COMMITTEE ON NATIONAL SECURITY SYSTEMS
CNSS
SYSTEMS SECURITY FOR THE 21st CENTURY

2007/2008 CNSS Report

An Agenda for Safeguarding National Security Systems

DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

MAR 10 2008

Pursuant to National Security Directive 42, the department is pleased to present to you the *2007/2008 Committee on National Security Systems (CNSS) Report: An Agenda for Safeguarding National Security Systems* describing recent strategic accomplishments of the CNSS and individual Federal departments and agencies, along with priorities for 2008.

The CNSS performs the vital function of mobilizing the full, interagency National Security Community for the protection of telecommunications and information systems that support U.S. national security. The CNSS works in close partnership with the private sector and key allied nations to develop and implement policies, execute critical programs, and perform essential technical services to strengthen the security of information and communication systems. This report describes the strong, cross-government impact of the Committee and individual Federal departments and agencies in promoting assured information sharing; managing risk; facilitating identity assurance; ensuring network resilience for mission assurance; and building and sustaining a superior information assurance workforce.

For 2008, the Committee has outlined an ambitious agenda consistent with the Administration's *National Strategy to Secure Cyberspace* and closely aligned with the *National Strategy for Information Sharing.* CNSS priorities for 2008 also support your national cyber security initiative and focus on increasing the level of trust in national security systems, protecting them from our adversaries, and making certain that mission essential functions can be performed in the increasingly hostile cyber environment.

The CNSS will continue to work closely with the interagency community and its partners to improve the defense of our national security systems and critical infrastructure from cyber attack.

DEPARTMENT OF STATE
UNITED STATES OF AMERICA
DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA
DEPARTMENT OF COMMERCE
UNITED STATES OF AMERICA
DEPARTMENT OF ENERGY
UNITED STATES OF AMERICA
THE DEPARTMENT OF THE TREASURY
1789
DEPARTMENT OF JUSTICE
DEPARTMENT OF TRANSPORTATION
UNITED STATES OF AMERICA
U.S. DEPARTMENT OF HOMELAND SECURITY
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
GENERAL SERVICES ADMINISTRATION
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
UNITED STATES OF AMERICA
DEPARTMENT OF THE ARMY
UNITED STATES OF AMERICA
DEPARTMENT OF THE AIR FORCE
UNITED STATES OF AMERICA
CENTRAL INTELLIGENCE AGENCY
UNITED STATES OF AMERICA
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
DEPARTMENT OF THE NAVY
UNITED STATES OF AMERICA
DEPARTMENT OF THE NAVY
UNITED STATES MARINE CORPS
DEFENSE INTELLIGENCE AGENCY
UNITED STATES OF AMERICA

Overview

In 2007, the work of the Committee on National Security Systems (CNSS) grew in importance with the continuing impact of the proliferation of cyberspace threats to national security systems, greater integration among Federal departments and agencies in the conduct of national security missions, and increasing reliance on telecommunications and information systems to support national security missions. The CNSS and its individual Federal departments and agencies focused on five key national goals to enhance the security of national security systems—(1) assured information sharing; (2) managing risk; (3) identity assurance; (4) network resilience for mission assurance; and (5) building and sustaining a superior information assurance (IA) workforce. Four major accomplishments stand out in 2007—

- The CNSS approved over 60 requests to release IA products and services to our foreign partners, thereby facilitating secure communication and information exchange between the United States and our allies.

- In March 2007, CNSS issued Policy Number 12, *National IA Policy for Space Systems Used to Support National Security Missions,* which has already improved the security of commercial communications satellite assets.

- The CNSS led the establishment of Government-wide efforts to address the risk of supply chain attacks to national security systems and other critical government and private sector systems and networks stemming from globalization and offshore development of information systems and communications technologies, products, and services. The CNSS set the vision for supply chain lifecycle risk management efforts across the Federal Government in its 2006 report, *Framework for Lifecycle Risk Mitigation for National Security Systems in the Era of Globalization: A Defense-in-Breadth Approach.*

- CNSS training and education standards provided the foundation for developing the next generation of IA professionals. By the end of 2007, 169 government, academic, and private sector institutions in 42 states had embraced CNSS standards that support the National Centers of Academic Excellence in IA Education and contributed a widening stream of workforce-ready IA professionals.

Building on its long legacy of achievement, the CNSS continued to promote a common purpose within the National Security Community and to foster partnerships with the private sector, academia, other councils and committees, and our allies. These efforts have enabled the vital sharing of talents, knowledge, and practices for protecting our national security systems.

The *2007/2008 CNSS Report: An Agenda for Safeguarding National Security Systems* illuminates the challenges, priorities, and accomplishments in assuring the security of national security systems and promotes further public and private sector collaboration on this important national security endeavor.

Sincerely,

John G. Grimes

John G. Grimes
Chair
Committee on National Security Systems

At a Glance

The Committee on National Security Systems (CNSS) represents the National Security Community of the Federal Government—comprised of 21 Members and 10 Observers—in the protection of telecommunications and information systems that support U.S. national security. In 2007, the CNSS and its individual Federal departments and agencies made significant contributions that enhanced the overall security of the Nation, benefited users of national security systems (NSS), and shaped priorities for 2008 across five areas that the Nation must continue to focus on to achieve national security objectives.

Assured Information Sharing

Available, trustworthy data; secrets kept from adversaries; seamless collaboration with national security partners

2007 Accomplishments

- **Secure personal electronic devices**—New secure portable electronic devices revolutionized the way information is shared and enabled e-mail and Web browsing from unclassified through Secret and telephone calls from unclassified through Top Secret
- **Cross-domain solutions**—A newly established joint Department of Defense (DoD) and Office of the Director of National Intelligence (ODNI) office identified best solutions for sharing information across classification domains

2008 Priorities

- Issue a process to implement solutions for sharing information across classification domains
- Further deploy secure portable electronic devices to promote secure, highly mobile leadership communications

Managing Risk

Common approach to assessing risk that promotes trust among system owners; measurable security

2007 Accomplishments

- **Supply chain risk management**—For the first time, a strategy was developed to guide efforts to counter threats posed by adversaries who seek to infiltrate the production of hardware and software upon which we rely
- **Certification and Accreditation (C&A) Transformation**—A joint DoD and ODNI activity supported by the CNSS laid out a common community approach that will reduce the time to perform C&A and improve interoperability and sharing

2008 Priorities

- Implement and operationalize common methodologies and processes for C&A, risk assessment, and supply chain risk management throughout the Federal Government

Identity Assurance

Accountable information flow made possible through the ability to identify and authenticate people and devices

2007 Accomplishments

- **Adoption of identity assurance technologies**—Measurably fewer intrusions were seen in DoD unclassified networks as a result of widespread use of Common Access Cards
- **Federal agency interoperability**—Illinois became the first state to be certified under the Federal Public Key Infrastructure (PKI) architecture; Federal identity credentialing moved us closer to operation as "one government"

2008 Priorities

- Expand PKI architectures to additional communities of interest to promote greater interoperability; leverage biometrics and other technologies to strengthen identification
- Operationalize an attribute-based access control capability across the Federal Government to improve both access control and information sharing

The CNSS and its Member organizations are advancing our ability to manage mission, system, information, and infrastructure risks. Safeguarding NSS is a shared responsibility. It starts with each individual user and requires each Federal Department and Agency to work together and in partnership with the private sector, academia, other organizations, and international partners to address the changing security environment. The common goal of enhancing the security of the Nation depends on all of the communities working together and in harmony to leverage effective and comprehensive solutions. CNSS brings the National Security Community together to address traditional and emerging information assurance (IA) issues and to achieve national security goals. With strong, tangible outcomes in 2007 and a prudent strategy for the future, the CNSS is well-positioned for success in the coming years.

Network Resilience for Mission Assurance

Works under fire; attacks are prevented, deflected or do little damage; operates through or recovers quickly following successful attacks.

2007 Accomplishments

- **DoD mission assurance**—DoD launched a major initiative to assure DoD missions against sophisticated, top-tier threats, which will lead to a transformation in DoD cyber operations
- **Off-the-shelf operating system security**—Defense and civilian agencies gained access to the locked-down desktop configuration for Microsoft Windows XP and Vista and can now more easily manage their enterprises and reduce vulnerabilities using a common data strategy
- **Space systems security**—CNSS issued Policy Number 12, National IA Policy for Space Systems Used to Support National Security Missions, which has already improved the security of commercial communications satellite assets

2008 Priorities

- Conduct national exercises to determine how the government and critical infrastructure owners and operators will respond to serious cyber degradation and accelerate the development of capabilities that are needed for network resilience
- Develop a government-wide vision and strategy for promoting the security and stability of the Internet as it evolves
- Implement across the National Security Community a standardized desktop configuration for the Microsoft Windows XP and Vista operating systems consistent with Office of Management and Budget guidance

Building and Sustaining a Superior IA Workforce

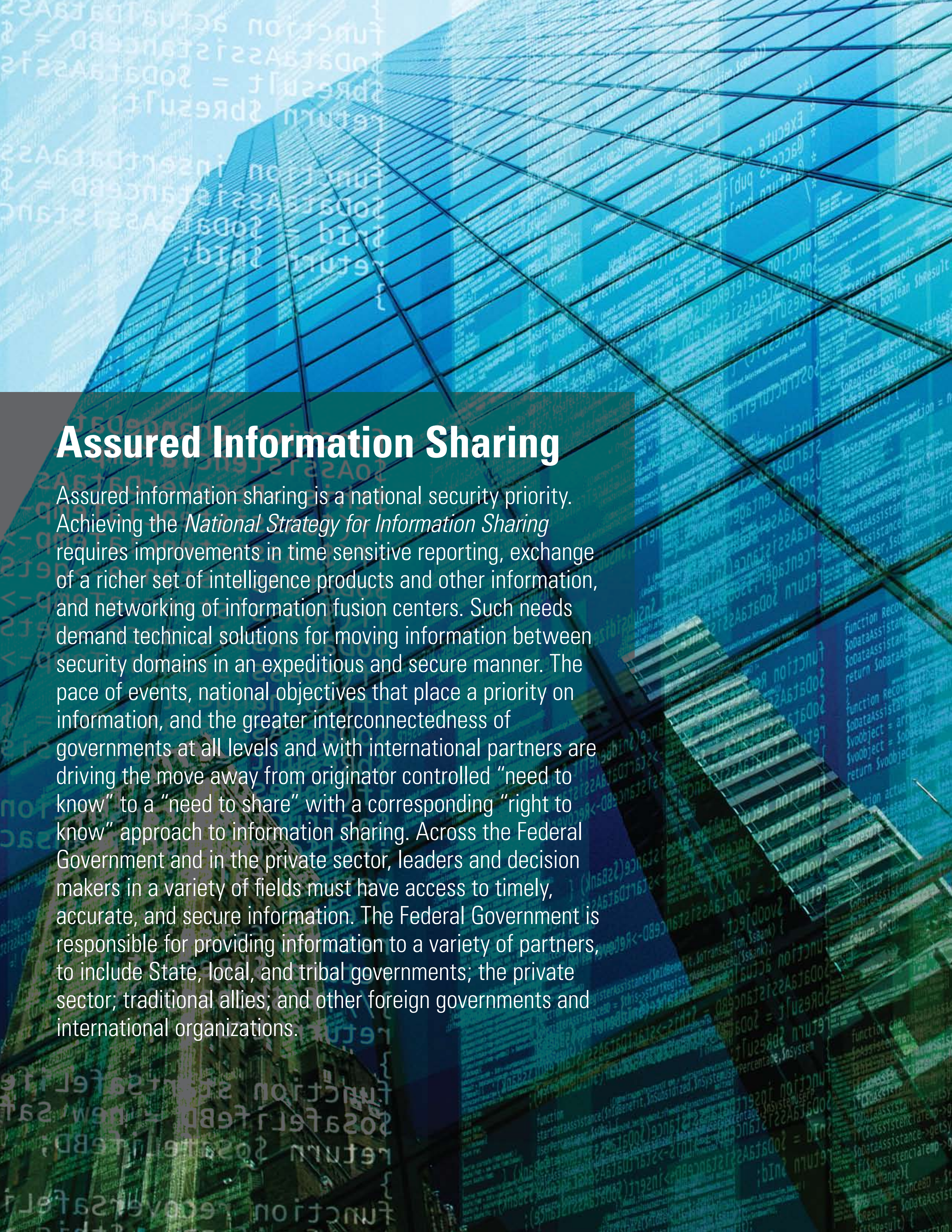
Qualified people who can defend NSS against attacks and ensure the proper use of policies, processes, and technology

2007 Accomplishments

- **Standards for IA professionals**—CNSS standards for training and education were embraced by 169 U.S. institutions providing the baseline for producing a cadre of IA professionals
- **New Centers of Academic Excellence in IA Education (CAEIAE)**—12 new universities were accredited this year, bringing the grand total to 86 approved centers; CNSS begun updating all CNSS extant training and education standards as well as developing four new ones

2008 Priorities

- Advance the use of commercial IA certification across the National Security Community as a baseline for IA knowledge and skills and promote continuous learning
- Promote innovation in IA through use of the CAEIAE to conduct leap-ahead research projects for NSS and expand the use of IA scholarships to attract and retain top IA talent to meet mission essential needs of the Federal Government



Assured Information Sharing

Assured information sharing is a national security priority. Achieving the *National Strategy for Information Sharing* requires improvements in time sensitive reporting, exchange of a richer set of intelligence products and other information, and networking of information fusion centers. Such needs demand technical solutions for moving information between security domains in an expeditious and secure manner. The pace of events, national objectives that place a priority on information, and the greater interconnectedness of governments at all levels and with international partners are driving the move away from originator controlled "need to know" to a "need to share" with a corresponding "right to know" approach to information sharing. Across the Federal Government and in the private sector, leaders and decision makers in a variety of fields must have access to timely, accurate, and secure information. The Federal Government is responsible for providing information to a variety of partners, to include State, local, and tribal governments; the private sector; traditional allies; and other foreign governments and international organizations.

Assured Information Sharing | Accomplishments

CNSS and individual Federal Department and Agency efforts have been instrumental in harnessing the power of information and ensuring that information is available where and when it is needed. CNSS supported the following in 2007—

Cross Domain Investments, Solutions, and Activities

The Office of the Director of National Intelligence (ODNI) and the Department of Defense (DoD) established the Unified Cross Domain Management Office (UCDMO), which supports assured information sharing objectives by expediting the delivery of cross domain capabilities to the field. The UCDMO provides centralized coordination and oversight of all cross domain activities and ensures that DoD and the Intelligence Community (IC) have a common approach to cross domain standards, policies, implementation, and research. It also produced a technology roadmap that sets forth the plan for achieving a unified technology base for cross domain solutions in DoD and the IC. The UCDMO published the first cross domain inventory in February 2007 with an update in July 2007. The inventory contains a list of accredited cross domain solutions (narrowed down to 15 from approximately 800) in research, development, test and evaluation and solutions to be retired. The inventory has enabled Combatant Commands, Services, and Agencies to efficiently identify and implement solutions to better meet their information sharing requirements while at the same time improving network security. UCDMO will use the CNSS to issue its cross domain policy and instructions and extend its expertise to other Federal departments and agencies.

Secure Communications and Data Protection

The National Security Agency (NSA) introduced the Secure Mobile Environment Portable Electronic Device (SME PED), which offers data protection for information sharing anytime, anywhere. SME PED allows unclassified and secure (up to the Secret level) e-mail and web browsing and unclassified and secure (up to the Top Secret level) telephone calls. The SME PED offers the homeland and national security communities, especially "on the move" users, secure communications services whenever and wherever they are needed.

Secure Voice over Internet Protocol

NSA successfully certified a Voice-over-Internet-Protocol (VoIP) telephone (*i.e.,* vIPer™) for secure voice communications up to and through the Top Secret Codeword level. The VoIP telephone is a secure Type 1 and Non-Type 1 voice product and is compatible with Secure Communications Interoperability Protocol-enabled secure telecommunications devices (*e.g.,* Secure Telephone Equipment and Secure Wireline Terminals). It supports customer requirements to move to an all Internet Protocol network and meet foreign interoperability and releasability goals, and offers the National Security Community secure VoIP communications.

Data at Rest

The CNSS provided support to the Data at Rest Tiger Team (DARTT) by shaping policy to create a new, accelerated acquisition process that makes data at rest (DAR) encryption capabilities available to the Federal Government. Led by DoD and the General Services Administration, with the participation of other Federal departments and agencies, State, local, and tribal government entities, and the North Atlantic Treaty Organization, DARTT developed Federal Government-wide Blanket Purchase Agreements.

Trustworthy Computing

The National Security Community is on the verge of achieving objectives for trustworthy computing and high assurance platforms, products, and services. Several private sector vendors are developing and promoting open, vendor-neutral, industry-standard specifications that help users and information technology (IT) administrators protect information assets from compromise and enable a more secure computing environment. CNSS Members and Observers continue to promote public and private sector trustworthy computing efforts to ensure that national security requirements for high assurance products and services are met. NSA's High Assurance Platform Program teamed with commercial partners and DoD customers to develop the first commercial workstation that supports simultaneous connection to two networks with single-level classification separation (*i.e.,* Unclassified to Secret or Secret to Top Secret). Trusted platform modules (TPM) serve as the hardware root of trust for trusted computing initiatives and are endorsed by the CNSS. Recognizing the importance of TPM, DoD required that, beginning with those procured in 2007, all new laptops and desktops must contain TPM. NSA also successfully championed new state-of-the-art cryptographic algorithms for the next generation TPM that will enable the certification of commercial off-the-shelf (COTS) products incorporating trusted computing technology to protect Federal Government classified data and communications. Because these are COTS products, these security features will be available to the private sector and State and local governments for non-NSS, which in turn increases the overall security of the Nation's networks.

Assured Information Sharing in Support of the Global War on Terrorism

The *National Strategy for Information Sharing* identifies enhancements that are needed for an improved information sharing environment to confront the threats to the Nation from terrorism. This environment will be constructed upon a foundation of trusted partnerships among all levels of government, the private sector, and our allies. To this end, the CNSS began a partnership with the Program Manager Information Sharing Environment (PM-ISE) to facilitate collaboration on policies, processes, and technology for information sharing. In addition, the CNSS continued to perform a critical role in facilitating secure communication and information exchange between the United States and our allies through the release of IA products and services to key allied nations. In 2007, CNSS approved more than 60 such releases, which directly contributed to building a collaborative and trusted information sharing environment and supported the global war on terrorism.

2008 Priorities

- Establish a single DoD/IC cross domain implementation process to promote information sharing throughout the Federal Government.
- Deploy SME PED devices to key members of the national and homeland security communities to ensure they have secure and reliable access to information.
- Expand the development and deployment of a modern cryptographic inventory through a COTS protection strategy to promote more effective information sharing with foreign and private sector partners, along with State and local governments, and users in geographically remote locations.
- Protect all sensitive unclassified data residing on critical, high value mobile computing devices and removable media, leveraging the heavily discounted DAR procurement vehicles across the National Security Community.
- Increase the number of trusted computing platforms and peripherals in the Federal Government's inventory by procuring laptops, desktops, workstations, servers, and printers with TPM.
- Enhance the partnership between the CNSS and PM-ISE to support PM-ISE architecture and common standards initiatives and implementation of the *National Strategy for Information Sharing.*

Managing Risk

A common understanding of risk must be established across the homeland and national security communities and among organizations and enterprises, taking into consideration what missions or functions are important, how they might be impacted, and what happens if they are lost or compromised. A universally accepted risk assessment methodology will provide information and system owners with confidence that the risks associated with sharing their information over interconnected systems are mutually understood and accepted. In addition, users must determine acceptable levels of risk and work to mitigate and manage the risk introduced by acquired products and services. Globalization of commercial information and communications technologies provides our adversaries increased opportunities to penetrate our supply chain to gain unauthorized access to U.S. data, alter U.S. data, or interrupt U.S. communications. Outsourcing reduces the ability to control the content and the output of the organization's activities, increasing the likelihood that vulnerabilities will be introduced into delivered products and services. The trend toward universal networking also increases our risk. Inevitably, increased functionality means increased vulnerability.

Managing Risk | Accomplishments

The CNSS and Federal departments and agencies are managing risk to NSS and related systems by introducing and operationalizing common security approaches and procedures across the enterprise that are consistent with similar guidance from the National Institute of Standards and Technology (NIST) for non-NSS; increasing the attention on supply chain risk; ensuring and preserving the integrity of IT products and services; and managing programs to ensure the National Security Community's continued access to trusted sources of hardware, software, and services. Specific accomplishments for 2007 include—

Supply Chain Risk Management

As a direct result of the CNSS report, *Framework for Lifecycle Risk Mitigation for National Security Systems in the Era of Globalization: A Defense in Breadth Approach,* the Federal Government established an interagency initiative to implement a defense-in-breadth supply chain risk management (SCRM) approach. The defense-in-breadth approach has four primary components: (1) enhancing acquisition processes and policies; (2) advancing the state-of-the-art in IT assurance; (3) identifying, developing, and implementing standards, policies, and best practices to mitigate risk; and (4) providing a robust awareness and training program. Building on the foundation and vision set by the CNSS, the interagency effort will enhance the overall security of NSS and information and communication technologies and will reduce risk at every stage of the system lifecycle by developing acquisition policy, developing lifecycle acquisition processes and guidance, and implementing an SCRM threat information sharing process across the Federal Government. The CNSS continues to drive progress by working with the Federal Chief Information Officers (CIO) Council to develop policy that ensures adequate and consistent adoption of SCRM practices in all Federal Government information and communications technologies. In addition, the CNSS is developing relevant implementing policy guidelines in anticipation of a national policy on SCRM that would apply to all Federal Government systems, including NSS.

Certification and Accreditation Transformation

Risk management is embodied in the C&A process. Organizations currently follow a variety of disparate C&A approaches and methodologies. A common, unified process will reduce the resources needed for C&A and compliance with the Federal Information Security Management Act, facilitate interconnection, and provide the trust needed for sharing information across different communities. DoD, ODNI, and CNSS are establishing a single, unified C&A process within the National Security Community as the first step toward achieving the goal of a single-unified Federal C&A process. Seven key C&A transformation objectives guide the development of a uniform and streamlined approach—

- Define and apply a common set of trust levels across the IC and DoD;
- Adopt a reciprocal environment backed by policy among the IC, DoD, and our foreign partners;
- Define and adopt a single set of security controls, using NIST Special Publication 800-53 as a starting point, for use by the IC and DoD;
- Define a common lexicon of terms, using CNSS 4009 glossary as a baseline, for establishing reuse and reciprocity across the IC and DoD;
- Look beyond individual systems or events when making risk decisions; a senior risk executive function inside IC and DoD entities bases decisions on an "enterprise" view;
- Design and operate IA within the enterprise operational environments, as a coherent whole across the IC and DoD; and
- Institute a common process for the IC and DoD incorporating security engineering within lifecycle processes.

The DoD IA C&A Process and the newly introduced IC Directive 503 offer interim policy guidance for C&A until the unified C&A policy and methodology are issued under CNSS and NIST.

Common Risk Assessment Approach

CNSS is developing a new policy for analyzing information system threats and vulnerabilities to determine the potential impact from compromised or degraded information or system capabilities. A common risk assessment approach is essential for achieving the interconnectivity required to meet the National Security Community's assured information sharing goals. A common risk assessment methodology for NSS will also provide a robust, repeatable, and more objective process than those currently in use. Similarly, for non-NSS, NIST is finalizing *Special Publication 800-39, Managing Risk from Information Systems: An Organizational Perspective.* This document will provide a disciplined, structured, flexible, extensible, and repeatable approach for managing that portion of risk resulting from the incorporation of information systems into the organization's mission and business processes. NIST and CNSS are working closely to mirror as much as possible their risk methodologies to complement the work of both communities and align them more closely to protect the Federal enterprise.

Software Assurance

The Department of Homeland Security (DHS) led development of the draft guidance document, *Software Assurance in Acquisition: Mitigating Risks to the Enterprise* that addresses some SCRM challenges by proposing an approach for integrating IA and security concerns into the acquisition process. The document reflects a consensus-based process that incorporates contributions from many public and private sector organizations. Major vendors participated in the development of the guide and are planning to adopt its principles. The guidance was released for initial public review and comment in October 2007. Individual CNSS Members and Observers also participated in the Defense Science Board on Software Assurance.

Common Vocabularies for Vulnerabilities

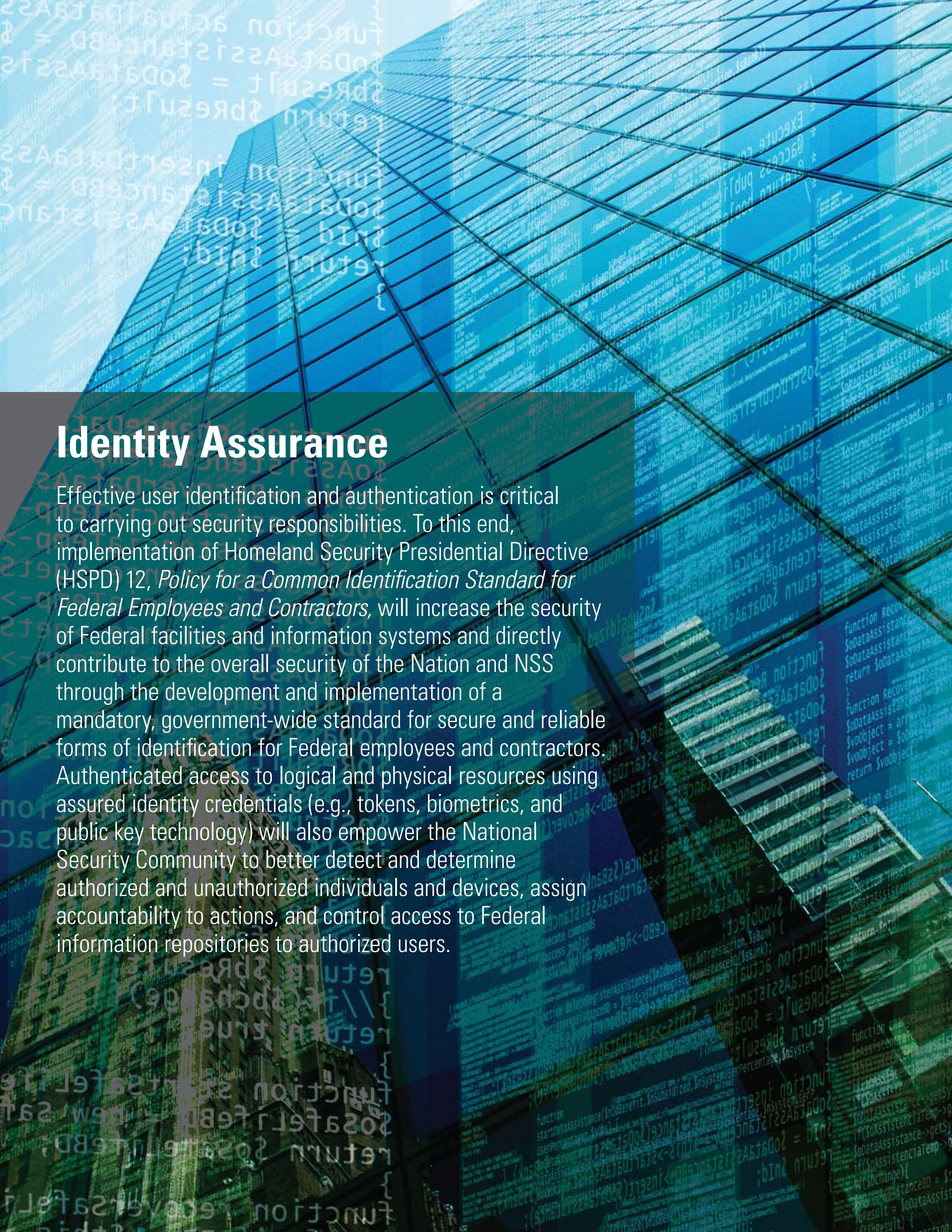
The National Vulnerabilities Database (NVD), co-sponsored by NIST and DHS and based on the Common Vulnerabilities and Exposures vulnerability naming standard, continues to offer a comprehensive cyber security vulnerability database that integrates all publicly available Government vulnerability resources and provides references to industry resources. The NVD is utilized by the Security Content Automation Protocol. In 2007, the payment card industry issued a data security standard requiring use of the NVD. Widespread use of the NVD facilitates discussion about vulnerabilities and makes it easier to identify and compare vulnerabilities across organizations and domains, further promoting activities to manage risk.

Trusted Advanced Microelectronics Products

The Trusted Access Program Office (TAPO) manages formal, trusted relationships with selected vendors and contracts with other suppliers that make it possible to better manage risk in the fabrication of classified circuits for mission critical NSS. At the leading edge of modern microelectronics technology, the TAPO oversaw in Fiscal Year 2007 the development of 334 unique new integrated circuit designs, the delivery of over 20,000 parts (chips), and the production of 3,686 wafers in support of dozens of key programs. The number of *certified* trusted integrated circuit suppliers expanded to nine, enabling the NSS community to improve the security of critical operations and information and thus help to mitigate potential risks.

2008 Priorities

- Implement a common, unified C&A process for the Federal Government and issue a CNSS policy and instructions on security controls, impact levels, and the unified certification process.
- Operationalize a common risk assessment methodology for NSS through formal policy and promote its adoption across the Federal Government through the Federal CIO Council and in partnership with NIST.
- Support supply chain risk management implementation across the Federal Government by developing acquisition policy, processes, and guidance; ensuring alignment of NSS policies and practices with Federal acquisition processes and guidance; and implementing a supply chain risk management information sharing process.
- Leverage lessons learned from DoD's Defense Trusted Integrated Circuits Strategy and the Trusted Access Program to mitigate supply chain risk to other national security mission critical system components.



Identity Assurance

Effective user identification and authentication is critical to carrying out security responsibilities. To this end, implementation of Homeland Security Presidential Directive (HSPD) 12, *Policy for a Common Identification Standard for Federal Employees and Contractors,* will increase the security of Federal facilities and information systems and directly contribute to the overall security of the Nation and NSS through the development and implementation of a mandatory, government-wide standard for secure and reliable forms of identification for Federal employees and contractors. Authenticated access to logical and physical resources using assured identity credentials (e.g., tokens, biometrics, and public key technology) will also empower the National Security Community to better detect and determine authorized and unauthorized individuals and devices, assign accountability to actions, and control access to Federal information repositories to authorized users.

Identity Assurance | Accomplishments

CNSS and Federal departments and agencies have taken action to implement technological solutions that enhance the security of NSS and non-NSS. Accomplishments for 2007 include—

E-Authentication, Federal Identity Credentialing, and the Federal Bridge

The Federal Public Key Infrastructure (PKI) Policy Authority continues to develop policy mappings; focus on advancing PKI technology through discussing and investigating proposed modifications to the system's architectural design; and make recommendations to the Federal PKI community on infrastructure and desktop solutions that will facilitate bridge-enabled certificate validation. In addition, the State of Illinois became the first state to be certified with the Federal PKI Architecture, an information system that allows a transaction to be processed where one entity accepts certificates issued by another. Progress is being made to ensure the interoperability of commercial smart cards across Federal departments and agencies. Such interoperability will support first responder use of smart cards for identity management and will facilitate access during times of crisis. Federal PKI initiatives make it easier for the National Security Community to verify and trust users with access to its networks.

Attribute-Based Access Control

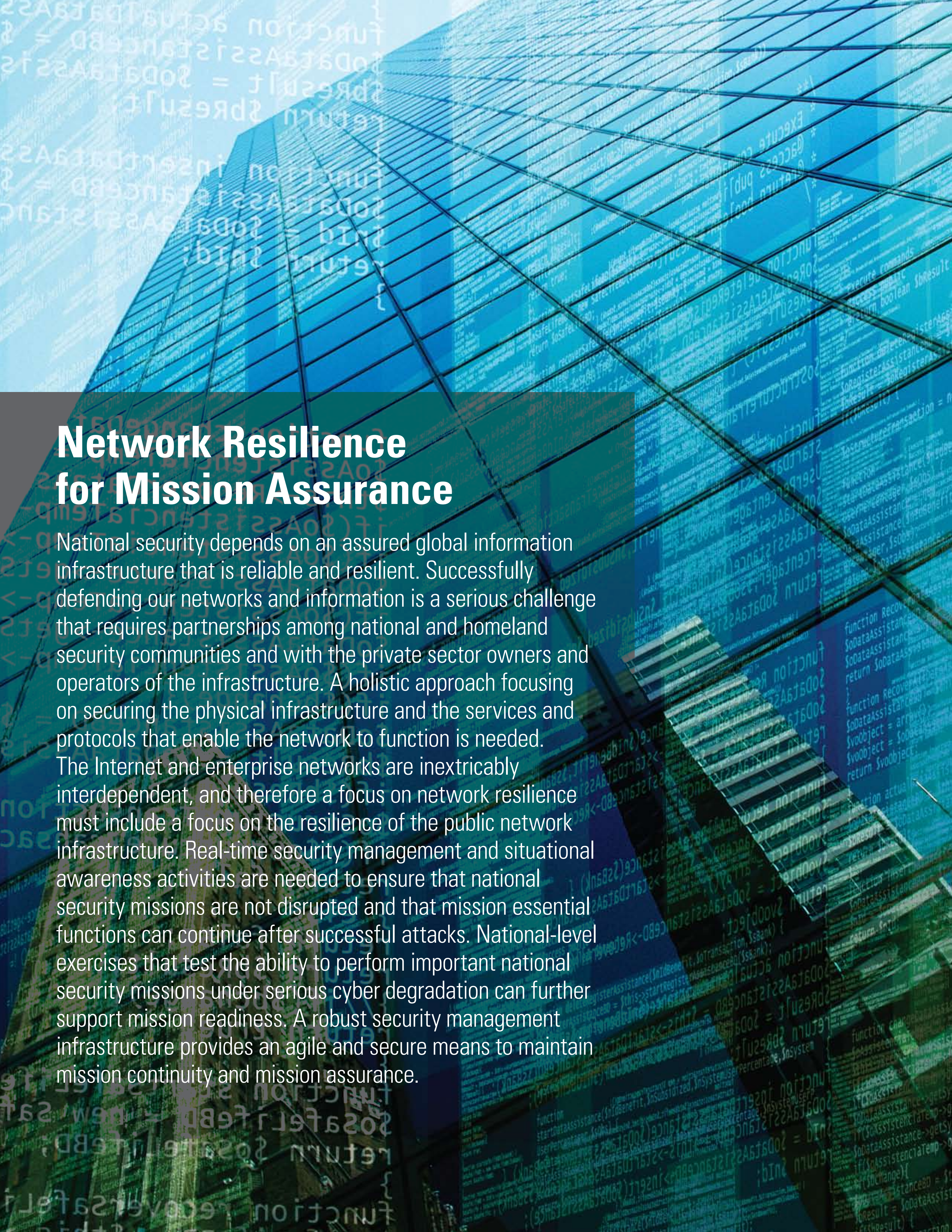
ODNI and DoD have worked collaboratively to define a common set of attributes and authoritative sources for controlling access to information based on identity. A joint ODNI and DoD working group comprised of DoD and IC representatives is developing an enterprise attribute-based access control capability to publish user attributes to information providers across all DoD and IC networks, enabling the ability to rapidly share networked information. Authorizing access based on attributes will help realize National Security Community goals for assured information sharing.

HSPD-12 Implementation

CNSS Members and Observers continue to support their respective Department and Agency efforts to implement HSPD-12 for non-NSS. DoD has in place the largest PKI and has worked to raise awareness among its workforce to meet the HSPD-12 requirements. DoD is already enjoying success; intrusions on DoD unclassified networks decreased due to the requirement that DoD users log on using Common Access Cards, which electronically verify a user's identity.

2008 Priorities

- Issue NSS identity assurance roadmap and architecture for implementing multi-factor authentication and leveraging national biometrics efforts and federated COTS solutions.
- Develop a baseline for PKI interoperability and information sharing requirements for both classified and unclassified networks and promulgate it across the Federal Government.
- Certify additional State governments with the Federal PKI architecture and partner with the private sector to promote the development of commercial smart cards for first responders and others to aid in identity assurance and facility access, especially during times of crisis.
- Expand the number of attribute-based access control pilots and extend the construct across the Federal Government.
- Establish formal policy requiring the use of biometrics in identity management for high trust level NSS.



Network Resilience for Mission Assurance

National security depends on an assured global information infrastructure that is reliable and resilient. Successfully defending our networks and information is a serious challenge that requires partnerships among national and homeland security communities and with the private sector owners and operators of the infrastructure. A holistic approach focusing on securing the physical infrastructure and the services and protocols that enable the network to function is needed. The Internet and enterprise networks are inextricably interdependent, and therefore a focus on network resilience must include a focus on the resilience of the public network infrastructure. Real-time security management and situational awareness activities are needed to ensure that national security missions are not disrupted and that mission essential functions can continue after successful attacks. National-level exercises that test the ability to perform important national security missions under serious cyber degradation can further support mission readiness. A robust security management infrastructure provides an agile and secure means to maintain mission continuity and mission assurance.

Network Resilience for Mission Assurance | Accomplishments

The CNSS and Federal departments and agencies are working in partnership with the private sector and our allies to ensure the resilience of our networks for the President, military commanders, and homeland security leaders. Accomplishments in 2007 include—

Mission Assurance

Consistent with national critical infrastructure protection objectives and the National Infrastructure Protection Plan (NIPP), DoD established the Global Information Grid (GIG) Mission Assurance Working Group to determine the failure modes and cascading affects of networks, services, and information on which critical mission essential functions depend. These findings led to four key recommendations: (1) exercise operations under sophisticated cyber attacks; (2) identify single points of failure, prioritize resources based on missions, and redesign network architectures for resilience; (3) improve command and control capability, particularly with regard to reconstitution; and (4) improve intelligence support for mission assurance. Through this effort, DoD and the National Security Community will improve its ability to react to and carry on essential missions if the GIG is disrupted, degraded, unavailable, or compromised, and will lay out a roadmap of activities to address priority needs for the future.

Critical Infrastructure Protection

Pursuant to HSPD-7 and as part of the NIPP's implementation, DHS is working closely with the IT and Communications Sectors to facilitate the continued operation and protection of the IT and Communications infrastructures. In May 2007, the IT and Communications Sectors published their respective Sector-Specific Plans describing approaches for managing sector risk; enhancing information sharing; identifying existing and future protective programs; structuring research and development priorities; and tracking progress. DHS also assists all other sectors in assessing cyber risk and addressing cyber security as part of their overall infrastructure protection efforts. Fifteen other critical infrastructure and key resource Sector-Specific Plans were also published in May 2007. These plans describe individual sector efforts to implement cyber security within and for the cyber infrastructure that they use. The infrastructure protection efforts of the IT and Communications Sectors to address cyber security, in combination with similar efforts of the other sectors, promote coordinated sector-wide approaches to managing risk and the sharing and implementation of proven cyber security practices and information, ultimately helping to ensure that the cyber infrastructure supporting NSS is reliable and resilient.

Defense Industrial Base Information Assurance

DoD is working to protect Controlled Unclassified Information (CUI)—particularly unclassified critical program information—resident on Defense Industrial Base (DIB) networks. To achieve this objective, DoD used the Critical Infrastructure Partnership Advisory Council framework to establish a partnership with industry to share cyber threat information. To complement this effort, DoD plans to establish an Information Sharing Center to interface with DIB industry members to support cyber reporting and response activities and institutionalize processes for self assessments and acquisition program damage (consequence) assessments. Through this partnership with the DIB Sector, the security of the Nation's critical infrastructure will be improved and network resilience enhanced.

Evolution of the Internet

The Internet Governance and Security Working Group (IGSWG), led by DoD, provides a forum for Federal departments and agencies to address and make recommendations on Internet policy and security issues that have the potential to impact national security. IGSWG participants were critical players in ensuring that security was substantively addressed in the Department of Commerce/Internet Corporation for Assigned Naming and Numbering Joint Project Agreement. DoD is developing an Internet Influence and Evolution Vision and Strategy to ensure that DoD equities in preserving a robust and resilient global public Internet are represented in key forums. As the Internet is an essential component of ensuring end-to-end, global, and multi-modal communications and information delivery, DoD involvement in influencing Internet security policy is essential to overall network resilience for the National Security Community.

Space Systems Security

To ensure the success of national security missions that use space systems, the CNSS issued CNSS Policy (CNSSP) No. 12 in March 2007. This policy guides the integration of IA into the planning, development, design, launch, sustained operation, and deactivation of space systems used to collect, generate, process, store, display, or transmit national security information. Although CNSSP-12 is a relatively new policy, it has already improved the security of commercial communications satellite assets that are a critical element of network resilience. Requests for compliant command uplink protections increased from five to nine in 2007. Industry seeks to comply with CNSSP-12 by accessing threat data, products, and strategies to protect space and ground assets and testing and evaluating existing systems.

National Cyber Exercises

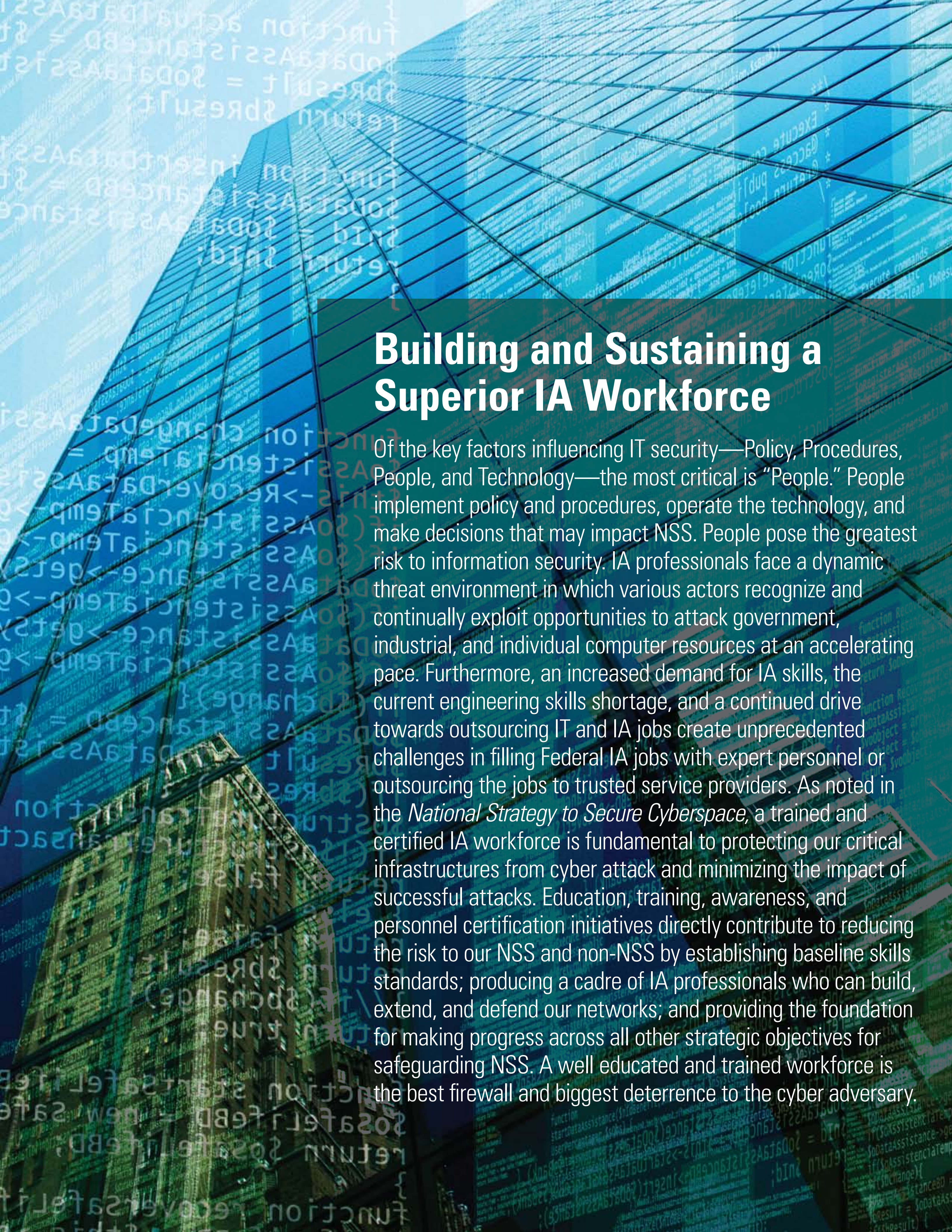
Exercises help raise awareness about the importance of security and the need for resilient networks; test policies, processes, and procedures; and build and maintain important relationships for information sharing. For example, DHS is leading the biennial National Cyber Exercise: Cyber Storm, which allows Federal, State, local, tribal, and foreign governments and private sector counterparts to address critical cyber incident response issues. Scheduled for March 2008, Cyber Storm II will enable participants (including several CNSS Members and Observers) to exercise and improve cyber incident response and coordination capabilities. Lessons learned during such exercises can demonstrate how standard configurations, common taxonomies, clear governance structures, a solid IA baseline, and information sharing will make response to cyber incidents more seamless.

Standard Security Configuration

In 2007, the Office of Management and Budget (OMB) directed civilian agencies to implement a standardized desktop configuration for the Microsoft Windows XP and Vista operating systems using specifications developed by NIST, DHS, the Defense Information Systems Agency, NSA, and Microsoft. Implementation of the standard security configuration, which is underway in DoD and other Federal departments and agencies, will allow the Federal Government to more easily manage their desktops, rapidly push patches to fix security vulnerabilities, reduce risk, and save time and resources. Implementation will also help ensure public confidence in the confidentiality, integrity, and availability of government information and improve the Nation’s ability to respond to network attacks.

2008 Priorities

- Operationalize the DoD pilot partnership with the DIB Sector to transform and dramatically improve the level of protection of CUI resident on DIB networks and support the exchange of best practices and techniques to other critical infrastructure and key resource sectors as necessary through appropriate channels.
- Through the Internet Governance and Security Working Group, develop a Government-wide strategy to address the security and stability of the Internet, including governance, authentication, technological innovation, standards, risk mitigation, and operational issues.
- Conduct national-level exercises that position the Federal Government and critical infrastructure owners and operators to demonstrate how they would operate and respond to a serious cyber degradation and increase the number of NSS exercises across key communities of interest to fully evaluate the ability to execute mission essential functions.
- Implement across the National Security Community a standardized desktop configuration for the Microsoft Windows XP and Vista operating systems consistent with OMB guidance.
- Accelerate the development of the next generation security management infrastructure to enable rapid key management and security provisioning to support a global information sharing environment and the achievement of agile missions able to reconstitute and ensure continuity of operations.
- Establish a CNSS Working Group on network resilience to identify shortfalls and potential improvements needed for network diversity and resilience to address the National Security Community’s dependency on the global information infrastructure.



Building and Sustaining a Superior IA Workforce

Of the key factors influencing IT security—Policy, Procedures, People, and Technology—the most critical is "People." People implement policy and procedures, operate the technology, and make decisions that may impact NSS. People pose the greatest risk to information security. IA professionals face a dynamic threat environment in which various actors recognize and continually exploit opportunities to attack government, industrial, and individual computer resources at an accelerating pace. Furthermore, an increased demand for IA skills, the current engineering skills shortage, and a continued drive towards outsourcing IT and IA jobs create unprecedented challenges in filling Federal IA jobs with expert personnel or outsourcing the jobs to trusted service providers. As noted in the *National Strategy to Secure Cyberspace,* a trained and certified IA workforce is fundamental to protecting our critical infrastructures from cyber attack and minimizing the impact of successful attacks. Education, training, awareness, and personnel certification initiatives directly contribute to reducing the risk to our NSS and non-NSS by establishing baseline skills standards; producing a cadre of IA professionals who can build, extend, and defend our networks; and providing the foundation for making progress across all other strategic objectives for safeguarding NSS. A well educated and trained workforce is the best firewall and biggest deterrence to the cyber adversary.

Building and Sustaining a Superior IA Workforce | Accomplishments

The CNSS and Federal departments and agencies have embraced the challenge of building and sustaining a superior IA workforce. Some of the accomplishments for 2007 include—

Training and Education Standards

The CNSS has collaboratively produced robust role-based training and education performance standards for IA professionals. As of November 2007, 169 Government, academic, and private sector institutions in 42 states and the District of Columbia have embraced the National Centers of Academic Excellence in IA Education (CAEIAE) and have formally mapped to the CNSS standards. The CNSS standards also provide the foundation for the curricula of NSA- and DHS-sponsored CAEIAE. Two other countries are considering these standards as a basis for their own programs.

National Centers of Academic Excellence in IA Education

In 2007, NSA and DHS jointly designated 12 universities as CAEIAE. Another 17 universities reapplied for designation and were successfully evaluated against strengthened criteria. As a result, there are now 86 Centers across 34 states and the District of Columbia. CAEIAE are recognized within the National Security Community and academia for their commitment to academic excellence in IA education and role in securing our Nation's information systems. Students attending CAEIAE are eligible for scholarships and grants through the DoD IA Scholarship Program and the Federal Cyber Service Scholarship for Service Program. The CAEIAE Program reduces vulnerabilities in the national information infrastructure by promoting higher education in IA and increasing the number of professionals with IA expertise in various disciplines.

Professional Certification

Some Federal departments and agencies and private sector partners are using professional certifications to make informed hiring decisions and keep workforce skills current. For example, DoD now requires all employees—active duty and reserve military, civilian personnel, including foreign nationals and contractors—who have privileged access to a DoD system, or who are involved in security management, to obtain professional certification by the end of Fiscal Year 2010. This requirement will apply to approximately 100,000 individuals. Various commercial certifications have been approved as meeting the requirement in both the managerial and technical tracks. DoD is leveraging International Organization for Standardization/International Electrotechnical Commission 17024, Conformity Assessment—General Requirements for Bodies Operating Certification of Persons. Others in the National Security Community, notably the Department of State and the Department of Veterans Affairs, use the Certified Information Systems Security Professional certification to evaluate an individual's overall security knowledge. NSA has expanded its on-site review and testing services for the Information Systems Security Engineering Professional credential to establish an additional level of knowledge and expertise tailored to U.S. national security.

IT Security Essential Body of Knowledge

DHS is leading the development of the IT Security Essential Body of Knowledge (EBK) that characterizes the IT security workforce and provides a national baseline representing the essential knowledge and skills that IT security practitioners should have to perform specific roles and responsibilities. This national initiative extends beyond the Federal Government, reflecting the vast contribution of public and private sector resources and established references and best practices. It further clarifies key IT security terms and concepts for well-defined competencies; identifies notional security roles; defines four primary functional perspectives; and establishes an IT Security role, competency, and functional matrix. The draft IT Security EBK was published in the Federal Register in October 2007. Promotion of its use will help ensure that the Nation has the most competent IT security workforce possible.

2008 Priorities

- Test all CNSS constituent agency IA professionals against CNSS training standards. This will raise the bar to an appropriate level for those who manage, operate, or acquire NSS.
- Fund training and education modules based on the CNSS Instruction 4000-series standards for distribution to interested institutions of higher education. These curricula resources will enhance the state of IA education and training nation-wide for those institutions that now cannot afford to become CAEIAE.
- Leverage CNSS relationships with private sector training and certification vendors to infuse CNSS standards and the IT Security EBK into their certification programs and training curriculum.
- Promote innovation in IA through use of the CAEIAE to conduct leap-ahead research projects for NSS and expand the use of IA scholarships to attract and retain top IA talent to meet mission essential needs of the Federal Government.

Conclusion

The *2007/2008 CNSS Report: An Agenda for Safeguarding National Security Systems* highlights a number of significant accomplishments made by the CNSS and several Federal departments and agencies in the areas of assured information sharing; managing risk; identity assurance; network resilience for mission assurance; and building and sustaining a superior IA workforce. These and other efforts contribute to the overall health of our NSS. These accomplishments were achieved through strong partnerships among Federal, State, local, and tribal government authorities; academia; private sector organizations; and our foreign partners and allies. The CNSS provides an invaluable forum for engaging the National Security Community to collaborate and achieve long-term, integrated solutions vital to safeguarding NSS and protecting the global information infrastructure. The CNSS plays a vital role in bringing complex challenges and issues to the forefront and in developing common policies and approaches for the Federal Government that are applicable to other communities of interest.

The 2008 priorities identified in this report represent an ambitious agenda that supports the implementation of the Administration's cyber security and information sharing agenda and the *National Military Strategy for Cyberspace Operations.* In addition, the 2008 priorities will continue to strengthen our partnerships by having common approaches to common challenges, which in turn will increase information collaboration, knowledge sharing, and trust among the various players, helping to further mitigate risk, and improving the competency and awareness of our workforce. Most importantly this report should strengthen relationships with key public and private sector security partners by focusing our energy and attention on five overarching goals for enhancing the security of NSS and ultimately the Nation.

COMMITTEE ON NATIONAL SECURITY SYSTEMS

CNSS

SYSTEMS SECURITY FOR THE 21st CENTURY

CNSS Secretariat
National Security Agency

9800 Savage Road, STE 6716
Fort George G. Meade, MD 20755-6716

410.854.6805 unclassified phone
410.854.6814 unclassified fax
410.854.0217 secure fax

cnss@radium.ncsc.mil
http://www.cnss.gov