Preventing and Defending Against Cyber Attacks
November 2010

The Nation's first ever Quadrennial Homeland Security Review (QHSR), delivered to Congress in February 2010, identified "safeguarding and securing cyberspace" as one of the Nation's five priority homeland security missions.

The Department of Homeland Security (DHS) is responsible for helping Federal Executive Branch civilian departments and agencies secure their unclassified networks (.gov). DHS also works with owners and operators of critical infrastructure and key resources (CIKR)—whether private sector, state, or municipality-owned—to bolster their cybersecurity preparedness, risk assessment and mitigation and incident response capabilities.

Cybersecurity Coordination and Outreach

National Cyber Incident Response Plan
The President's Cybersecurity Policy Review called for *"a comprehensive framework to facilitate coordinated responses by Government, the private sector, and allies to a significant cyber incident."* DHS coordinated the interagency, state and local government, and private sector working group that developed the National Cyber Incident Response Plan.

The Plan provides a framework for effective incident response capabilities and coordination between federal agencies, state and local governments, the private sector, and international partners during significant cyber incidents. It is designed to be flexible and adaptable to allow synchronization of response activities across jurisdictional lines.

National Cybersecurity and Communications Integration Center
In October 2009, DHS established the National Cybersecurity and Communications Integration Center, a 24-hour, DHS-led coordinated watch and warning center, to serve as the Nation's principal hub for organizing cyber response efforts and maintaining the national cyber and communications common operational picture.

- The NCCIC combines two of DHS's operational organizations: the U.S. Computer Emergency Readiness Team (US-CERT) and the National Coordinating Center for Telecommunications (NCC), the operational arm of the National Communications System.
- It also integrates the efforts of DHS's National Cybersecurity Center (NCSC), which coordinates operations among the six largest federal cyber centers, the DHS Office of Intelligence and Analysis and private sector partners.
- Additional representatives from federal agencies, the private sector and state and local governments are also collocated at the NCCIC.

U.S. Computer Emergency Readiness Team
DHS's U.S. Computer Emergency Readiness Team (US-CERT) provides response support and defense against cyber attacks for the Federal Civilian Executive Branch (.gov) networks. US-CERT also collaborates and shares information with state and local government, industry and international partners to address cyber threats and develop effective security responses.

Critical Infrastructure and Key Resources
DHS works to ensure the systems that support critical infrastructure and key resources (CIKR) – the essential functions that underpin American society – are protected from cyber threats.

- The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides onsite support to owners and operators of critical infrastructure for protection against and response to cyber threats, including incident response, forensic analysis, and site assessments. ICS-CERT also provides tools and training to increase stakeholder awareness of evolving threats to industrial control systems.
- In August 2009, DHS and the Information Technology Sector Coordinating Council released the IT Sector Baseline Risk Assessment (ITSRA) to identify and prioritize national-level risks to critical sector-wide IT functions while outlining strategies to mitigate those risks and enhance national and economic security.
    - The ITSRA validated the resiliency of key elements of IT sector infrastructure while providing a process by which public and private sector owners and operators can continually update their risk management programs.
    - The ITSRA links security measures to concrete data to provide a basis for meaningful infrastructure protection metrics.

Cybersecurity Initiatives and Exercises

The EINSTEIN Program
The EINSTEIN system is designed to provide the U.S. Government with an early warning system for intrusions to Federal Executive Branch civilian networks, near real-time identification of malicious activity, and automated disruption of that malicious activity.

- EINSTEIN 1: The first iteration of the EINSTEIN system was developed in 2003 and automates the collection and analysis of computer network security information from participating agency and government networks to help analysts identify and combat malicious cyber activity that may threaten government network systems, data protection and communications infrastructure.
- EINSTEIN 2: The second phase of EINSTEIN, developed in 2008, incorporated intrusion detection capabilities into the original EINSTEIN system. DHS is currently deploying EINSTEIN 2 to federal executive branch civilian agencies and Networx Managed Trusted Internet Protocol Services (MTIPS) providers, private internet service providers that serve federal agencies, to assist them with protecting their computers, networks and information.
- EINSTEIN 3: DHS is currently testing the technology for the third phase of the EINSTEIN intrusion prevention system, which will provide DHS with the ability to automatically detect and disrupt malicious activity before harm is done to critical networks and systems.

Trusted Internet Connections Initiative
As part of the President's Comprehensive National Cybersecurity Initiative (CNCI), DHS works with the Office of Management and Budget (OMB) to reduce and consolidate the number of external connections to the Internet that federal agencies have to the Internet through the Trusted Internet Connections (TIC) initiative.

- This initiative reduces the number of potential threats to government networks and allows DHS to focus monitoring efforts on limited and known avenues through which Internet traffic must travel.

National Strategy for Trusted Identities in Cyberspace
In July 2010, DHS and the White House published a draft National Strategy for Trusted Identities in Cyberspace – which seeks to secure the identities of individuals, organizations, services and devices during online transactions, as well as the infrastructure supporting the transaction – fulfilling one of the near-term action items of the President's *Cyberspace Policy Review*.

- The Strategy supports the protection of privacy and civil liberties by enabling only the minimum necessary amount of personal information to be transferred in any particular transaction.

Intergovernmental Partnerships
DHS works closely with its federal and state partners to protect government cyber networks.

- In August 2009, the DHS National Cybersecurity Center developed a prototype "cyber wiki" – a web-based tool for federal departments and agencies to collaborate on cyber incident reporting and analysis in real time.
- In December 2009, DHS initiated a first-of-its-kind federal-state cybersecurity partnership to deploy DHS's EINSTEIN 1 cybersecurity system to the state of Michigan's government networks. As part of the partnership with Michigan, DHS's U.S. Computer Emergency Readiness Team (US-CERT) will identify possible abnormal activities on Michigan's networks and address threats to critical cyber infrastructure—strengthening defenses against cyber attacks and the overall resiliency of Michigan's networks and cyber resources.
- DHS and OMB work cooperatively with agencies across the federal government to coordinate the protection of the nation's federal information systems through compliance with the Federal Information Security Management Act of 2002.
- In October 2010, DHS and the Department of Defense (DoD) signed a memorandum of agreement that aligns and enhances America's capabilities to protect against threats to our critical civilian and military computer systems and networks, including deploying a DoD support team to the NCCIC to enhance the National Cyber Incident Response Plan and sending a full-time senior DHS leader and support team to DoD's National Security Agency.
- In November 2010, the Multi-State Information Sharing and Analysis Center (MS-ISAC) opened their Cyber Security Operations Center, a 24-hour watch and warning facility, which is similar to the Department-led NCCIC and facilitates information sharing between and among the federal government and state, local, tribal and territorial governments.

Public-Private Partnerships and Information Sharing
Private industry owns and operates the vast majority of the nation's critical infrastructure and cyber networks. Consequently, the private sector plays an important role in cybersecurity, and DHS has initiated several pilot programs to promote public-private sector collaboration.

- In February 2010, DHS, the Department of Defense, and the Financial Services Information Sharing and Analysis Center launched a pilot designed to help protect key critical networks and infrastructure within the financial services sector by sharing actionable, sensitive information.
- In June 2010, DHS implemented the Cybersecurity Partners Local Access Plan, which allows security-cleared owners and operators of CIKR, as well as state technology officials and law

enforcement officials, to access secret-level cybersecurity information and video teleconference calls via local fusion centers.

- In November 2010, DHS signed an agreement with the Information Technology Information Sharing and Analysis Center (IT-ISAC) to embed a full-time IT-ISAC analyst and liaison to DHS at the NCCIC. The IT-ISAC consists of information technology stakeholders from the private sector and facilitates cooperation among members to identify sector-specific vulnerabilities and risk mitigation strategies.

Cyber Storm III

In September 2010, DHS will host Cyber Storm III, a response exercise in which members of the cyber incident response community address the scenario of a coordinated cyber event in which the National Cyber Incident Response Plan is activated, testing the National Cybersecurity and Communications Integration Center and the federal government's full suite of cybersecurity response capabilities.

Stop. Think. Connect. National Cybersecurity Awareness Campaign

In October 2010, DHS launched the "Stop. Think. Connect." public cybersecurity awareness campaign—a national public education campaign designed to increase public understanding of cyber threats and how individual citizens can develop safer cyber habits that will help make networks more secure. The campaign fulfills a key element of President Obama's 2009 Cyberspace Policy Review, which tasked DHS with developing a public awareness campaign to inform Americans about ways to use technology safely.

Promoting Public Awareness of Cybersecurity

DHS is committed to developing innovative new ways to enhance public awareness about the importance of safeguarding America's computer systems and cyber networks from attacks.

- In March 2010, Secretary Napolitano launched the National Cybersecurity Awareness Challenge—which called on members of the public and private sector companies to develop creative and innovative ways to enhance awareness of the importance of cybersecurity and safeguard America's computer systems and networks from attacks.
- In July 2010, seven of the more than 80 proposals were selected and recognized at a White House ceremony. The winning proposals will help inform the National Cybersecurity Awareness Campaign, which is designed to engage the American public, the private sector and state and local governments in efforts to guard against cyber threats and communicate strategies for the public to help keep themselves, their families and communities safer online.
- The Campaign will kick off in October 2010, in conjunction with National Cybersecurity Awareness Month – every October, DHS and its public and private sector partners promote efforts to educate citizens about guarding against cyber threats.

Cybersecurity Workforce Development

DHS is moving aggressively to build a world-class cybersecurity team.

- DHS's National Cybersecurity Division tripled its federal workforce from 35 to 118 in fiscal year 2009 and is on track to nearly double that number in FY 2010.

- DHS and the National Security Agency co-sponsor the Centers of Academic Excellence in Information Assurance Education and Research programs, the goal of which are to produce a growing number of professionals with information assurance expertise in various disciplines.
- DHS and the Department of State co-hosted Operation Cyber Threat (OCT1.0), the first in a series of Government-wide experiential and interactive cybersecurity training pilots designed to apply learning concepts and share best practices in a secure, simulated environment to build capacity within the federal workforce.

Privacy and Civil Liberties

DHS is committed to supporting the public's privacy, civil rights, and civil liberties. Accordingly, the Department has implemented strong privacy and civil rights and civil liberties standards into all its cybersecurity programs and initiatives from the outset.

- DHS established an Oversight and Compliance Officer within the Office of Cybersecurity and Communications.
- Key personnel receive specific training on the protection of privacy and other civil liberties as they relate to computer network security activities.
- In an effort to increase transparency, DHS has published on its Web site, www.dhs.gov, privacy impact assessments of all of its cybersecurity systems.