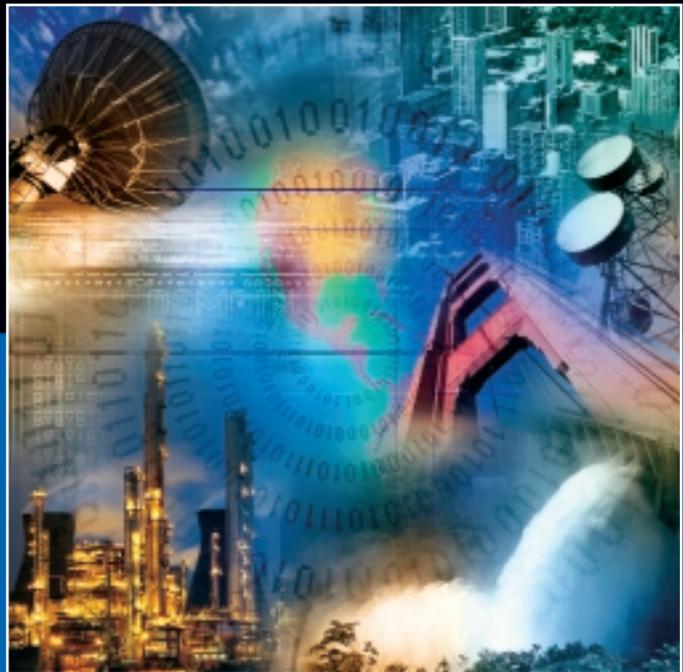


# CRITICAL INFRASTRUCTURE PROTECTION



WORKING TOGETHER WITH INDUSTRY  
AND GOVERNMENT TO PROTECT OUR  
NATION'S INFORMATION SYSTEMS



Securing our nation's information systems for critical infrastructure has become even more important in light of Sept. 11. As stated in the Executive Order on Critical Infrastructure Protection in the Information Age: *Protection of these systems is essential to the telecommunications, energy, financial services, manufacturing, water, transportation, healthcare, and emergency services sectors.*

Many organizations, both inside and outside of the federal government, have important roles to play to ensure that our nation can operate under times of stress. Owners and operators of the supporting infrastructures and developers of the technology deployed to operate the infrastructures are all involved, along with the research community, which is developing new approaches to security for these complex systems. In the area of security standards and testing, the National Institute of Standards and Technology (NIST) is helping to protect the nation's critical infrastructures, consistent with its overall mission and long-standing security responsibilities in information technology (IT).

NIST recognizes that government and the private sector share common security requirements. Commercial products that implement standards and provide security assurance to users are needed. To meet these needs, NIST works with industry, federal agencies, testing organizations, standards groups, academia, and private sector users. Cooperation and collaboration are essential to solve many common problems facing users throughout the country.

## NIST'S IT SECURITY ROLE

NIST is improving IT and critical infrastructure security by raising awareness of the need for cost-effective security, engaging in voluntary standards activities, developing standards and guidelines, and providing national leadership for security evaluation and testing. NIST has two vital and unique roles. The first is supporting federal departments and agencies under the Computer Security Act of 1987 and follow-on legislation, which assign to NIST responsibility to develop security standards and guidelines for sensitive federal systems. The second is helping vendors build products and users assemble systems that will protect information and improve security. By working with IT vendors and users to develop security standards and security testing programs, NIST helps strengthen the security of commercial products, which provide the communications and information processing backbone of our infrastructures. Moreover, NIST's efforts to enhance the security of products support users' confidence in their systems and networks, thus enabling more widespread and secure infrastructures supporting e-government and e-commerce.

## STANDARDS

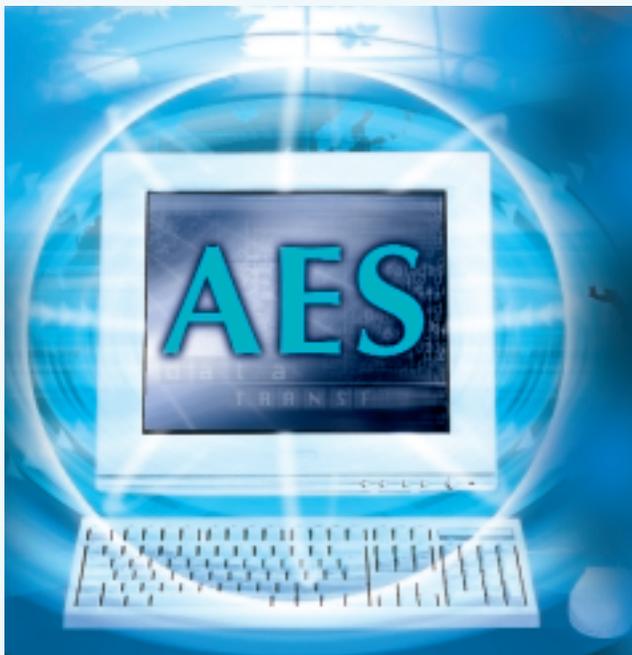
NIST works with industry to develop voluntary industry standards that support security, interoperability, and data exchange. Such standards are widely used to support the operation of the Internet. NIST participants contribute their expertise and neutrality to formulate public specifications that enable industry to improve the security and competitiveness of commercial products and help users to be informed consumers when specifying their requirements. Stronger security specifications, when



correctly implemented and deployed, strengthen our nation's infrastructures.

One area of particular concentration is the development of cryptographic-based standards. A highly complex mathematics-based technology, cryptography is a critical component needed to support and protect our infrastructures. Cryptographic standards include the algorithms used to encrypt and decrypt information, and for other security functions such as digital signatures, authentication, and key exchanges. Electronic activities are increasing daily, affecting people worldwide, and strong security technology is needed to encourage continued growth and success.

**Advanced Encryption Standard.** NIST has been particularly successful in its development of the Advanced Encryption Standard (AES), which provides a highly efficient and secure means to encrypt information. A worldwide, multiyear project was conducted to develop



a new technical standard to replace the aging Data Encryption Standard, first adopted in 1977, which has been widely used by government and industry. AES will be used to protect a wide variety of federal information (e.g., tax and social security records), as well as sensitive commercial data (e.g., financial and healthcare records) throughout the world. NIST fully expects AES, as adopted in Federal Information Processing Standard (FIPS) 197, to become the dominant worldwide encryption standard.

*See: <http://csrc.nist.gov/encryption/aes/>*

**Digital Signatures.** NIST supports the development of other high-quality cryptographic technology standards through participation in formal voluntary standards community activities. Standards for digital signatures are needed to authenticate electronic information and transactions and to assure high levels of integrity of information. Several techniques have already been endorsed for industry and government use by the American National Standards Institute (ANSI). NIST is pursuing the enhancement of these techniques to provide security levels commensurate with those of the Advanced Encryption Standard (AES).

*See: <http://csrc.nist.gov/encryption/tkdigsigs.html>*

**Public Key Infrastructure.** One of the principal means by which cryptographic mechanisms will be efficiently deployed is via use of Public Key Infrastructure (PKI) technology. PKI refers to the issuance, distribution, and binding of the keys and other necessary information to enable the use of digital signatures, or other forms of public-key cryptography. NIST is actively working in this area to spur the development of needed standards and their deployment within the federal government in support



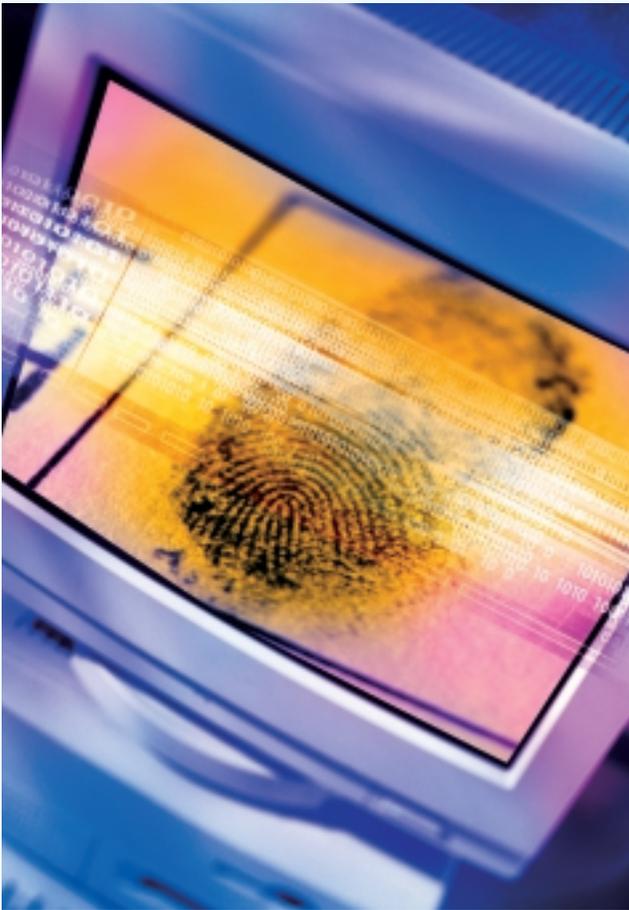
of e-government activities. PKI can speed up and simplify delivery of products and services by providing electronic processes to replace paper-based approval processes. For example, signing a purchase order can be accomplished electronically with digital signatures. They can provide a mathematically infinitesimal risk of forgery, provided the user's signature key is protected and linked to its owner. This is done through the use of "certificates" that bind cryptographic keys and other security information to specific users or entities in the network.

*See: <http://csrc.nist.gov/pki/>*

**Biometrics.** The use of biometrics — automated methods of recognizing a person based on a physiological or behavioral characteristic — can provide higher levels of security in personal identification and verification applications. NIST has been working to improve biometric standards and technologies, which include testing and evaluation methods for recognition technologies — fingerprint and facial — and interoperable authentication systems. NIST and the National Security Agency co-chair the Biometric Consortium, a focal point for research, development, testing, evaluation, and application of biometric-based technologies. The consortium consists of over 800 members from government, industry, and academia.

*See: <http://www.nist.gov/biometrics>*

**Internet Infrastructure.** NIST is engaged in a series of projects aimed at protecting the Internet infrastructure from cyberterrorism, particularly the security of the domain name system (DNS). A critical component, DNS is a globally distributed database that provides two-way mappings between names (e.g., [www.nist.gov](http://www.nist.gov)) and Internet addresses. Malicious parties could impersonate DNS zones



and redirect network traffic away from the user's intended destination. In collaboration with industry partners, NIST is working to expedite the standardization and commercial adoption of technical security specifications aimed at strengthening the DNS.

*See: <http://www.antd.nist.gov/dnssec/>*

**Computer Forensics.** Computers are being used as tools in criminal activities. To aid investigators and law enforcement personnel, NIST has developed a software tool, the **National Software Reference Library**, which allows a comparison of potentially altered desktop computer files against legitimate ones contained in the library. Reducing



search time dramatically, this automated program presents investigators with files that may require further scrutiny. NIST is also developing tests and a testing framework under its Computer Forensics Tool Testing project that will enable an evaluation of commercially available products for use in forensic examinations.

See: <http://www.nsr1.nist.gov>

## TESTING

Standards enable users to identify security specifications appropriate for their needs and provide a quick way to express their requirements to vendors. Unfortunately many of today's IT products in the marketplace do not implement security standards correctly — when appropriate standards exist — or contain vulnerabilities that are discovered only after the product's commercial release. This leads to an almost never-ending stream of security patches, which must be installed by users or system administrators, at some inconvenience and security risk, to patch vulnerabilities known to be exploitable by hackers. If such patches are installed improperly or not at all, the system remains vulnerable.

Testing addresses these risks and can reduce the need and cost of such patching. Testing of products gives users and vendors confidence that security standards and specifications have been correctly implemented in new products. Testing also helps reduce the potential for products containing vulnerabilities that could be used to attack systems. NIST develops tests, tools, profiles, implementations, and recommendations for timely and cost-effective testing programs. IT security validation programs developed by NIST are conducted in cooperation with the private sector testing laboratories.

Security testing, however, is not an exact science. Very complex products may contain millions of lines of computer code. Extensive testing of such code in a timely manner to meet vendors' time-to-market requirements requires significant additional research. Moreover, there are many research challenges remaining to be addressed when individual products are linked together in whole systems and in large network infrastructures.

### **Cryptographic Module Validation Program (CMVP).**

Created by NIST and the Communications Security Establishment of the Government of Canada in 1995, the CMVP provides validation testing for cryptographic modules and for federally recognized algorithms that are implemented in the modules. Testing of algorithms for conformance to standards determines whether a product faithfully implements the specification and raises the confidence of developers and users in product quality. By helping to ensure that cryptography is correctly and securely implemented, the CMVP aids the security of our infrastructures. Private sector laboratories, accredited by NIST, perform the testing. Validated products are then included in directories maintained by NIST and available for public access.

See: <http://csrc.nist.gov/cryptval/>

### **National Information Assurance Partnership (NIAP).**

A collaboration between NIST and the National Security Agency, NIAP is designed to meet the security testing, evaluation, and assessment needs of IT producers and consumers alike through cost-effective programs. The partnership, originated in 1997, combines the extensive security experience of both agencies to promote the development of technically sound security requirements for IT products and systems and appropriate metrics for



evaluating them. Important constituencies such as the healthcare sector and telecommunications industry have developed security specifications in collaboration with NIAP. The private sector has brought important technologies, such as firewalls, smart cards, operating systems, and databases, into NIAP laboratories for security evaluation.

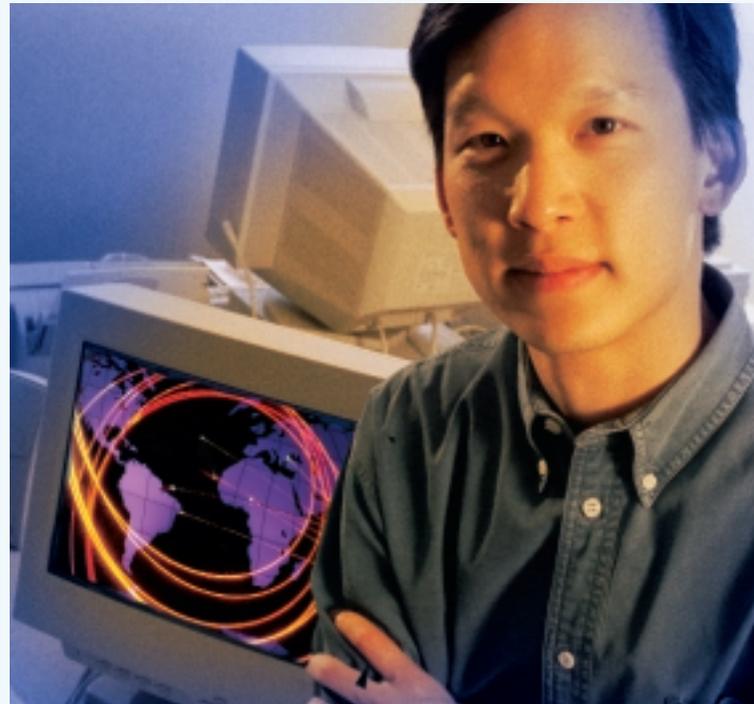
The long-term goal of NIAP is to increase the level of trust consumers have in their information systems and networks — and thereby the nation’s infrastructures. NIAP uses NIST-accredited private sector laboratories to accomplish its security evaluations, which are conducted using specifications based on the ISO/IEC 15408 (Common Criteria for IT Security).

To date, fourteen countries recognize results from the NIAP-sponsored IT security testing program as part of an international mutual recognition arrangement recently negotiated and signed by the U.S. Government and other key foreign governments. This reduces the costs of testing to U.S. companies and the barriers to their acceptance in foreign countries. NIAP continues to build important relationships with government agencies and industry in a variety of areas to help meet current and future security challenges affecting the nation's critical information infrastructure.

See <http://niap.nist.gov/>

## GUIDELINES

The key to strengthening the nation’s critical infrastructure and better securing information assets from cyber threats and other types of abuse is development and dissemination of guidelines to assist government agencies



in the selection and implementation of technology. Technology alone will not solve most security problems. Issues of correct installation, ongoing configuration management, and proper integration are all important components of a comprehensive equation. In addition, strong monitoring and compliance methodologies are essential in proper identification and containment of threats against the network infrastructure.

NIST advocates taking a holistic view of information security, which addresses the entire life cycle of a system including management, operational, and technical controls. NIST’s current publications address a number of topics, such as computer security basics, sensitive system planning, security training and awareness requirements, risk management, telecommunications and network security, Internet security, firewall implementation,



incident handling techniques, and security program assessment strategy.

Guidelines on good security practice for management, users, and technical support personnel are essential elements in maximizing the strength of the human interface. This has often been noted as the weakest link in security. Both the human interface and the supporting technology must be effective to enable quick identification and elimination of existing and emerging threats.

*See <http://csrc.nist.gov/publications/>*

#### **Information Technology Laboratory (ITL) Bulletins.**

ITL bulletins are designed to raise awareness about the risks, vulnerabilities and requirements of new technologies used for protection of our critical infrastructures.

Some recent topics include: Engineering Principles for Information Technology Security, Biometrics - Technologies for Highly Secure Personal Authentication, Guidelines on Firewalls and Firewall Policy, and Risk Management Guidance for Information Technology Systems.

*See: <http://csrc.nist.gov/publications/nistbul/index.html>*

## A W A R E N E S S

In addition to guidelines, NIST offers a number of programs and resources designed to raise awareness of the need for security across industry and government.

**Computer Security Resource Center.** NIST maintains a security Web site, the Computer Security Resource Center (CSRC), which provides easily accessible information to

users, vendors, agencies, organizations, and individuals. CSRC provides timely, up-to-date information on significant security issues.

*See <http://csrc.nist.gov>*

**Vulnerability and Patch Information.** Many software programs contain vulnerabilities that can be easily exploited to gain unauthorized access to sensitive systems and information used in the operation of the nation's infrastructures. In order to protect a system, a system manager/operator must first be aware of the vulnerabilities and then patch or replace the software on a timely basis to minimize the threat from intruders. This is challenging since new vulnerabilities in various IT programs are found daily.

NIST has developed a user-friendly tool service known as ICAT to assist managers/operators. ICAT provides a Web-based searchable index of computer vulnerabilities and links users into a variety of publicly available vulnerability databases and patch sites. This enables users to find and fix the vulnerabilities existing on their systems.

ICAT allows searching at a fine granularity, a feature unavailable with most vulnerability databases, characterizing each vulnerability by over 40 attributes (including software name and version number). ICAT indexes the information available in Computer Emergency Response Team advisories, ISS X-Force, Security Focus, NT Bugtraq, Bugtraq, and a variety of vendor security and patch bulletins.

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



### **Federal Computer Security Program Managers’**

**Forum.** In support of protecting the federal government’s own systems and in promoting secure e-government, NIST hosts and sponsors information-sharing through the Federal Computer Security Program Managers’ Forum.

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

### **IT Security Seminars for Small and Medium-Sized Businesses.**

Large organizations have justified and committed considerable time and resources to implementing effective information security programs. However, small to medium-sized businesses cannot always justify an extensive security program, or a single 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 cost-effective security mechanisms and obtain practical training. Such organizations need sufficient information to be educated purchasers and users of security technology and services, so that their limited security resources are well applied to meet the most obvious and serious threats.

In order to give these businesses a head start, NIST, in co-sponsorship with the Small Business Administration and the National Infrastructure Protection Center’s InfraGard program, is conducting a series of one-day security seminars specially designed for them. Security experts 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 IT personnel can apply directly or use to task contractor personnel.

*See: [http://csrc.nist.gov/Bus\\_Regional\\_Mtgs](http://csrc.nist.gov/Bus_Regional_Mtgs)*

### **Computer Security Expert Assist Team (CSEAT).**

NIST’s CSEAT was established to improve federal critical infrastructure protection planning and implementation efforts by assisting governmental entities in improving the security of their IT assets. CSEAT accomplishes this by performing a review of an agency’s computer 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 roadmap to cost-effectively enhance the protection of the information system assets. Each agency must implement and maintain an active information technology security program that adequately secures agency information assets. An agency’s IT security program must:

- 1) assure that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability; and
- 2) protect information commensurate with the level of risk and magnitude of harm resulting from the information’s loss, misuse, unauthorized access, or modification.

*CSEAT review reports provide recommendations relative to:*

- ◆ computer security management and culture
- ◆ computer security plans
- ◆ computer security training, awareness, and education
- ◆ budget and resources
- ◆ life cycle management
- ◆ incident and emergency response
- ◆ IT security controls
- ◆ physical security
- ◆ operational security controls

*See <http://cseat.nist.gov/>*



## ELECTRIC POWER AND INDUSTRIAL CONTROL SYSTEM SECURITY

The widespread use of IT for remote monitoring and control of the electric power system and for controlling industrial processes in the chemical, oil and gas, pharmaceutical, food and beverage, pulp and paper, and other process control industries has unintentionally introduced security vulnerabilities. These systems have been designed solely on a functional basis where real-time response and operational flexibility are the major design drivers. Because security issues have not been addressed, there are weaknesses that potentially can be exploited to:

- ◆ Disrupt the electric power system resulting in blackouts
- ◆ Give independent power generators unfair advantage over competitors
- ◆ Harm personnel and capital facilities
- ◆ Endanger public health and safety
- ◆ Cause loss of production and economic disruption

NIST is working with EPRI, the research arm of the electric power industry, to identify where these weaknesses exist and to develop security requirements for the real-time systems that control the power grid and critical industrial production processes. A NIAP Process Control Security Requirements Forum has been established to:

- ◆ Identify and assess threats and risks to process control information and functions
- ◆ Make and promote adoption of security requirements recommendations
- ◆ Promote security awareness and integration of security considerations in the life cycle of electric power and industrial process control systems

NIST is also working with the Institute of Electrical and Electronics Engineers (IEEE), the International Electrotechnical Commission (IEC), and the Instrumentation Systems and Automation Society (ISA) to incorporate security requirements into the standards relevant to control of electric power and industrial control systems.

See: <http://www.isd.mel.nist.gov/projects/processcontrol>



## BUILDING AUTOMATION AND CONTROL SYSTEMS PROTECTION

Building automation and control systems used for heating, ventilating and air-conditioning, fire alarm systems, lighting control systems, access control, and vertical transport are increasingly being integrated with each other and with IT networks used by business management. Control systems in multiple buildings are being connected over wide area networks, and in the near future, buildings will exchange information directly with utility providers, service companies, and emergency response organizations. NIST is working in the following three areas to protect integrated building systems and services.

**Extension of BACnet®.** NIST is working to extend BACnet®, a Data Communication Protocol for Building Automation and Control Networks developed by the

American Society of Heating, Refrigeration and Air-Conditioning Engineers (ASHRAE) with NIST help, to provide secure information transfer between the control of integrated building systems and services. Current activities include assuring: **1)** the security of life safety and access control systems in an integrated building system environment, **2)** secure interactions between building control systems and utility providers, and **3)** secure interconnection of building control systems using BACnet®/IP and BACnet® Annex H tunneling routers.

**Research Using the Virtual Cybernetic Building Testbed.** NIST has developed a Virtual Cybernetic Building Testbed, a facility that combines real commercial building control products with simulated building systems, to study the interactions of these systems and to develop appropriate security techniques. This work is being conducted in cooperation with industry partners and both



national and international standards bodies. The work involves customizing existing security tools to building control applications, developing security enhancements for existing national and international standards for building control systems, developing best practice guidelines, and exploring the information exchange and security needs of future applications for integration of building systems with outside entities.

**Research In Real Facilities.** NIST is also working with the General Services Administration (GSA), the State of Iowa, and the Architect of the Capitol to implement security features in large-scale BACnet systems. For GSA, this is part of the GSA Energy Management Network (GEMnet), which currently connects twelve buildings in the Southwest and will eventually expand to include all GSA buildings in that area. In Iowa, the Smart Buildings Demonstration project is linking Army National Guard facilities across the state. On Capitol Hill, NIST is assisting on a project that involves replacing in stages the building control systems in many high-profile buildings.

See: [http://www.bfrl.nist.gov/goals\\_programs/02prgmCBS.htm](http://www.bfrl.nist.gov/goals_programs/02prgmCBS.htm)

## EXPLORING NEW TECHNOLOGIES

NIST conducts research to identify the security risks and opportunities of new information technologies. This research leads to the development of models, reference implementations, and demonstrations. Experience gained enables NIST scientists to provide advice to the public and private sectors on securely using technologies, such as intrusion detection, access control, Internet Protocol Security, mobile agents, and on building the

architecture for future systems. This research enables NIST to find cost-effective ways to implement and address government security requirements.

See: [http://csrc.nist.gov/focus\\_areas.html#research](http://csrc.nist.gov/focus_areas.html#research)

**Advanced Technology Program (ATP).** This program provides cost-shared funding to companies (and universities and nonprofits) for high-risk, high-payoff R&D in new technologies. Through partnerships with the private sector, ATP's early-stage investment is accelerating the development of innovative technologies that promise significant commercial payoffs and widespread benefits for the nation.

Proposals in the area of dependable computing systems (security and reliability) continue to be received and evaluated by ATP. In some cases they involve stand-alone hardware/software systems, and in other cases, security-related tasks are included in a larger overall project. This includes research and prototype development of products, tools, and services to enable the creation and maintenance of highly dependable computer systems and networked applications. Technical areas include, but are not limited to, Automatic Problem Diagnostic and Repair Tools, Biometrics, Business to Business/Consumer Security, Cryptographic Toolkits, Encryption Systems, Fail-Safe Designs, Fault Tolerant Systems, Internet Security, Mobile Agent Security, Module Validation, System and Network Testing Tools and Services.

See: <http://atp.nist.gov/itao/directions.htm>

**NIST**

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

**May 2002**