Homeland Security

DHS Cyber Preparedness eNewsletter

June 2006

Contents

Welcome to the first edition of the National Cyber Security Division's (NCSD) eNewsletter, a quarterly update on our collaborative activities and progress towards our two overarching priorities:

1. Leading implementation of an integrated cyber security risk management program.
2. Enhancing the National Cyberspace Security Response System.

2006 has already been a busy year for NCSD and our partners. In partnership with our public, private, and international stakeholders, we successfully conducted Cyber Storm, the largest cyber security exercise in history with 115 different organizations participating and examining their situational awareness and incident response capabilities. We hosted the second annual conference for Government Forum of Incident Response Security Teams (GFIRST), which brought together some of our nation's top information security professionals to share lessons learned and discuss strategies for enhancing the security of our government information systems. We also helped to solidify the Information Technology (IT) Sector component of the National Infrastructure Protection Plan (NIPP) and hosted inaugural meeting of the IT Sector Coordinating Council (SCC) and IT Government Coordinating Council (GCC). We look forward to rolling out the final NIPP Base Plan in the very near future and to our collaborative effort on development of the IT Sector Specific Plan.

My hope is that this eNewsletter will provide you with insights into our strategic collaborative initiatives for enhancing our nation's cyber security preparedness and response capabilities.

For those of you who have been working with us, I would like to thank you for your tireless efforts. I hope we can continue to work together. For those of you with whom we have not had the opportunity to engage, I hope you will join forces with us and our partners in our effort to protect our country's economic well being and ensure the safety and security of the American people.

With Best Wishes,

Andy Purdy
Acting Director,
National Cyber Security Division/US-CERT

Managing Cyber Risk

Critical infrastructure and key resources support the essential functions and services that underpin American society. Some critical infrastructure is so vital that its incapacitation, exploitation, or destruction, through a terrorist attack or natural disaster, could have a debilitating impact on our security and economic well-being.

The final draft of the National Infrastructure Protection Plan (NIPP) Base Plan is undergoing a final review and moving through the approval process. The NIPP was developed through coordination with security partners at all levels of government and in the private sector. The review process included two public comment periods in November 2005 and January 2006 for security partners to review the document and provide comments. The Final NIPP Base Plan is expected to be released Summer 2006.

The NIPP provides a consistent, unifying structure for integrating the current multitude of critical infrastructure protection (CIP) efforts into a single national program. The cornerstone of the NIPP is the risk management framework that establishes the processes for combining consequence, vulnerability, and threat information to produce a comprehensive and systematic assessment of national or sector risk. The results of these processes drive critical infrastructure and key resource (CI/KR) risk reduction and risk management activities. According to Secretary Michael Chertoff, Department of Homeland Security, "Risk management must guide our decision-making as we examine how we can best organize to prevent, respond, and recover from an attack."

The scope and framework of the NIPP are established in Homeland Security Presidential Directive 7 (HSPD-7), "Critical Infrastructure Identification, Prioritization, and Protection," issued in December 2003. HSPD-7 also designates DHS "as a focal point for the security of cyberspace." NCSD is facilitating this effort by actively pursuing and promoting a cyber risk management approach to enhance security and mitigate the risk of attacks across all CI/KR.

Effective and efficient public-private partnership provides the foundation for the NIPP and for securing cyberspace. In order to enhance the public-private partnership, Secretary Chertoff recently established the Critical Infrastructure Partnership Advisory Council (CIPAC) to facilitate interaction among government representatives at the Federal, State, local, and tribal levels and representatives from the community of CI/KR owners and operators for critical infrastructure protection. Additional information on the CIPAC is available through the Federal Register at http://www.gpoaccess.gov/fr/.

Under the NIPP framework, NCSD is the designated Sector Specific Agency (SSA) for the Information Technology (IT) Sector. NCSD and the IT Sector security partners are actively working to improve the security of the IT Sector by implementing the NIPP's risk management framework. This collaborative effort includes:

- Composing and maintaining the IT Sector Specific Plan (SSP);
- Assessing the risks to IT Sector critical infrastructure; and,
- Determining appropriate protective measures for the IT Sector.

NCSD is also responsible for leading cross-sector cyber security collaborative efforts under the NIPP. Other critical infrastructure sectors are the consumers of IT, and as such, are responsible for implementing cyber security within and for the cyber infrastructure that they use. The NCSD is assisting SSAs and other security partners with improving the cyber security of their respective CI/KR cyber assets. NCSD provides cyber guidance and methodologies to sectors to assist them in mitigating cyber risk (including cyber infrastructure vulnerabilities) and in developing effective and appropriate protective measures. This guidance includes:

- Contributing cyber elements to the NIPP Base Plan;
- Delivering cyber CIP training to SSAs and SSP authors to help them enhance the cyber aspects of their risk management efforts;
- Providing cyber expertise and content to various DHS risk assessment methodologies (e.g., Risk Analysis and Management for Critical Asset Protection [RAMCAP], the Comprehensive Review Program, and the Vulnerability Identification Self Assessment Tool [ViSAT]); and
- Reviewing SSPs to ensure sectors' CIP efforts address cyber assets and risks.

Under the NIPP framework, the NCSD has established three additional programs to manage cyber risk and improve the robustness of the nation's cyber security posture: the Internet Disruption Working Group (IDWG), the Control Systems Security Program (CSSP), and the Software Assurance Initiative.

- The IDWG was established by NCSD in partnership with the National Communications System (NCS), in response to security concerns surrounding the growing dependency of critical infrastructures and national security and emergency preparedness users on the Internet for communications, operational functions, and essential services. The IDWG's near-term objectives are to improve the resiliency and recovery of Internet functions in the event of a cyber-related incident of national significance; work with both government and private sector stakeholders to identify and prioritize protective measures necessary to prevent and respond to major Internet disruptions; and assess the operational dependencies of critical infrastructure sectors on the Internet. The 2005 IDWG Forum identified specific areas for action by both government and private sector stakeholders, including risk assessments, information sharing, protective measures, research and development, and Internet development issues. The IDWG is engaging with both public and private stakeholders to address these action items. The IDWG also plans to hold future forums and tabletop exercises, including an IDWG Tabletop Exercise, on June 15, 2006, to maintain both a pulse of the issues and an understanding of existing capabilities.

  For more information on the IDWG, please contact Michael Smith at mike.c.smith@dhs.gov

- NCSD's Control Systems Security Program (CSSP) is a specialized resource which addresses control systems cyber vulnerabilities. Control systems are computer-based systems used within many infrastructures and industries to monitor and control sensitive processes and physical functions. The CSSP develops and implements initiatives aimed at reducing risk and impacts of cyber attacks and incidents involving critical infrastructure control systems. It coordinates government and industry activities to facilitate control system incident management, provides timely situational awareness information, and manages control system vulnerability and threat reduction activities.

For more information on the CSSP, please email control-systems@us-cert.gov.

- The NCSD's Software Assurance Initiative, a comprehensive strategy that addresses people, process, technology, and acquisition throughout the software lifecycle, promotes more secure and better quality software products. Efforts to encourage a broader ability to routinely develop and deploy trustworthy software products through public-private partnerships make a significant contribution to securing cyberspace and our nation's critical infrastructure. These efforts will encourage the production of more secure and higher quality software by promoting the development of practical guidance, review tools, and research and development investment in cyber security. The overall goal is enabling secure and reliable software supporting mission requirements and, therefore, more resilient organizations. NCSD held its fourth Software Assurance forum on March 16-17, 2006, which brought together members of government, industry, and academia with vested interests in software assurance to discuss and promote integrity, security, and reliability in software.

  For more information on the Software Assurance Initiative, please contact Joe Jarzombek at joe.jarzombek@dhs.gov

The risk management initiatives described above are representative of broader efforts by NCSD to improve the security of cyberspace and to protect the nation's critical physical and cyber infrastructures. ◆

DHS Conducts First Full-Scale Cyber Security Exercise to Enhance Nation's Cyber Preparedness

The NCSD hosted the first government-sponsored National Cyber Exercise, Cyber Storm, in February, 2006. Cyber Storm was designed to exercise federal, state, private, and international security response and recovery mechanisms related to a cyber incident of national significance. The initiative is in accordance with an FY05 Congressional appropriations mandate to conduct exercises that test response to cyber attacks on critical infrastructures. The exercise acted as a catalyst for assessing and improving communications, coordination, and partnerships across infrastructure sectors and between private sector and government. Cyber Storm participants included members of the federal and state governments; members of the information technology, telecommunications, transportation and energy industries' private sector institutions, and several international partners. A total of 115 public, private, and international agencies, organizations, and companies were involved in the planning and implementation of Cyber Storm.

"Cyber security is critical to protecting our nation's infrastructure because information systems connect so many aspects of our economy and society," said George W. Foresman, DHS Under Secretary for Preparedness. "Preparedness against a cyber attack requires partnership and coordination between all levels of government and the private sector. Cyber Storm provides an excellent opportunity to enhance our nation's cyber preparedness and better manage risk."

Cyber Storm emphasized the Administration's commitment to

GFIRST Conference Unites Public and Private Incident Response Teams

The Government Forum of Incident Responders and Security Teams (GFIRST) successfully held its second annual conference in Orlando, Florida from April 30 – May 4. The theme of the conference, "GFIRST: A Nation Working Together to Secure Government Cyberspace," resonated with the crowd of GFIRST members, cyber incident responders, Chief Information Security Officers (CISO), private sector representatives, cyber security vendors, and law enforcement personnel. "It was information sharing at its best—I really appreciated the breadth and the depth of the topics covered—a well balanced agenda," stated Dennis Heretick, CISO, Department of Justice.

Robert Zitz, Special Assistant to the Undersecretary of Preparedness at DHS, opened the conference with a keynote on emergency preparedness and the importance of information sharing between the private and public sectors. Mr. Zitz was followed by Andy Purdy, Acting Director, National Cyber Security Division, who discussed various aspects of cyber preparedness and the need to build trust and collaboration for cyber preparedness. "Partnerships are the key to intra-government preparedness and cyber risk management," said Purdy.

The conference was managed and sponsored by NCSD's operations component, the United States Computer Emergency Readiness Team (US-CERT). The goal of the conference was to identify and improve information gathering and dissemination techniques, demonstrate proven information exchange methodologies, and provide superior training to incident responders, CISOs, and other players in the cyber security field.

To learn more about GFIRST and other US-CERT government initiatives, please visit http://www.us-cert.gov/federal/ or send an email to gfirst@us-cert.gov. ◆

cyber security and preparedness. The exercise simulated a sophisticated cyber attack through a series of scenarios directed against critical infrastructures. For example, one of the scenarios simulated a cyber incident where a utility company's computer system was breached, causing numerous disruptions to the power grid. The intent of this scenario was to highlight the interconnectedness of cyber security with the physical infrastructure and to exercise coordination and communication between the public and private sectors. Each of the scenarios was developed with the assistance of industry experts and was executed in a closed and secure environment.

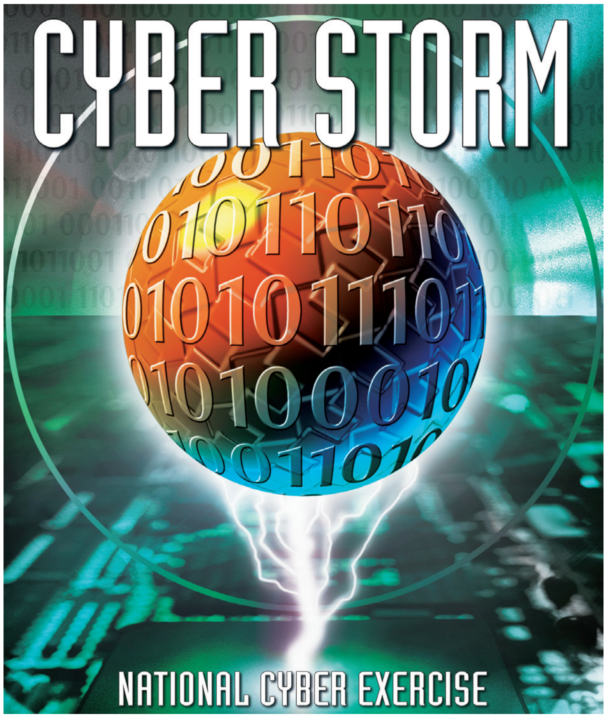
"With the proliferation of information technology and systems that provide the nervous system for the nation's critical infrastructure, the increasing integration and interdependencies between physical and cyber have important implications for economic and national security. The opportunity to exercise cyber preparedness, response, and recovery plans with both the public and private sector is an important part of securing the homeland. Federal, state, and international counterparts, along with the private sector, are all critical partners in our collective mission to reduce risk to the nation's information infrastructure," said Jeff Wright, Director, NCSD Exercise Program.

Cyber Storm exercised national cyber incident response within the context of a large-scale cyber incident affecting participating sectors. Capabilities examined, include:

- Interagency coordination through the National Cyber Response Coordination Group (NCRCG);
- Identification of policy issues that affect response and recovery;
- Identification of critical information sharing paths and mechanisms among public and private sectors; and
- Improvement and promotion of public and private sector interaction.

Some of the participant organizations, in addition to DHS components, included:

- Department of Commerce
- Department of Defense
- Department of Energy
- Department of State
- Department of Transportation
- Department of Treasury
- Department of Justice
- Director of National Intelligence
- Central Intelligence Agency
- National Security Agency
- National Security Council
- Homeland Security Council
- States of Michigan, Montana, and New York
- FBI
- U.S. Secret Service
- NORTHCOM
- American Red Cross
- Canada (PSEP-C)



The exercise was a simulated event, and there were no real world effects on, tampering with, or damage to any critical infrastructure. While the exercise scenario was based on a hypothetical situation, it was not intended as a forecast of future terrorist threats.

For additional information on Cyber Storm, please contact Jeffrey Wright, Director, NCSD Exercise Program at Jeffrey.Wright@dhs.gov or 703-235-5134. ◆

US-CERT—The Operations Component of NCSD

The United States Computer Emergency Readiness Team (US-CERT) is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and response to cyber attacks across the nation. US-CERT interacts with federal agencies, state and local governments, industry professionals, international counterparts, and others to improve information sharing and incident response coordination and to address threats and vulnerabilities to reduce our cyber risk.

US-CERT Operations provides the following functions:

- 24 x 7 x 365 triage support to federal, public, and private sectors, and the international community;
- cyber security event monitoring and predictive analysis;
- advanced warning on emerging threats;
- incident response capabilities for federal and state agencies;
- malware analysis and recovery support;
- trends and analysis reporting tools; and
- development and participation in national and international level exercises.

US-CERT Operations also manages the National Cyber Alert System, America's first cohesive system for identifying, analyzing, and prioritizing emerging vulnerabilities and threats. In addition to postings on the US-CERT website, warning information and cyber security updates are emailed to users who have subscribed to the mailing lists. Alerts are available at the technical and non-technical levels. The alerts can also be received via RSS and Atom feeds. Subscription to the National Cyber Alert System is free. To learn more and to sign up for the Alert System, visit http://www.us-cert.gov/cas/signup.html. ◆

US-CERT Situational Awareness

Increasing our cyber situational awareness is crucially important to our ability to detect and prevent cyber incidents before they can adversely impact our information infrastructure. As such, the DHS National Cyber Security Division (NCSD) has a situational awareness program in its U.S. Computer Emergency Readiness Team (US-CERT) Operations branch that includes monitoring government agency systems and assessing the overall health of the Internet. In order to do that, NCSD works closely with industry, government agency response teams, law enforcement, and key international partners to gather and analyze information across the Internet infrastructure. We are consistently working to increase our information sources through increasingly effective information sharing mechanisms. We work with our stakeholders in government and industry to determine the best way to share information that is useful and not over-burdensome for the receiver of that information, thereby improving the quality of the information that we share and use to enhance our overall preparedness and prevention efforts.

For more information about US-CERT, visit http://www.us-cert.gov. ◆

Useful Tools—The National Vulnerability Database

The National Vulnerability Database (NVD), available at http://nvd.nist.gov/, is a comprehensive cyber security database created by the National Institute of Standards and Technology (NIST) Computer Security Division and sponsored by the Department of Homeland Security's (DHS) National Cyber Security Division. The database was created to help system administrators and other security professionals stay informed about vulnerability information and assist them with incident management by providing a central repository of searchable information.

Created in 2005, the NVD includes a catalog of more than 15,000 vulnerabilities collected from Common Vulnerability Exposure (CVE), US-CERT, and Open Vulnerability Assessment Language (OVAL). They are all "CVE-compatible," meaning that they use CVE names to cross-link with other repositories that also use CVE names, facilitating the exchange of vulnerability information and making it easier to share data in a vendor-independent manner. Approximately 400 new vulnerabilities are published to the NVD web site each month.

Information from the NVD is incorporated into US-CERT's weekly security bulletin. To learn more, visit http://www.us-cert.gov/cas/bulletins/ to learn more. ◆

National Response Plan—Cyber Incident Annex

In December 2004, DHS released the National Response Plan (NRP) to align Federal coordination structures, capabilities, and resources into a unified, all discipline, and all-hazards approach to domestic incident management. To establish federal cyber security incident response procedures, DHS created a Cyber Incident Annex to the NRP (http://www.dhs.gov/interweb/assetlibrary/NRPbaseplan.pdf). This Annex is based on the National Cyberspace Security Response System—a public-private framework that provides mechanisms for rapid identification, information exchange, response, and remediation to mitigate the damage caused by malicious cyberspace activity.

The Cyber Incident Annex provides the framework for federal cyber incident response coordination among federal agencies and, upon request, state, local, tribal, and private sector entities. This framework may be utilized in any incident of national significance with cyber-related issues including cyber threats and disruptions, crippling cyber attacks against the Internet or critical infrastructure, technological emergencies, or Presidential declared disasters. The Annex established the National Cyber Response Coordination Group (NCRCG) to serve as the federal interagency body responsible for its implementation.

The NCRCG is co-chaired by DHS (with NCSD as the Executive Agent), the Department of Justice, and the Department of Defense and is comprised of senior representatives from federal agencies responsible for preventing, investigating, defending against, responding to, mitigating, and assisting in the recovery from cyber incidents. When activated, the NCRCG coordinates with the National Operations Center (NOC) and supports the member-agency department heads and the Executive Office of the President as appropriate. The NCRCG members will use integrated analysis and situational awareness of a cyber incident to govern response and remediation efforts and to guide senior policy makers.

More information on the National Response Plan and the Cyber Incident Annex can be found at: www.dhs.gov/dhspublic/interapp/editorial/editorial_0566.xml ◆

Cyber Preparedness Outreach and Awareness Efforts

Education Roundtable

DHS/NCSD is co-sponsoring a series of education roundtables with the National Cyber Security Alliance (NCSA) and the Cyber Security Industry Alliance (CSIA) on K-12 Cyber Security, Safety, and Ethics education. The roundtables bring together stakeholders to discuss strategies for implementing a national campaign to inform educators and parents about the need for teaching cyber security, safety and ethics courses in schools along with providing tips and guidelines they can use to teach children about how to stay safe online.

National Cyber Security Awareness Month Planning Begins

NCSD, and our government and industry partners in the National Cyber Security Alliance (NCSA), the Multi-State Information Sharing Analysis Center (MS-ISAC), and other organizations are planning initiatives for the third annual National Cyber Security Awareness Month in October 2006. The mission of this annual initiative is to raise awareness of safe cyber security practices so that computer users can improve their cyber security preparedness despite the ever changing threats. National Cyber Security Awareness Month is dedicated to raising cyber security awareness and preparedness levels amongst home users, small businesses, and education audiences (K-12 and higher education).

Last year, the activities of National Cyber Security Awareness Month reached more than 60 million Americans through the web, print, radio, and television. These efforts helped to push users toward NCSA's website staysafeonline.org—growing website traffic dramatically from 15,000 visitors to approximately 100,000 visitors in one month.

The Month demonstrates NCSD's commitment to sustaining successful public/private collaboration efforts. A few highlights from October 2005 include:

- NCSA and NCSD teamed on a Satellite Media Tour. This effort reached 14 live and taped interviews on "morning news programs" all over the country. Some of these news programs were played in major markets such as Washington, D.C.; Dallas, TX; and Cincinnati, OH.
- The MS-ISAC and NCSD's webcast "Protecting Our Children on the Internet- Being Cyber Smart in Cyber Space" was geared towards fourth and fifth grade students in which actors performed a cyber security-related skit and kids in the audience participated. The webcast had a high level of participation and raised cyber security awareness at the state and local level with school children across the country.
- The House of Representatives passed House Resolution 491, declaring October National Cyber Security Awareness Month.

- NCSA launched both a television Public Service Announcement and a Radio Public Service Announcement for Cyber Security awareness. These announcements were played across the U.S. during the Month and throughout 2005 and into 2006.

NCSD is actively preparing for October's 2006 National Cyber Security Awareness Month activities. We will be working with multiple stakeholders in government and in the private sector to directly reach out to home users, education audiences and small businesses.

"DHS would like to thank everyone who participated in the 2005 National Cyber Security Awareness Month," said Liesyl Franz, Deputy Director of NCSD for Outreach and Awareness. "We are looking forward to another successful Awareness Month in 2006 and continuing to work with our stakeholders to promote cyber security awareness among home users, small businesses, and students."

For more information on NCSD's Outreach and Awareness efforts, please contact Liesyl Franz, Deputy Director, Outreach and Awareness, NCSD, at Liesyl.franz@dhs.gov or (703) 235-5136. ◆

US-CERT Alerts

Keep informed and involved by subscribing to the products included in the US-CERT National Cyber Alert System. There are four different products available for various technical levels and needs:

- Technical Cyber Security Alerts - Technical alerts are for system administrators and experienced users, technical alerts provide timely information about current security issues, vulnerabilities, and exploits.
- Cyber Security Bulletins - Bulletins summarize information that has been published about new vulnerabilities. They are published weekly and are written primarily for system administrators and other technical users.
- Cyber Security Alerts - Written for home, corporate, and new users, these alerts are published in conjunction with technical alerts when there are security issues that affect the general public.
- Cyber Security Tips - Tips provide information and advice about a variety of common security topics. They are published monthly and are written primarily for home, corporate, and new users.

To find out more or to subscribe, please visit http://www.us-cert.gov/cas/signup.html ◆

Reporting Incidents to US-CERT

We encourage you to report any activities that you feel could meet the criteria for a cyber incident. Note that our policy is to keep any information specific to your site confidential unless we receive your permission to release that information. To find out more about reporting guidelines, or to report an incident, visit http://www.us-cert.gov or call 1-888-282-0870 ◆

NCSD Speaking Engagements

Listed are NCSD speaking engagements and events that are open to the public and press.

June 16, 2006

Deloitte Energy Conference

Washington, DC

Julio Rodriguez, Program Manager, Control Systems Program

http://www.deloitte.com/dtt/section_node/0,1042,sid%253D2206,00.html

June 26, 2006

IDGA's Critical Infrastructure Resilience Conference

Arlington, VA

Jeff Wright, Strategic Initiatives, Director Exercises

www.idga.org

June 27, 2006

18th Annual InfoSec Conference and Exhibit

New York City, NY

Andy Purdy, Acting Director, NCSD

www.aitglobal.com

July 11 & 13, 2006

Japan Anti-Cyber Crime/Anti-Cyber Terrorism Forum

Tokyo, Japan

Andy Purdy, Acting Director, NCSD

No website available

July 19, 2006

Network Security for Utilities

Atlanta, GA

Jerry Dixon, Deputy Director, US-CERT Operations

www.marcusevans.com

Cyber Preparedness Information Sheets—Now Available Online

Cyber preparedness information sheets are now available to download at your convenience. The information sheets include relevant information in a one-page format about Cyber Security Preparedness, US-CERT, the National Infrastructure Protection Plan, and Software Assurance. To download the .PDF files, visit, http://www.us-cert.gov/reading_room/distributable.html#dhs. ◆

The NCSD newsletter is a quarterly eNewsletter about the National Cyber Security Division at DHS. We welcome your feedback. If you have any comments about the newsletter or suggestions for items to include in future issues, please send them to: kristin.walters@associates.dhs.gov