation tests have been developed for the Digital Signature Algorithm (DSA), the Secure Hash Algorithm (SHA), the Keyed-Hash Message Authentication Code (HMAC) and ANSI X9.62 the Elliptic Curve Digital Signature Algorithm (ECDSA), and will be delivered to the validation laboratories early next year.

<http://csrc.nist.gov/CryptoToolkit/index.html>

Contact: Ms. Elaine Barker
(301) 975-2911
elaine.barker@nist.gov

BIOMETRIC STANDARDS PROGRAM

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 standards developments, migration from proprietary systems to open-systems standard-based solutions will be more difficult and expensive. Therefore, standards are the corner-

stone of our biometrics program. Deploying new information technology systems for homeland security and for preventing ID theft will require both national and international consensus standards for biometrics. NIST is responding to government and market requirements for open-system standards by accelerating development of formal national and international biometric standards and associated conformity assessment.

These standards and associated conformity assessment need further development in order to help deploy significantly better, open-systems security solutions. NIST has 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 NIST has 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 U.S. This program is a major catalyst for biometric standardization and adoption of biometric standards.

Nationally, the 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. We are active technical contributors to this standards development body and have sponsored several of their standards development projects. The program experts work in close collaboration with NIST's Information Technology Laboratory (ITL) Information Access

Division (IAD) biometric experts. 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. We have also participated in related consortia efforts, including the U.S. Biometrics Consortium.

Our strategy in this program includes:

- ◆ Leveraging existing consortia standards (such as the Bio Application Programming Interface (BioAPI) Consortium and Common Biometric Exchange File Format (CBEFF))
- ◆ 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)

- ◆ 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

In 2004, the International Civil Aviation Administration (ICAO) adopted a global, harmonized blueprint for the integration of biometric identification information into passports, which requires conformance to JTC 1/SC 37 standards. Also in 2004, five biometric data interchange formats developed by INCITS M1 were approved as America National Standards. In late 2004, DHS is expected to adopt the face recognition standard developed by INCITS M1.

The U.S. Biometric Consortium (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 academia. 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 (a) Biometric Data Protection and Usage; (b) Biometric Application Programming Interface for Java Card, and (c) an augmented version of the Common Biometric Exchange File Format (the initial version of CBEFF was published as NIST Interagency Report (NIST IR) 6529). A revised and augmented version of CBEFF was published as NIST IR 6529-A. An international version of CBEFF is being developed within JTC 1/SC 37. CBEFF is a requirement for conformance for all

of 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 is an International Organization of Standardization (ISO) standard candidate (under development in JTC 1/SC 37-Biometrics).

Mr. Fernando Podio manages this ITL/CSD program. In the past year he was recognized by INCITS for his excellent leadership and work as the Chair of the TC M1 on Biometrics. In 2003, he was awarded, together with several ITL/IAD biometric experts, a Group Gold Medal Award for Scientific/Engineering Achievement for this program's impact on biometric standards development.

<http://csrc.nist.gov/CryptoToolkit/tkkeymgmt.html>

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

MODES OF OPERATION FOR BLOCK CIPHER ALGORITHMS

A mode of operation, or mode for short, is an algorithm that features the use of a symmetric key block cipher algorithm to provide an information service, such as confidentiality or authentication. With the advent of new block ciphers, such as the Advanced Encryption Standard (AES), there is a need to update long-standing modes of operation and an opportunity to consider the development of new modes. One important motivation for updating modes is the increased block size of the AES algorithm

compared to the Digital Encryption Standard (DES) algorithm (128 bits instead of 64 bits).

NIST is in the process of specifying modes in the Special Publication (SP) 800-38 series. Work in 2004 focused on the second part of the series – specifying an authentication mode – and the third part – specifying a combined mode for authentication and confidentiality.

A draft version of SP 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Authentication Mode*, underwent internal technical review in 2004 and is expected to be released for public comment in March 2005. The CMAC (Cipher-based Message Authentication Code) mode is essentially the OMAC (One-key Cipher Block Chaining Message Authentication Code) variation of the XCBC (Extended Ciphertext Block Chaining) authentication algorithm. This part of the series is expected to be finalized in 2005.

Special Publication 800-38C specifies the CCM (Counter with CBC MAC) algorithm, 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). This part in the series was finalized in 2004.

Mode development is expected to be an ongoing effort. Later parts of the series may be devoted to the specification of new modes. In the next year, for example, NIST will consider whether to propose additional combined confidentiality-authentication modes, possibly including an AES key wrap.

<http://nist.gov/modes>
Contact: Dr. Morris Dworkin
(301) 975-3356
morris.dworkin@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 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, CSD's 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 remote-

ly 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. After completing a risk assessment and mapping the identified risks to the required assurance level, Federal agencies can identify and implement appropriate authentication mechanisms based on the guidance in SP 800-63. This publication assumes the person and Federal IT system are communicating over an open network. 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.

While not addressed in SP 800-63, NIST is studying e-authentication mechanisms that are not based on possession and control of a secret, such as knowledge-based authentication (KBA) and remote biometrics. KBA techniques achieve authentication by testing the personal knowledge of the individual. Since this information is private but not actually secret, confidence in the identity of an individual may be hard to achieve. In February 2004, NIST hosted a Knowledge-Based Authentication Symposium to help identify standard authentication metrics that can be applied to KBA tools and solutions. 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, NIST will hold a workshop to examine remote authentication protocols and biometrics. NIST will continue to study both the topics of knowledge-based authentication and biometrics, and may issue additional guidance in the future on their uses for remote authentication of individuals across a network.

Federal agencies may choose to authenticate users through credentials issued by industry, associations, or local government. NIST is supporting the development of accreditation procedures for Credential Service Providers (CSPs) based on the technical requirements in SP 800-63. These procedures will provide the foundation for efficient evaluation and selection of acceptable CSPs by Federal agencies without requiring specialized expertise.

In this project, NIST is collaborating with Federal agencies and industry partners. Federal agencies include the Office of Management and Budget, Government Services Administration, the Federal Identity and Credentialing Committee and the Social Security Administration. Industry partners include Wells Fargo Bank, VeriSign, Digital Signature Trust/Identrus, ElectroSoft Systems, Phoenix Technologies and Caradas.

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

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

E-GOV IDENTITY MANAGEMENT INFRASTRUCTURE

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 system that could span numerous agencies and applications. The Federal government spent in excess of \$160M in fiscal year 2003 and 2004 on potentially inconsistent or agency-unique authentication and identity management infrastructure. 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 approach for authentication and identity management is a better alternative. One type of approach – an identity management infrastructure – brings scalability and higher cost-effectiveness to an environment of widely varying authentications techniques and identity verification needs.

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 NIST 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. It is the expectation of the Federal Identity Credentialing Committee (FICC) that 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).

NIST continues 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.

CSD plays a leading role on the FICC's SSP Subcommittee. We provide the technical knowl-

edge 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, support smart cards that implement the Government Smart Card Interoperability Specification (GSC-IS) version 2.1 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.

It has been asked why the SSP system is necessary when services are currently available under the Access Certificates for Electronic Services (ACES) program or the GSA smart card contract. The SSP Program does not establish a contract but creates a qualified bidders list. The SSP Subcommittee does not want to limit agencies to one solution. The SSP Subcommittee does want to set a standard for PKI that implements a common policy in the Federal government that ensures a minimum level of security and quality when agencies contract for PKI services.

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 will mediate 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. NIST 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.

As part of this project, NIST is researching Web services protocols including Simple Object Access Protocol (SOAP) and Security Assertion Markup Language (SAML), effective password use and registration and identity proofing. We are collaborating with many entities, including the Federal PKI Policy Authority (FPKIPA), FICC, GSA, the Government Accountability Office (GAO), the National Security Agency (NSA), the Federal Deposit Insurance Corporation (FDIC), OMB, the States of Illinois and Washington and EduCause, which includes 1,800 universities, colleges and educational institutions.

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

Mr. Wm. Tim Polk (301) 975-3348 william.polk@nist.gov	Ms. Donna Dodson (301) 975-3669 donna.dodson@nist.gov
--	--

HONORS AND AWARDS

DEPARTMENT OF COMMERCE GOLD MEDAL FOR SCIENTIFIC/ENGINEERING ACHIEVEMENT



The NIST Smart Card Team, consisting of (left to right) John Wack, Teresa Schwarhoff, James Dray, and Alan Goldfine, Software Diagnostics and Conformance Testing Division, received the 2004 Gold Medal Award for the development of a framework and specification that dramatically advanced interoperability among smart card applications, coalesced U.S. government requirements and forged alliances with the world's foremost authorities on smart cards. The work of the NIST Smart Card Team served to open an entire market to U.S. businesses while dramatically increasing the security of government agencies.

WORLD STANDARDS DAY 2004 BEST PAPER

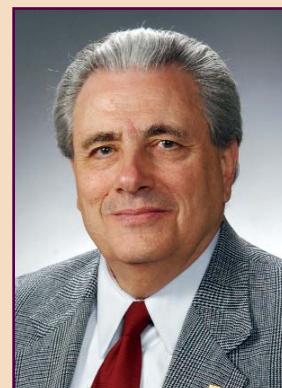
Alicia Clay and Michael Hogan (ITL) were awarded First Place in the World Standards Day 2004 Paper Competition for their paper, "Securely Connecting the World with Cyber Security Standards." Since 1990, the U.S. standards community has annually observed World Standards Day, so designated by the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC) and the International Telecommunications Union (ITU).



The theme for the 2004 celebration was "Standards Connect the World." The U.S. celebration, co-chaired by NIST and ANSI with participation by some 50 trade associations, professional societies, standards development organizations, corporations and government agencies, paid tribute to the value of standardization to the Nation's economy and the consuming public. The paper was published in the November/December 2004 issue of *Standards Engineering: The Journal of the Standards Engineering Society*.

GENE MILLIGAN AWARD FOR EFFECTIVE COMMITTEE MANAGEMENT FOR 2003

Fernando Podio was awarded the Gene Milligan Award for Effective Committee Management for 2003 by the InterNational Committee for Information Technology Standards (INCITS) for his work with the Technical Committee M1, Biometrics. This award recognizes individuals who, as officers, have provided outstanding leadership to the subgroup in its national and/or international work, have demonstrated proficiency in achieving consensus in the national and/or international arenas and have followed the approved procedures in an exemplary fashion.



INCITS SERVICE AWARD FOR 2003

Teresa Schwarhoff was recognized by the InterNational Committee for Information Technology Standards (INCITS) for her contribution to the INCITS B10 committee on standardization of the U.S. Government Smart Card Interoperability Specification. Ms. Schwarhoff's excellent work toward standardization of the specification had a clear and positive impact on national security and competitiveness of the U.S. smart card industry.



FED 100 AWARD – FEDERAL COMPUTER WEEK

Joan Hash was selected by Federal Computer Week to receive a 2004 "Fed 100" Award. The judges for these awards look for someone who has made a noticeable difference in an agency or in the community at large. Ms. Hash was recognized for providing principal direction to the development of security management guidelines and serving as key reviewer and often co-author to ensure overall quality and consistency with legal, policy and other existing security guidelines.



PRESIDENTIAL MANAGEMENT FELLOW

Tanya Brewer completed and became an alumnus of the Presidential Management Fellows Program. The Presidential Management Fellows Program was established by Executive Order in 1977 to attract to the Federal service outstanding graduate students from a wide variety of academic disciplines who demonstrate an exceptional ability for, as well as a clear interest in and commitment to, leadership in the analysis and management of public policies and programs. Not more than 400 Fellowships are awarded annually. In addition to being a CSD staff member, Ms. Brewer completed a temporary detail in the Office of U.S. Senator Ron Wyden during the 108th Congress.



Computer Security Division Publications - 2004

NIST SPECIAL PUBLICATIONS

SP 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher	May 2004
SP 800-64	Security Considerations in the Information System Development Life Cycle	October 2003
SP 800-63	Recommendation for Electronic Authentication	July 2004
SP 800-61	Computer Security Incident Handling Guide	January 2004
SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories	June 2004
SP 800-50	Building an Information Technology Security Awareness and Training Program	October 2003
SP 800-42	Guideline on Network Security Testing	October 2003
SP 800-38C	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality	May 2004
SP 800-37	Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems	May 2004
SP 800-27 Rev A	Engineering Principles for Information Technology Security (A Baseline for Achieving Security)	July 2004

DRAFT NIST SPECIAL PUBLICATIONS

SP 800-72	Guidelines on PDA Forensics	August 2004
SP 800-70	Security Configuration Checklists Program for IT Products	July 2004
SP 800-68	Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist	June 2004
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule	May 2004
SP 800-65	Integrating Security into the Capital Planning and Investment Control Process	July 2004
SP 800-58	Security Considerations for Voice Over IP Systems	May 2004
SP 800-53	Recommended Security Controls for Federal Information Systems	October 2003
SP 800-52	Guidelines on the Selection and Use of Transport Layer Security	September 2004

FEDERAL INFORMATION PROCESSING STANDARDS

FIPS 199	Standards for Security Categorization of Federal Information and Information Systems	February 2004
----------	--	---------------

NIST INTERAGENCY REPORTS

NIST IR 7111	Computer Security Division - 2003 Annual Report	April 04
NIST IR 7100	PDA Forensic Tools: An Overview and Analysis	August 04
NIST IR 7056	Card Technology Development and Gap Analysis Interagency Report	December 03

INFORMATION TECHNOLOGY LABORATORY BULLETINS WRITTEN BY THE CSD

October 2003	Information Technology Security Awareness, Training, Education, and Certification
November 2003	Network Security Testing
December 2003	Security Considerations in the Information System Development Life Cycle
January 2004	Computer Security Incidents: Assessing, Managing, And Controlling The Risks
March 2004	Federal Information Processing Standard (FIPS) 199, Standards For Security Categorization Of Federal Information And Information Systems
April 2004	Selecting Information Technology Security Products
May 2004	Guide For The Security Certification And Accreditation Of Federal Information Systems
June 2004	Information Technology Security Services: How To Select, Implement, And Manage
July 2004	Guide For Mapping Types Of Information And Information Systems To Security Categories
August 2004	Electronic Authentication: Guidance For Selecting Secure Techniques
September 2004	Information Security Within the System Development Life Cycle

Ways to Engage Our Division and NIST

GUEST RESEARCH INTERNSHIPS AT NIST

Opportunities are available at NIST for 6 to 24-month internships within the CSD. Qualified individuals should contact the CSD, provide a statement of qualifications and indicate the area of work that is of interest. Generally speaking, the salary costs are borne by the sponsoring institution; however, in some cases, these guest research internships carry a small monthly stipend paid by NIST. For further information, contact Mr. Ed Roback, (301) 975-2934, edward.roback@nist.gov.

DETAILS AT NIST FOR GOVERNMENT OR MILITARY PERSONNEL

Opportunities are available at NIST for 6- to 24-month details at NIST in the CSD. Qualified individuals should contact the CSD, provide a statement of qualifications and indicate the area of work that is of interest. Generally speaking, the salary costs are borne by the sponsoring agency; however, in some cases, agency salary costs may be reimbursed by NIST. For further information, contact Mr. Ed Roback, (301) 975-2934, edward.roback@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, no kidding, 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*

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

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

Technology Administration
Phillip J. Bond, *Under Secretary for Technology*

National Institute of Standards and Technology
Hratch Semerjian, *Acting Director*

NIST IR 7219
April 2005

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

AUTHORIZATION GUIDELINES

Verification

LIFECYCLE

111011100101101001000101100110101010101010111
111011100100010100010110101010101010111
1100000100000000