CNSS: Interagency Partnering to Protect Our National Security Systems

The Honorable John G. Grimes
Department of Defense Chief Information Officer

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. This article describes recent strategic accomplishments of the CNSS and individual federal departments and agencies along with priorities for 2008.

The United States faces increasing threats in the homeland security, cyber security and information sharing environments, and the need for increased cooperation among key members of government, industry, academia, the private sector, and allied nations has never been greater. CNSS provides an interagency forum for addressing IA policy issues impacting critical NSS. Through its membership and partnerships (a total of 21 members and 10 observers from the executive branch of the U.S. government) the CNSS has a history of addressing vulnerabilities that have the potential to impact the national security community's ability to safeguard key systems. In 2007, the CNSS made significant contributions to federal, state, local, and coalition security efforts across the following five areas:

1. Assured Information Sharing (AIS)

AIS is fundamental to the integrity of our data and systems, and is essential to the nation's well-being and defense. The CNSS is actively engaged in making significant improvements across these areas. The UCDMO – a joint effort between the DoD and the DNI – has put out a unified technology road map to expedite the use of information sharing solutions between classification domains. The CNSS will extend the UCDMO's progress to other federal departments and agencies and improve information sharing among government departments and agencies. One of the key tools that revolutionized communications in recent years has been wireless devices such as PDAs and Blackberries. The emergence of the Secure Mobile Environment Portable Electronic Device – with e-mail and Web browsing capabilities up to the Secret level and voice capabilities up to Top Secret – is taking wireless to the next level. It will provide the homeland and national security communities with secure communications whenever and wherever they are needed. Another area the CNSS has emphasized is the use of data at rest encryption to protect sensitive unclassified data stored on removable media and mobile computing devices like laptops. Communication and information exchange between the U.S. and our allies in the global war on terror has been an area where the CNSS has been actively engaged. In 2007, the CNSS approved more than 60 transfers of critical products to improve information sharing. For 2008, CNSS priorities for AIS will highlight the need for developing and deploying more tools, technologies, and products that will ensure the national security community has secure, reliable access to information whenever and wherever it is needed.

Access control based on standard user characteristics (like the user s organization or role) increases both speed and security when it comes to information sharing.

2. Managing Risk

Assessing and managing risk is essential to safeguarding NSS, and we have a solid strategy to counter the threats posed by those who attempt to exploit vulnerabilities in the hardware and software we rely on. The CNSS is championing a common risk assessment methodology and a common C&A process across the government. These changes will help identify vulnerabilities, determine acceptable risk levels, and increase trust among system owners. The use of common approaches will improve capabilities, reduce costs, and increase interoperability. For the coming year our priorities for managing risk include establishing common approaches for C&A, risk assessment, and managing supply chain risk.

3. Identity Assurance

The majority of successful network penetrations today are due to failures in identity assurance where a compromised password and user ID have been used to gain unauthorized access. Establishing strong identification and authentication techniques for people and devices are central to any security effort, and that makes assurance critical. Access control based on standard user characteristics (such as the user's organization or role) increases both speed and security when it comes to information sharing. Members of the CNSS are working to promote the use of identity assurance technologies such as smart cards, tokens, biometrics, and public key technologies. Identity assurance priorities include expanding the public key infrastructure to additional communities of interest and leveraging other promising technologies such as biometrics.

4. Network Resilience for Mission Assurance

The global information infrastructure supporting the President, our military commanders, and homeland security leaders must be reliable and resilient even in the face of attacks. National security rests on having the confidence that these critical functions will be accessible during disrupted and distressed conditions. By working with private sector and allied partners, we ensure critical capabilities and missions remain operational.

CNSS Policy No. 12, issued in March 2007, emphasized integrating IA into the life-cycle of space systems that collect, generate, process, store, display, or transmit national security information. This was a huge step forward and had a dramatic impact on the commercial satellite assets so critical to keeping our networks

Coming Events

August 4-7
2nd IEEE International Conference on Semantic Computing
Santa Clara, CA
http://icsc.eecs.uci.edu/index.html

August 11-15
Integrated Systems Health Management Conference
Covington, KY
www.usasymposium.com/ishm/default.htm

August 18-20
The 10th IASTED International Conference on Signal and Image Processing
Kailua-Kona, HI
www.iasted.org/conferences/home-623.html

August 18-21
Guidance, Navigation and Control Conference
Honolulu, HI
www.aiaa.org

August 25-28
COMSEC Managers Conference
Boston, MA
www.nsa.gov

August 25-28
Implementation Fest 2008
Lake Buena Vista, FL
www.adlnet.gov

September 15-18
4th World Congress for Software Quality
Bethesda, MD
www.asq.org/conferences/wcsq

2009

2009 Systems and Software Technology Conference
Salt Lake City, UT
www.sstc-online.org

Coming Events: **Please submit coming events that are of interest to our readers at least 90 days before registration. E-mail announcements to: nicole.kentta@hill.af.mil.**

resilient. Additional priorities for 2008 include national-level exercises to enhance responses to serious cyber-degradation by critical infrastructure owners/operators, accelerating next-generation security management infrastructure development, security capabilities supporting global information sharing, and increasing the focus on continuity of operations and reconstitution.

5. Building and Sustaining the IA Work Force

People are the most critical element in securing national security systems. They operate the technology, implement the procedures, execute the policies, and make the decisions that impact everything the CNSS touches. The IA professionals who build, maintain, and defend our critical networks deserve the best education and training possible, and the CNSS has established strict standards for national IA training and education to support them. These standards have been incorporated into the training curriculum at more than 160 institutions in government, academia, and the private sector. In 2007, more than 80 centers of academic excellence across 34 states and the District of Columbia provided college students with high-level IA education, along with the opportunity to earn federal scholarships. Many scholarship students are now working for the federal government where their IA expertise is contributing to the security of our national information infrastructure. CNSS priorities for 2008 include improving IA education nationwide and working more closely with private sector training and certification vendors to infuse standards into their certification programs.

As the CNSS Chair, I am proud to say it continues to be an invaluable interagency forum for engaging the national security community on long-term, integrated solutions so vital to protecting the global information infrastructure. CNSS priorities for 2008 support the President's national cyber-security initiative, and focus on increasing the level of trust in NSSs, protecting them from our adversaries and making certain that mission-essential functions can be performed in an increasingly hostile cyber-environment. The complex challenges and emerging issues brought to the forefront by this invaluable group not only delivered benefits for national security, they also created a ripple effect that touches countless other functional areas and communities.◆

About the Author

The Honorable John G. Grimes was nominated by President Bush on June 17, 2005 and sworn in as the Assistant Secretary of Defense for Networks and Information Integration/DoD CIO on November 14, 2005. He has extensive technical and policy experience in telecommunications, information systems, and the command and control fields. Grimes' public service includes the White House National Security Council Staff as Director for National Security Telecommunications Policy; Director of Defense Command, Control and Communications Programs; and Senior Director White House Situation Support Staff. He served as Deputy Assistant Secretary of Defense for Defense-wide Command, Control, and Communications and was the Deputy Assistant Secretary of Defense for Counterintelligence and Security Countermeasures. As a member of the DoD senior executive service, Grimes held senior technical and staff positions with the National Communications System; Defense Communications Agency; and the U.S. Army Communications Command following his military service in the U.S. Air Force. Previously with Raytheon, he served as Vice President of Intelligence and Information Systems, Washington Operations. Grimes has served on four Defense Science Board Task Forces and was a member of the Industry Executive Subcommittee of the President's National Security Telecommunications Advisory Committee. Grimes is a graduate of the University of Arizona, and has a master's degree from Shippensburg University in Pennsylvania. He is a graduate of the U.S. Army War College, Carlisle Barracks, Pennsylvania; the Federal Executive Institute, Charlottesville, Virginia; and Harvard University's National and International Security Policy program. He is the recipient of the American Institute of Aeronautics and Astronautics' Command, Control, Communications, and Intelligence award among other public, military and federal civil service awards, including two Presidential Rank awards.

6000 Defense Pentagon
Washington, D.C. 20301-6000

Acronym Key for This Issue

AIS: Assured Information Sharing
C&A: Certification and Accreditation
CIO: Chief Information Officer
CNSS: Committee on National Security Systems
DASD(IIA): Deputy Assistant Secretary of Defense for Information and Identity Assurance
DIACAP: DoD Information Assurance Certification and Accreditation Process
DIAP: Defense Information Assurance Program
DISA: Defense Information Systems Agency
DNI: Director of National Intelligence
DoD: Department of Defense
GIAP: GIG IA Portfolio (Management)
GIG: Global Information Grid
IA: Information Assurance
IC: Intelligence Community
INFOSEC: Information Security
IT: Information Technology
NII: Networks and Information Integration
NSA: National Security Agency
NSS: National Security Strategy
R&D: Research and Development
SME: Subject Matter Expert
UCDMO: Unified Cross Domain Management Office
USG: United States Government