COMMITTEE ON NATIONAL SECURITY SYSTEMS

CNSS

SYSTEMS SECURITY FOR THE 21st CENTURY

CNSS Report

Progress Against 2008 Priorities

April 2009

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 · QUI PRO DOMINA JUSTITIA SEQUITUR
DEPARTMENT OF TRANSPORTATION · UNITED STATES OF AMERICA
U.S. DEPARTMENT OF HOMELAND SECURITY
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
JOINT CHIEFS OF STAFF
GENERAL SERVICES ADMINISTRATION
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES · OFFICE OF MANAGEMENT AND BUDGET
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE · UNITED STATES OF AMERICA
FIDELITY BRAVERY INTEGRITY
DEPARTMENT OF THE ARMY · UNITED STATES OF AMERICA · 1775
DEPARTMENT OF THE AIR FORCE · MCMXLVII · 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

Committee on National Security Systems

April 30, 2009

In March 2008, the Committee on National Security Systems (CNSS) delivered to the Executive Office of the President the *2007/2008 CNSS Report, "An Agenda for Safeguarding National Security Systems,"* that described strategic accomplishments of the CNSS and its individual Federal Departments and Agencies to enhance the security of national security systems (NSS) and outlined priorities for 2008. The priorities were categorized under five major focus areas: (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 workforce.

The attached CNSS Progress Report highlights key actions taken in those five focus areas against the 2008 priorities and recommendations. These efforts were consistent with National Security Presidential Directive 54/Homeland Security Presidential Directive 23 and the Comprehensive National Cybersecurity Initiative (CNCI). In addition, it is important to note that a significant event occurred in late 2008 when existing CNSS authorities and policies enabled the National Security Agency to engage directly with Departments and Agencies from across the National Security Community to provide situational awareness and advise them on current threats to our networks. This activity ensured the delivery of a consistent message across the Federal Government; promoted a sense of urgency and enhanced the level of cooperation among all affected Federal Departments and Agencies; and increased the sharing of information to defend critical NSS.

The CNSS continues to work closely with the Federal Departments and Agencies that comprise the National Security Community to improve the security of NSS. Interagency participation and CNSS commitment to defending NSS continue to provide the foundation for initiatives designed to defend against and defeat cyber attacks in spite of an increasing and constantly changing threat.

Although this report details progress to date, there is still much work to do, especially in light of the CNCI. We must build on these accomplishments and remain vigilant in leading the effort to strengthen NSS and the cyber infrastructure vital to national security. The CNSS will work to support the new Administration's goal of cooperation and sharing with our Allies and the private sector to identify and protect against emerging cyber threats.

Sincerely,

John G. Grimes
Chair
Committee on National Security Systems

At a Glance…

The Committee on National Security Systems (CNSS), comprised of 21 Members and 11 Observers, represents the National Security Community of the Federal Government in protecting telecommunications and information systems that support U.S. national security. In 2008, the CNSS delivered to the Executive Office of the President the *2007/2008 CNSS Report, "An Agenda for Safeguarding National Security Systems,"* that described recent strategic accomplishments of the CNSS and its individual Federal Departments and Agencies along with priorities for 2008 in the following focus areas—assured information sharing; managing risk; identity assurance; network resilience for mission assurance; and building and sustaining a superior information assurance (IA) workforce.

Then President George W. Bush directed the CNSS to act on the priorities and provide a progress report in 2009. In May 2008, the CNSS Members and Observers identified the top two to three priorities for each focus area to pursue over the next 9 to 12 months. The Members and Observers focused on priorities that realistically could be accomplished in the designated period with available resources. These priorities and accomplishments are highlighted below. This report also features additional actions that individual CNSS Members and Observers took to improve the protection of national security systems (NSS).

Assured Information Sharing

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

2008 Priorities	2008 Accomplishments
▸ Enhance the partnership between the CNSS and the Program Manager for the Information Sharing Environment (PM-ISE) to support PM-ISE architecture, common standards initiatives, and implementation of the *National Strategy for Information Sharing.*	▸ CNSS reinvigorated the Assured Information Sharing Working Group (AISWG) with a new vision for responsible information sharing across domains and an enhanced partnership with the PM-ISE to support its architecture, common standards initiatives, and implementation of the *National Strategy for Information Sharing.* The AISWG drafted CNSS Policy No. 24, "The National Information Sharing Policy for National Security Systems."
▸ Protect all sensitive but unclassified data residing on critical, high-value mobile computing devices and removable media, leveraging the heavily discounted Data at Rest procurement vehicles across the National Security Community.	▸ 1.5 million licenses were sold via the Data at Rest Tiger Team Blanket Purchase Agreements (BPA) to Federal, State, and local governments to help ensure controlled unclassified information (CUI) is protected on mobile and removable devices. ▸ CNSS established a Wireless Tiger Team to update CNSS Policy No. 17, "National Information Assurance Policy on Wireless Capabilities," to incorporate guidelines on risk management, use in an operational environment, and common processes for the assessment and introduction of emerging wireless technology.
▸ Support a single Department of Defense (DoD)/Intelligence Community (IC) domain implementation process to promote information sharing throughout the Federal Government.	▸ The Unified Cross Domain Management Office (UCDMO) developed a streamlined process for agencies to obtain cross domain solutions to support NSS. ▸ Increased use of Blackberry and Voice over Internet Protocol (VoIP) telephones in the National Security Community.

Managing Risk

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

2008 Priorities	2008 Accomplishments
▸ Operationalize a common risk assessment methodology for NSS through formal policy and promote its adoption across the Federal Government.	▸ CNSS developed CNSS Policy No. 22, "Risk Management Policy for National Security Systems," to promote the acceptance of a single, unified risk management framework and system authorization (*i.e.,* certification and accreditation) process.
▸ Implement a common, unified certification and accreditation process for the Federal Government and issue a CNSS policy and instructions on security controls, impact levels, and the unified certification process.	▸ The CNSS, DoD, Office of the Director of National Intelligence (ODNI), and National Institute of Standards and Technology (NIST) developed policies and instructions that will provide the foundation for a common approach for certifying and accrediting NSS.
▸ Support supply chain risk management implementation across the Federal Government by developing acquisition policy, processes, and guidance; and ensuring alignment of NSS policies and practices with Federal acquisition processes and guidance.	▸ Addressed supply chain risk management by proposing approaches for integrating IA and security concerns into the Federal acquisition process through adoption of several guides and pilot programs. ▸ The CNSS is developing policies to address security requirements for software acquisition as part of supply chain risk management.

Identity Assurance

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

2008 Priorities	2008 Accomplishments
▶ Develop a baseline for public key infrastructure (PKI) interoperability and information sharing requirements for both classified and unclassified networks and promulgate it across the Federal Government.	▶ Finalized CNSS Policy No. 25, "National Information Assurance Policy for Public Key Infrastructure in National Security Systems," for the implementation of a PKI for the SECRET environment patterned after the hierarchical PKI implemented by the IC for the Sensitive Compartmented Information (SCI) environment. ▶ CNSS PKI Working Group drafted an instruction to govern the operation of PKI certificates for SECRET and below systems. ▶ DoD adopted a new policy to accept third party PKI through the Federal Bridge Certification Authority.
▶ Issue NSS identity assurance roadmap and architecture for implementing multi-factor authentication and leveraging national biometrics efforts and federated commercial, off-the-shelf solutions.	▶ To increase information sharing among Federal Department and Agency personnel and reduce the cost associated with providing credential management, DoD extended electronic authentication to several DoD Web sites and information systems to Federal Department and Agency users with Homeland Security Presidential Directive (HSPD) 12-compliant cards.

Network Resilience for Mission Assurance

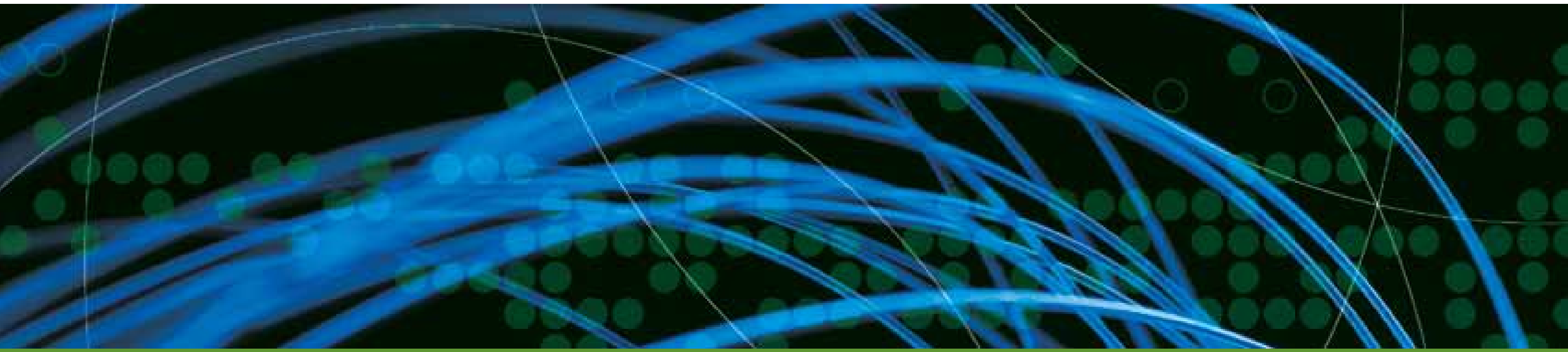
Works under fire; attacks are prevented, deflected or do little damage; operates through or recovers quickly following successful attacks.

2008 Priorities	2008 Accomplishments
▶ Improve the level of protection of CUI resident on Federal networks and support the exchange of best practices and techniques.	▶ Through the Defense Industrial Base (DIB) Cyber Security and IA Program, DoD, CNSS, and the DIB Sector are partnering to protect CUI residing on DIB unclassified networks. ▶ Two new DoD offices were established to share threat information, IA best practices, and cyber alerts with DIB Sector partners.
▶ 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.	▶ A DoD Task Force identified key capability and resource gaps for network resiliency and promoted realistic modeling, exercises, and simulations, which enhanced network resilience, continuity of operations planning, and protection of critical information infrastructures for NSS. DoD developed a plan of action and milestones to improve policies, plans, and programs for implementing and regularly exercising capabilities for continued operation through cyber or kinetic attacks. ▶ CNSS established the Network Resilience Tiger Team to expand the DoD Task Force findings and results across the National Security Community and develop resiliency policy and standards for NSS and the supporting infrastructure.

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.

2008 Priorities	2008 Accomplishments
▶ Enhance international academic outreach efforts.	▶ The National Security Agency (NSA) briefed British universities and United Kingdom Government officials on the U.S. CAE in IA Education Program and developed a report on the CAE Program and processes that was distributed to partners in the United Kingdom, Australia, New Zealand, and Canada.
▶ Promote innovation through use of the national Centers of Academic Excellence (CAE) in IA Education.	▶ NSA and the Department of Homeland Security (DHS) co-sponsored the Annual Principals meeting of the CAE to provide a forum for discussing the role of higher education in securing America's critical information infrastructure; updating the CAE on IA efforts and opportunities at the national level; and promoting CAE collaboration with government to maximize expertise and resources. ▶ As part of the Comprehensive National Cybersecurity Initiative (CNCI), the CAE are developing "Communities of Interest" on research topics (*e.g.,* software assurance) to increase collaboration among NSA, DHS, CNSS, CAE, and industry on leap-ahead research topics and IA curriculum improvement.
▶ Leverage CNSS relationships with private sector training and certification vendors.	▶ Collaboration and teaming with industry partners such as SANS Institute and the International Information Systems Security Certification Consortium have increased. CAE have joined forces with industry bodies to ensure the CAE curriculum meets their needs.



Assured Information Sharing

Accomplishments

The capability to fight terrorism; help citizens in the wake of natural disasters; assist law enforcement; and maintain national security is dependent on the ability to share information securely across various domains. Trust, established through common policies, strategies, frameworks, and approaches, is vital to national security and to the protection of NSS.

Enhanced Partnership with the PM-ISE

With the expanded use of secure personal electronic devices, the widespread deployment of cross domain solutions, and increased requirements for secure collaboration, the CNSS is committed to developing policies that support the "need-to-share." The CNSS Assured Information Sharing Working Group (AISWG) is drafting CNSS Policy No. 24, "The National Information Sharing Policy for National Security Systems." The AISWG has begun to enhance the partnership between the CNSS and the PM-ISE to support its architecture, common standards initiatives, and implementation of the *National Strategy for Information Sharing.* In addition, the AISWG is collaborating with the Information Sharing Council to develop policy that not only supports information sharing for counter-terrorism activities, but also supports all aspects of information sharing regarding national security priorities. Data at Rest. Since June 2007, Data at Rest Tiger Team BPA sold over 1.5 million licenses to Federal, State, and local governments to help ensure controlled unclassified information is protected on mobile and removable devices. Because of the large number of licenses issued, the license cost was minimal and generated a cost savings of $91 million for the Federal Government. The BPA contract vehicle has become the de facto standard for purchasing encryption equipment for protection of data at rest on mobile devices (*e.g.,* laptops, removable media)

Increased Wireless Capabilities

The wireless capability support to the National Security Community made significant progress, including acquiring new satellite capabilities, additional secure telephone equipment, the Wireless Priority Service, and the Government Emergency Telecommunications Service. To help ensure that senior leadership can continue to operate under all circumstances, the Office of Management and Budget (OMB) approved a plan to upgrade senior leadership facilities with access to additional cross domain classified networks, new communications tools, and more robust encryption capabilities. In addition, the CNSS established a Wireless Tiger Team to update CNSS Policy No. 17, "National Information Assurance Policy on Wireless Capabilities." The goal is to expand the current policy to incorporate guidelines on risk management; the use of wireless in a range of operational environments; common processes for risk assessment; and emerging wireless technologies. The Tiger Team is using collaborative online technologies to support policy revisions and permit the sharing of interagency policies on wireless security.

Cross Domain Investments, Solutions, and Activities

The UCDMO rolled out a new streamlined process for agencies to obtain cross domain solutions, which focuses on using enterprise services and existing baseline solutions before developing new capabilities. The new process also allows the National Security Community to vet and make recommendations to the Chief Information Officer (CIO) Oversight Panel before any new cross domain solution development occurs. In 2008, recommendations resulting from the cross domain review process totaled over $60 million in cost avoidance to the U.S. Government. In addition, a roadmap was developed to ensure information sharing requirements are satisfied; reduce duplication of effort; ensure the cross domain solutions capabilities are available when needed; and assist senior leaders and program managers in making prudent and cost-effective investment decisions regarding information sharing services.

Increased Information Sharing Capabilities

The National Security Community has expanded greatly its use of Blackberry devices and VoIP telephones. The Federal Bureau of Investigation, for example, is preparing to pilot Secure Mobile Environment Portable Electronic Devices and has implemented VoIP on its SECRET Collateral network. In addition, the Department of Justice is exploring the use of Federated Identity Management for sharing law enforcement information.

Assured information sharing continues to be a national security priority. The expanded used of secure personal electronic devices combined with the need to be accessible underscores the requirements for secure collaboration and responsive action. With increased wireless capabilities, cross domain solutions, dynamic access control capabilities, and enhanced partnerships, Federal Departments and Agencies have embraced assured information sharing as vital to national security.

Managing Risk

Accomplishments

Historically, the IC, DoD, and civil Departments and Agencies have had separate processes and procedures for performing certification and accreditation (C&A) and overall risk management. There was no real reciprocity, which caused duplication of C&A processes and increased costs, and no common risk management framework existed. Each Department and Agency handled risk as they deemed appropriate. Risk was evaluated on a system-by-system basis and not from an enterprise-wide perspective.

In 2008, the CNSS continued working closely with NIST, ODNI, and DoD to develop a unified information security framework for the Federal Government and its support contractors. The project, designated as the C&A Transformation Initiative, is on target to produce a series of new CNSS policies and instructions for managing risk. The C&A Transformation Initiative includes developing guidance on security categorization, security control specifications, and security control assessments that closely parallels the NIST security standards and guidelines developed in response to the *Federal Information Security Management Act of 2002.*

Common Risk Assessment Approach

Risk management is no longer risk avoidance. Risk management now considers protecting a Department or Agency's ability to perform its mission not just protecting its information systems. Focused at the enterprise level vice an individual system, it is now an essential management function tightly tied into the system development life cycle. The new process considers operational and economic costs of protective measures weighed against requirements for mission accomplishment. The unified process, which is under development, will provide the capability for managing risk in a highly dynamic environment of complex and sophisticated cyber threats, ever-increasing information system vulnerabilities, and changing missions. The new process promotes the concept of near real-time risk management and helps to ensure responsibility and accountability for the common security controls inherited by organizational information systems.

To promote the adoption of a single, unified risk management framework and system authorization (*i.e.,* C&A) process, the CNSS established a requirement for enterprise risk management within the National Security Community through development of CNSS Policies and Instructions. CNSS Policy No. 22, "Risk Management Policy for National Security Systems," establishes the requirements for enterprise risk management within the National Security Community and provides a framework for decision makers to continuously evaluate and prioritize risks in order to accept or recommend strategies to remediate or mitigate those risks to an acceptable level. In accordance with CNSS Policy No. 22, each Federal Department and Agency, including independent bureaus and offices, is required to establish and implement a Risk Management Program. In addition, the IC, DoD, NIST, and other CNSS Members and Observers participated in the development of NIST Special Publication (SP) 800-37, "Guide for the Security C&A of Federal Information Systems," and NIST SP 800-39, "Managing Risk from Information Systems: An Organizational Perspective."

The CNSS is defining a common methodology for conducting risk assessments of all NSS in CNSS Instruction No. 1230, "Risk Assessment Methodology for National Security Information and Systems." The instruction will supplement NIST SP 800-30, "Risk Management Guide for Information Technology Systems," assuring a comprehensive and rigorous approach for characterizing the threats facing our systems and managing risk across the National Security Community. In support of this instruction, a software tool is in development to significantly accelerate the speed by which assessments are conducted. CNSS Instruction No. 1230, along with CNSS Policy No. 22, will assist the IC, DoD, and civil Departments and Agencies in obtaining reciprocity and trust among disparate NSS owners.

C&A Transformation

The IC, DoD, and NIST are working together to create a common C&A process that focuses on a more holistic and strategic approach to the risk management of information technology (IT) systems and processes and procedures designed to develop trust across the communities' IT enterprises through use of common standards and reciprocally accepted C&A decisions. The IC developed standards that map to NIST SP 800-37. The Department of the Treasury recently issued a security policy manual that aligns with community-wide risk management principles, common security processes, and reciprocity. The CNSS drafted, in partnership with DoD, NIST, and ODNI, CNSS Instruction No. 1253, "Security Control Catalog for National Security Systems;" CNSS Instruction No. 1253A, "Guide for Assessing Security Controls;" and CNSS Instruction No. 1199, "Security Categorization of National Security Systems" as an initial step toward combining common C&A processes and procedures into single documents for use across the National Security Community. NIST and CNSS are working together to ensure their documents mirror each other as much as possible with the goal of having one set of documents for the entire Federal Government with respect to risk management and C&A. This effort to synchronize CNSS policies and instructions and NIST Special Publications represents a significant and unprecedented move toward convergence of information security standards, guidelines, and best practices across the National Security Community. The primary objective is to build a common foundation for information systems security for all Federal Departments and Agencies and supporting contractors that diverges only when necessary to satisfy community-specific requirements.

The UCDMO also made significant progress to support the Managing Risk priority by pursuing an initiative to coordinate testing of methodologies and procedures related to cross domain solutions across the IC and DoD. The outcome of this initiative has been to move toward common hardware and software testing standards, methodologies, and procedures that will enable a validated cross domain solution to be accepted by any agency or entity without requiring further certification.

Supply Chain Risk Management

One CNSS Member created a dedicated branch that performs supply chain risk management reviews of the vendor(s) associated and affiliated with a product. Purchases are pre-reviewed for foreign ownership, control, and influence before procurement. The Member also created a database to assist in "connecting the dots" to show links between the supply chain and countries of concern. Agency-wide procurement vehicles are being implemented and General Services Administration SmartBuy agreements are being used for software acquisition, where available. IA tools are vetted in laboratory tests and evaluations. Consequently, many Departments and Agencies have incorporated into their policies required compliance with National Security Telecommunications and Information Systems Security Policy No. 11, "National Policy Governing the Acquisition of IA and IA-Enabled Information Technology Products." Several Federal Departments and Agencies are evaluating changes and enhancements to existing procurement language to address supply chain issues. Some have implemented mandatory security clauses in their contracts to address the security of IT investments and services. Cybersecurity requirements are being integrated into configuration, patch, change, and release management disciplines.

Software Assurance

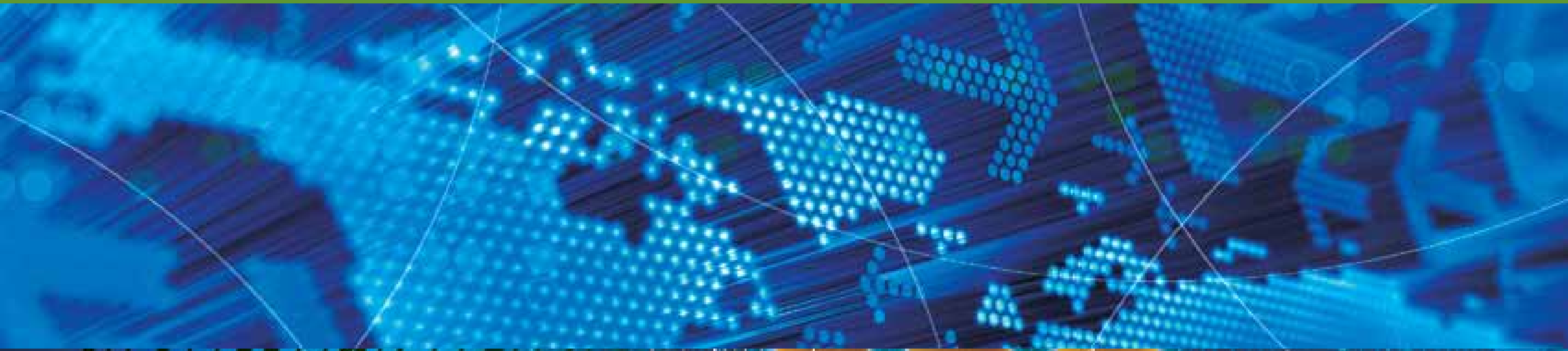
Many of the CNSS Members and Observers are reviewing their existing Department and Agency processes and developing a strategy to ensure compliance with future ODNI, CNSS, DoD, and NIST C&A and risk management process changes, including plans to educate their workforce. They are developing policies to address security requirements for software acquisition to include purchased and open source software as part of supply chain risk management efforts. Great advances were made through the Software Assurance Forum and Working Groups, which were co-sponsored by DHS, DoD, and NIST, that enabled software assurance stakeholders to collaborate on producing procurement, development, and measurement reference documents that reflect a consensus-based process involving contributions from many public and private sector organizations.

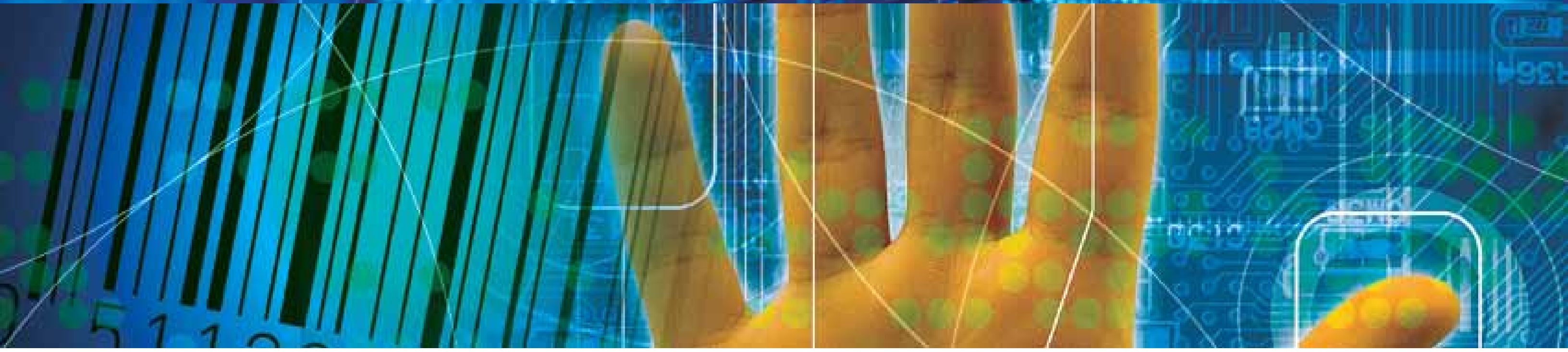
The National Security Community made great strides in addressing supply chain risks, finalizing a unified system authorization process, and embracing a common risk management framework. Having a common risk management approach that addresses supply chain risks and a unified process for assessing and authorizing the operation of NSS will enhance information sharing among the IC, DoD, CNSS, and civil communities as well as between individual Federal Departments and Agencies

Identity Assurance

Accomplishments

The CNSS supported several initiatives in 2008 to address identity assurance and further engage the National Security Community in the protection of vital telecommunications and information systems. Federal Departments and Agencies use a combination of technological architectures and solutions to improve interoperability, prevent spoofing, and increase information sharing. In addition to user IDs and passwords, which are commonplace throughout the Federal Government, token issuance, credential management, Common Access Card (CAC), PKI, and biometrics continue to evolve and operate as additional safeguards for IA.





PKI

The CNSS PKI Working Group (WG) engaged in a study to determine whether PKI can fill the gap between the unclassified/sensitive but unclassified environment (satisfied by the Federal Bridge) and the TS/SCI environment (satisfied by the IC PKI). Careful study of available options supported a recommendation that implementation of a PKI for the SECRET environment, patterned after the hierarchical PKI implemented by the IC for the TS/SCI fabric, was acceptable. The CNSS PKI WG developed CNSS Policy No. 25, "National Information Assurance Policy for Public Key Infrastructure in National Security Systems," which is with the CNSS Chair for signature. This policy establishes requirements for Federal Departments and Agencies to have a PKI to manage and support their SECRET and below classified networks and systems. The PKI WG is drafting the PKI Certificate Policy that will govern the creation, issuance, management, and use of the X.509 PKI certificates. The Certificate Policy facilitates identity authentication, technical non-repudiation, data integrity, and common privacy on these networks among trusted participating entities.

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

Various members of the National Security Community participated in the Executive Office of the President's National Science and Technology Council's Task Force on Identity Management. This Task Force conducted a six-month study of the current state of Federal identity management systems and delivered a report that provided a common foundation for installation of these systems and presented a high-level vision on how these systems can provide better services while increasing privacy protection. In addition, DoD adopted a new policy to accept third party PKI through the Federal Bridge Certification Authority, overseen by the Federal CIO Council, which facilitates trust between disparate PKI. The use of hardware credentials with PKI certificates for authentication has enhanced the security of information systems and business processes for DoD and may be considered for use throughout the Federal Government.

HSPD-12 Implementation

Federal Departments and Agencies continue to support efforts to implement HSPD-12 for non-NSS. Some organizations employ a tiered approach where users authenticate and log in to their networked workstations and Web sites using PKI certificates on a CAC. DoD extended this electronic authentication capability to several DoD Web sites and information systems to Federal Department and Agency users who have HSPD-12 compliant cards. By October 2008, the Department of Transportation had issued just over 6,000 Federal Information Processing Standard (FIPS) 201 Personal Identity Verification cards agency-wide as part of its initial implementation, enabled FIPS 201-compliant physical access control systems at its headquarters building for piloting, and began logical access pilots to support access to network, e-mail, and file services. The Department of Justice also implemented HSPD-12 cards for physical access to buildings and initiated piloting the use of the card at several of the bureaus for logical access, digital signing, and encryption. Electronic authentication facilitates general information sharing among Federal Department and Agency personnel and it reduces credential provisioning costs and help desk traffic.

PKI, HSPD-12 implementation, and the Federal Bridge lead the way for identity assurance and engage the National Security Community in the protection of vital telecommunications and information systems. Substantial reliance on the identity of those using and sharing information via NSS is key to establishing the foundation of interoperability and exchange. Measures including, but not limited to, token issuance, credential management, CAC, and biometrics help strengthen organizations' confidence in identity authentication, technical non-repudiation, and data integrity. Implementation of these developments assures more robust capabilities for the protection of NSS.

Network Resilience for Mission Assurance

Accomplishments

National security depends on a global information infrastructure that is reliable and resilient. The CNSS and Federal Departments and Agencies are working in partnership with the private sector and our Allies to ensure resilience of our networks for the National Security Community. Resilience encompasses more than networks; it includes human, physical, and knowledge domains and needs to be considered holistically. People, processes, and policies throughout these domains require examination and scrutiny to determine trustworthiness. Government and industry share responsibility for protecting the critical information infrastructure and public-private partnerships are essential to ensure resilience of the infrastructure. Moreover, common goals and approaches help to mitigate the risks facing the Nation. Given the sophistication of our adversaries, the National Security Community must assume that one day an adversary may succeed and use our net-centricity against us. Therefore, it is essential that the Nation have the ability to operate through such an event and be able to recover quickly.

Improve Protection of CUI

The threat to DIB Sector unclassified networks is real; they are being targeted daily. In 2008, DoD embarked on changing the culture both inside the Government and across industry. DoD developed and implemented the DoD-DIB Cyber Security and IA Program to protect DoD CUI (*e.g.,* unclassified weapons program, technology, and combat information) resident on DIB unclassified networks. Together, DoD and the DIB Sector initiated the pilot program, which included the development of a concept of operations, the DIB Cyber Security Capabilities Benchmark, and the DoD-DIB Security Classification Guide. To further implement the program, DoD established two new organizations—(1) the DoD-DIB Collaborative Information Sharing Environment (DCISE), located at the DoD Cyber Crime Center; and (2) the Damage Assessment Management Office (DAMO), located in the Office of the Under Secretary for Acquisition, Technology, and Logistics. Through DCISE, DoD shares classified and unclassified threat information, IA best practices, and cyber alerts with DIB Sector partners. In return, participating DIB Sector partners share incident and intrusion reports about their networks with DoD. The DAMO coordinates operational damage assessments of DoD programs through Military Service damage assessment teams. In addition, DoD is developing a real-time secure data/voice communication network (*i.e.,* DIBNet) to strengthen secure information sharing between DoD and its DIB Sector partners. The initial operating capability was activated on December 15, 2008. Finally, the DoD-DIB Program not only addresses the immediate need to mitigate, detect, and remedy cyber intrusions, it also provides a source of feedback to inform changes to the Federal Acquisition Regulation/ Defense Federal Acquisition Regulation-Supplement for enhanced IA and cybersecurity requirements in DoD contracts. The progress made to improve the security of CUI resident on DoD contractors' networks will benefit the entire National Security Community as it provides a roadmap for other Federal Departments and Agencies to follow in protecting CUI.

Cyber Exercises for Mission Assurance

A DoD task force, which was established to reduce the risk of degraded or failed missions by analyzing dependencies and cascading effects of information and communication technologies supporting primary mission essential functions, identified key capability and resource gaps for network resiliency. Findings resulting from the DoD task force's efforts were incorporated into Cyber Storm II (a DHS-sponsored, national-level cyber exercise) held in March 2008 and Global Lightning '09 (a DoD-sponsored exercise) held in November 2008 to promote realistic modeling, exercises, and simulations. These exercises enhanced network resilience, continuity of operations planning, and protection of critical information infrastructures for NSS. Conducting these cyber exercises is vital for mission assurance.

Resilience Standards

Based on National Security Presidential Directive 51/HSPD-20, "National Continuity Policy," recommendations from the President's National Security Telecommunications Advisory Committee (NSTAC) Global Infrastructure Resiliency Report, and a recognition of the growing sophistication of the cyber threat and dependence on information and communication technologies, the CNSS established the Network Resilience Tiger Team to evaluate capability gaps and identify strategic and policy actions for the future. The Team concluded that there are significant gaps with respect to continuity and cyber resilience and a lack of a unified strategy for the National Security Community. The Team outlined a plan of action for 2009 to address the need for policy regarding network resilience standards and the underlying critical infrastructures. The Team plans to represent the National Security Community's interests in discussions with the President's Office of Science and Technology Policy, NSTAC, DHS' National Communications System, and other groups to support the development of consistent network resiliency policies to improve network diversity and resilience for NSS.

Networks must be robust for enduring communications and data transfer, and our people, processes, and the information systems supporting national security missions must be flexible, adaptable, and trustworthy in order to evolve with today's fast-paced and agile operational and technological environment. Cyber resilience is much more than networks, and is built on survivable communications (transport), trustworthy information (content), and timely services (applications). Network resilience is more than just mission assurance; it is part of the foundation that enables mission success.

Building and Sustaining a Superior IA Workforce

Accomplishments

Challenges for creating and sustaining a superior IA workforce continue to exist. It is not possible simply to build an IA workforce as one might build a personal computer, and upgrade as necessary. The people who build, maintain, use, troubleshoot, extend, and defend the systems we depend on for our Nation's security require continuous education, training, awareness, and certification. With alarming acceleration, exploits, cyber attacks, and attempts to infect NSS, plague our efforts to defend, resist our efforts to prevent, and contest our efforts to destroy malware used in this cyber war. However, the CNSS and Federal Departments and Agencies have faced the challenges of this dynamic threat environment and have significantly advanced toward establishing the best and brightest IA workforce, which is the greatest deterrent to any cyber adversary.

Enhance International Academic Outreach Efforts

The U.S. CAE Program increased its outreach to international academic institutions. For example, accompanied by representatives from Detroit Mercy University, NSA representatives briefed London Southbank University and Oxford University in the summer of 2008 on the U.S. National CAE in IA Program. They gave similar presentations to United Kingdom (U.K.) Government officials from the British Standards Organization, Communications-Electronics Security Group, and Government Communications Headquarters. In addition, NSA prepared and distributed a report detailing the CAE program and processes to our partners in the U.K., Australia, Canada, and New Zealand. Finally, a workshop, "Creating and Improving on a National Support Structure for Information Security Education," was held at the International Conference on Systems Science in January 2009. The workshop provided awareness of the effectiveness of the National IA Education and Training Program and examined future growth of and opportunities for the program.

Promote Innovation Through the Use of CAE

On October 28, 2008, NSA and DHS co-sponsored the Annual Principals meeting of the CAE. Seventy-six of the 94 CAE attended. The meeting provided a forum for discussing the role of higher education in securing America's critical information infrastructure; updating the CAE on IA efforts and opportunities at the national level; and promoting CAE collaboration with government to maximize expertise and resources. The CAE are developing "Communities of Interest" on research topics (*e.g.,* software assurance) to increase collaboration other leap-ahead research topics. The CAE are also using their "CAE credentials" on the State and local levels to receive grants and scholarships to increase the skill levels of the workforce.

Leverage Relationships with Industry and Other Partners

Collaboration and teaming with industry partners such as the SANS Institute and the International Information Systems Security Certification Consortium have increased. The CAE joined forces with these industry bodies to ensure that the CAE curriculum meets their needs. For example, two industry groups are working with a CAE to develop a pilot for writing secure code and to make it available to other institutions across the country. While collaborating with government representatives, these institutions support the pilot with their own resources and funding of all the requirements to assure future success. The CNSS leverages its relationships with Information Security Privacy Advisory Board corporate board members and works to connect them with the CAE and other government bodies that are improving the IA workforce throughout the Nation.

The CNSS continues to collaborate with the National Security Community to enhance processes and procedures necessary to attract and retain IA professionals. By working together to address priorities for sustaining a superior IA workforce, recruitment and retention of knowledgeable IT professionals are more methodical, more exact, and less burdensome. At least one Department, the Department of State, offers "Skills Incentive Pay (SIP)." SIP permits employees serving in IT-specific positions to receive an additional 10 to 15 percent of their basic pay by attaining specific credentials, such as Certified Information Systems Security Professional (CISSP), Masters Degree in IT, Microsoft Certification, and other credentials. At least 80 percent of the Department's IT professionals possess a professional IT certification as a result.

DHS continues to promote the use of the IT Security Essential Body of Knowledge (EBK), which characterizes the IT security workforce and provides a national baseline for the essential knowledge and skills necessary for IT security practitioners to perform specific roles and responsibilities. This national initiative extends beyond the Federal Government, reflecting the vast contribution of public and private sector resources, as well as establishes references and best practices. Further, it clarifies key IT security terms and concepts for well-defined competencies, identifies notional security roles, and establishes an IT Security role, competency, and functional matrix. In addition, DHS is working to develop and implement a State government model for information security workforce development based on the EBK. The proposed model will provide a common framework to enable and foster State government IT security workforce development, education and training, and certification requirements. Once the State government model is developed, individual State governments will be able to implement according to their individual needs.

IA Training and Awareness

The National Security Community considers the extent and familiarity of IT training and awareness in its hiring programs. Some organizations include IA awareness training during the orientation phase of employment for new people, with periodic follow-on training. Most network users are required to complete an IA orientation course before permitted access to any network and complete annual awareness training to maintain access privileges. In addition, organizations report hiring more cybersecurity experts based on various professional certifications. These practices have been expanded to include IA training and awareness in statements of work for contractors. As a result, the percentage of network users and administrators having formal IA and IA awareness training continues to climb. Network users and administrators with formal training now range between 80 to 94 percent.

Federal Departments and Agencies have incorporated IA training and awareness into much of the curricula for which they are responsible. Many of the classes include videos, lectures, and practical exercises designed to increase awareness and emphasize the importance of safeguarding information and IT equipment. Other mediums used by the Federal Departments and Agencies include coordinated IT security awareness events, posters, and computer-based training to augment and reinforce IA awareness and best practices within every user, administrator, and IT professional. In addition, some organizations conduct professional training, hosting training and testing for CISSP and various Microsoft and Cisco certifications.

Leaders and managers are critical to the success of sustaining a superior workforce. As key stakeholders, they must have the ability to track their IA workforce, run reports, and receive automated notices when user training/certification is about to expire and take the steps necessary to maintain personnel compliance. For example, the Army Training and Certification Tracking System provides a centralized location for users to track training completions, certifications obtained, and other specialized training. This same system also affords managers the ability to monitor workforce compliance with training and certification requirements and provide early notification of pending expiration to assist personnel in maintaining compliance and certification.

Achieving and sustaining a superior IA workforce is not an easy goal, but it is an attainable one. The progress made over the past year highlights the commitment of the CNSS and the Federal Government. Through the perseverance and dedication of the CNSS, IC, DoD, and civil Departments and Agencies, the National Security Community will achieve this goal sooner rather than later.

Conclusion

This report highlights several significant steps that the CNSS, as well as other Federal Departments and Agencies, has taken to achieve goals necessary to help the National Security Community secure cyberspace. Cybersecurity is among the most serious economic and national security challenges we face as a Nation. With the publication of National Security Presidential Directive 54, "Cybersecurity Policy," many of the accomplishments in this report will prove invaluable in supporting the CNCI.

The National Security Community, through the CNSS, continues to work to increase the protection of our NSS and telecommunications and information systems from cyber attack. Although we may never achieve total security in cyberspace, we can work to enhance the availability of trustworthy data; reduce our risks; provide strong, reliable forms of identification; increase the resiliency of our networks; and improve the qualifications and skills of our IA workforce. We must be able to securely use cyberspace not only for defending our networks but also for our national benefit.

With the beginning of a new Administration come opportunities for change, new vision, growth, and collaboration. The CNSS is an invaluable forum for engaging the National Security Community and has strong partnerships across the National Security Community and with academia and industry. The CNSS is committed to supporting the new Administration as it seeks to enhance the security of our Nation's vital networks and protect our use of cyberspace.

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