Fact Sheet: Protecting America's Critical Infrastructure – Cyber Security

Release Date: 02/15/05

In February 2003, President George W. Bush issued the National Strategy to Secure Cyberspace. Recognizing the increasing danger posed by cyber threats and the devastating disruption that could result because of the interdependent nature of information systems that support our nation's critical infrastructure, the Strategy provides a strategic framework to prevent cyber attacks against America's critical infrastructures; reduce national vulnerability to cyber attacks; and minimize the damage and recovery time from cyber attacks should they occur. The Strategy outlines five national priorities including:

- A National Cyberspace Security Response System;
- A National Cyberspace Security Threat and Vulnerability Reduction Program;
- A National Cyberspace Security Awareness and Training Program;
- Securing Government Cyberspace; and
- National Security and International Cyberspace Security Cooperation.

The challenge to protect cyberspace is vast and complex and ultimately requires the efforts of all of us, recognizing that the threats are multi-faceted and global in nature, that the environment changes rapidly, and that information sharing and coordination are crucial to improving our overall national and economic viability. In less than two years since its creation, the Department of Homeland Security (DHS) has taken significant steps toward meeting the President's priorities and strengthening cyberspace security.

Building Cyber Security Operations

- Created the National Cyber Security Division (NCSD) in June 2003 to provide the federal government with a centralized cyber security coordination and preparedness function. The NCSD is the focal point for the federal government's interaction with state and local government, the private sector, and the international community concerning cyberspace vulnerability reduction efforts.
- Launched the United States Computer Emergency Readiness Team (US-CERT), a 24x7 operation that analyzes and disseminates threat information, works to reduce cyber vulnerabilities, and coordinates incident response. Receiving more than 100,000 visits each day, the US-CERT web site provides increased situational awareness for the cyber community.

National Cyber Security Response

- Established 24x7 Cyber Security Readiness and Response System responsible for tracking incident and trend data, ranking associated severity, generating real-time alerts, and maintaining on-going, real-time dialogue with US-CERT partners through the US-CERT portal, as well as outreach to the international community.
- Established the National Cyber Response Coordination Group (NCRCG), a forum of 13 principal agencies that coordinate intra-governmental and public/private preparedness operations to respond to and recover from large-scale cyber attacks.
- Created a formal annex to the National Response Plan to establish federal cyber security incident-response procedures.
- Co-sponsored Blue Cascades II and Purple Crescent II, two regional tabletop cyber exercises in Seattle, WA and New Orleans, LA. Each exercise brought together more than 200 government and private sector officials to examine cyber security readiness and response procedures, highlight the importance of cyber security in critical infrastructure protection, and discuss solutions for integrating physical security and cyber security. Region-specific coordination and communication plans between first responders, the federal government, and critical infrastructure owners/operators were exercised.
- Distribute a DHS/US-CERT daily unclassified briefing that contains a synopsis of noteworthy cyber-related activities over the past 24 hours to all US-CERT partners through the US-CERT portal.
- Developed a cyber guidance bulletin to coordinate and guide the sector-specific agencies in addressing cyber elements of their sector-specific critical infrastructure protection plans.

Cyber Security Education and Training

- Joined with the National Security Agency to co-sponsor the Centers of Academic Excellence in Information Assurance Education (CAEIAE) and expand the program at the national level. The CAEIAE program is improving the nation's pool of educated information assurance professionals to help prepare for, mitigate, respond to, and recover from cyber attacks. Currently, there are 52 universities in 26 states and the District of

respond to, and recover from cyber attacks. Currently there are 59 universities in 26 states and the District of Columbia designated as National Centers of Academic Excellence.
- Co-sponsor of the National Science Foundation Scholarship for Service Program, known as "Cyber Corps," to expand the ranks of the federal cyber workforce by providing scholarship grants to CAEIAE and other universities to fund information assurance education in return for student commitments to work for the federal government for two years. There are currently more than 300 Cyber Corps students enrolled at universities across the country.

Federal Governments Cyber Security Preparedness

- Created the Government Forum of Incident Response and Security Teams (GFIRST), a community made up of 40 government response teams responsible for securing government information technology systems.
- Launched the Einstein pilot program for cyber situational awareness, formerly known as Strategic Analysis Program at the Department of Transportation, to better monitor network security activity and increase global situational awareness at the Federal level.
- Co-hosted a Cyber Security Workshop with the National Defense University to improve coordination among government agencies in response to a national-level cyber attack. The workshop analyzed thresholds associated with convening the National Cyber Response Coordination Group and the use of the Cyber Annex to the National Response Plan.
- Played major role in Livewire in October 2003, the first-ever national-level cyber exercise to baseline government's capabilities for responding to national cyber attack. The exercise involved more than 300 participants representing more than 50 organizations across the federal, state, and local governments, and the private sector.
- Established the Chief Information Security Officers (CISO) forum to provide a venue for federal Information Security Officers to collaborate and leverage one another's experiences, capabilities, programs, lessons learned, and address and discuss cyber security problems or challenges.

Sharing Information with Private Sector, State and Local Partners

- Launched a national cyber security awareness effort in partnership with the Multi-State Information Sharing and Analysis Center, an information sharing organization among representatives of state and local governments that analyzes, sanitizes, and disseminates information pertaining to cyber events and vulnerabilities to its constituents and private industry through a series of conference calls and national webcasts. These webcasts examine critical and timely cyber security issues and assist home users and small businesses with improving their cyber security posture.
- Established the National Cyber Alert System to deliver targeted, timely, and actionable information to businesses and private citizens alike to better secure their computer systems. More than 270,000 direct subscribers have signed up to receive these alerts. These products provide timely information on computer security vulnerabilities, potential impacts and actions required to mitigate threats, and personal computer security "best practices" and "how to" guidance.
- Established a US-CERT Portal to serve as a communication mechanism that allows the safe sharing of sensitive cyber-related information with government and industry members on a real-time 24x7 basis.
- Facilitated and supported the Cybercop Portal, a group of more than 5,000 law enforcement members involved in electronic crimes investigations. Members represent all 50 States, working across all government agencies and more than 40 countries.
- Conduct a daily, secret-level conference call among multiple government agencies to discuss classified daily cyber intelligence data and increase information sharing among federal watch teams.

Standardizing Cyber Systems

- Implemented a process to maintain and support a Common Vulnerability & Exposure, Common Malware Enumerator, and Open Vulnerability Assessment Language to make security products more interoperable and to make response more efficient and effective. Completed compatibility process for more than 170 products and service offerings.
- Established the US-CERT Control Systems Center to bring together government, industry, and academia to reduce vulnerabilities, respond to threats, and foster public/private collaboration to improve the security of the data and process control systems that operate our nation's critical infrastructures.
- Established, the Control Systems Security and Test Center (CSSTC) in conjunction with Idaho National Environmental and Engineering Laboratory, to provide an opportunity for government and industry to collaborate on cyber vulnerability enumeration and reduction activities for control systems currently in use across critical infrastructure sectors. The CSSTC models map the cause and effect relationships of cyber attacks on control systems, assesses the outcomes of actual events in a simulated environment, and provides the US-CERT with

response and mitigation actions to share with partners in the control systems community.
- Launched a new Process Control Systems Forum as a joint effort between NCSD and Science & Technology, to bridge efforts between government and industry to accelerate the development of technology that will enhance the security, safety and reliability of process control and SCADA systems by providing a single venue for technologists from all user sectors to work together in evaluating, specifying, developing, refining and testing new technologies.

Collaborating with our International Partners

- Established regular International Information Sharing Conference calls with government cyber security policymakers and emergency response operations representatives from five key allied countries (US, UK, Australia, Canada, and New Zealand) to help participants prepare for and manage cyber incidents globally, improve overall situational awareness and early warning, and foster collaborative efforts on common strategic initiatives.
- DHS and the Germany Ministry of the Interior jointly hosted a Multilateral Cyber Security Conference in Berlin, Germany. The conference brought together cyber security policymakers, managers from computer security incident response teams with national responsibility, and law enforcement representatives responsible for cyber crime from 15 countries. The conference program included a facilitated tabletop exercise and interactive discussions on how to develop an international framework – as well as near term actionable steps – for watch, warning, and incident response.

Science and Technology Research Collaboration

- Science and Technology (S&T) Directorate has initiated an Internet Infrastructure Security Program. This program is engaged in research and development activities aimed at improving the security of the Domain Name System (DNS) and Internet routing protocols, two of the basic components that underlie communication on the Internet. Ongoing efforts in this program are focused on enabling the migration from existing protocols associated with DNS and routing infrastructure to more secure versions of these protocols.
- Science and Technology Cyber Security Testbed Program has established two multi-university testbed projects, with co-funding from the National Science Foundation. The first project is developing a large-scale network testbed to provide an experimental infrastructure for cyber security research testing. The second involves the development of software-based testing system, designed to assess the impact of cyber attacks as well as the testing and evaluation of defensive security technologies and approaches.
- Science and Technology supported a first-of-its-kind study performed by the United States Secret Service and Carnegie Mellon University's Software Engineering Institute analyzing insider threats and insider activities affecting information systems and data in critical infrastructure sectors. This comprehensive analysis of the behavioral and technical aspects of the threat will help prevent serious crimes such as network intrusions, identity theft, and financial fraud.

The U.S. Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) Directorate serves as the focal point for intelligence analysis, infrastructure protection operations, and information sharing. IAIP merges the capability to identify and assess a broad range of intelligence and information concerning threats to the homeland, maps that information against the nation's vulnerabilities, issues timely and actionable warnings, and takes appropriate preventive and protective measures to protect our infrastructures and key assets.