Homeland Security

NIPP-Cyber Security

Implementing the National Infrastructure Protection Plan

Critical Infrastructure and Key Resources (CI/KR) support the essential functions and services that underpin American society. Some CI/KR elements are so vital that their destruction, incapacitation, or exploitation could have a debilitating impact on national security and economic well-being. Homeland Security Presidential Directive-7 (HSPD-7), "Critical Infrastructure Identification, Prioritization, and Protection," issued in December 2003, directs Homeland Security to produce a comprehensive, integrated national plan for CI/KR protection. HSPD-7 also designates Homeland Security as a national focal point for the security of cyberspace.

The NIPP Helps Protect Our Critical Infrastructure

In response to HSPD-7, Homeland Security and its public and private sector partners developed and are implementing the National Infrastructure Protection Plan (NIPP). The NIPP Base Plan[1] and its complementary Sector-Specific Plans (SSP) provide a consistent, unifying structure for integrating current and future CI/KR protection efforts. The NIPP acknowledges that the U.S. economy and national security are highly dependent upon the cyber infrastructure because it enables the Nation's essential services. The term "cyber" refers to electronic information and communications systems and the information contained therein. To reflect the increasing convergence of IT and communication networks, the Department's cyber security division works closely with the National Communications System (NCS) to address cyber related issues. While the use of innovative technology and interconnected networks in operations improves productivity and efficiency, it also increases the Nation's risk to cyber threats if cyber security is not addressed and integrated appropriately. To address this cyber risk, the NIPP includes an IT Sector responsibility as well as a cross-sector cyber element.

Improving the Security of the IT Sector

The IT Sector produces and provides hardware, software, IT systems and services, and the Internet. The Department's cyber security division is the Sector Specific Agency (SSA) for the IT Sector and leads the IT Sector Government Coordinating Council (GCC). The Department's cyber security division and the IT GCC collaborated with the IT Sector Coordinating Council (SCC) to develop the IT Sector Specific Plan (SSP). The IT SSP is a policy and planning document that provides guidance on how public and private partners will work together to protect IT Sector CI/KR. The Department's cyber security division is also responsible for producing an IT Sector CI/KR Protection Annual Report. This report provides an operational perspective of the sector by communicating the IT Sector's protection efforts, the sector's priorities and needs that drive these efforts, and how such efforts are funded.

For critical infrastructure protection efforts to be successful there must be integrated and effective public-private partnerships. Security partners are encouraged to participate in the appropriate planning and information mechanisms described below to support effective CI/KR protection.

- **IT SCC:** Provides a framework for private sector IT infrastructure owners and operators and supporting associations to engage with Homeland Security and the IT GCC.
- **IT GCC:** Provides a forum for interagency communication, coordination, and partnership with Homeland Security, the Department's cyber division, and the supporting Federal departments and agencies that have a role in protecting the IT Sector.
- **IT Information Sharing and Analysis Center (IT-ISAC):** Provides operational and tactical capabilities for information sharing and support for incident response activities.
- **United States – Computer Emergency Readiness Team (US-CERT):** Coordinates defense against and responses to cyber attacks across the nation; operates as a focal point for Federal, state, and local governments' operational information sharing.

Helping Address Cross-Sector Cyber Risk

The cross-sector cyber responsibility is a collaborative effort between the Department's cyber security division, SSAs, and other security partners to improve the cyber security of the CI/KR by facilitating cyber risk reduction activities. The Department's cyber security division

[1] http://www.dhs.gov/NIPP

provides cyber guidance to all sectors to assist them in understanding and mitigating cyber risk and in developing effective and appropriate protective measures.

In addition to the SSAs' efforts, cyber security is a concern to individuals because of their increasing reliance on the cyber infrastructure, including the Internet. Individuals play a significant role in managing the security of their computer systems and preventing attacks against CI/KR. Therefore, Homeland Security's cyber security public awareness efforts are key to reducing overall cyber risk.

Working Together to Secure Cyberspace

Homeland Security is committed to working collaboratively with other public, private, academic, and international entities to enhance cyber security awareness and preparedness efforts, and ensure that the cyber elements of CI/KR are:

- Robust enough to withstand attacks without incurring catastrophic damage;
- Responsive enough to recover from attacks in a timely manner; and
- Resilient enough to sustain nationally critical operations.

Obtaining Additional Information

To learn more about the cyber security in the NIPP, contact the Department's cyber security division at **IT.Sector@dhs.gov**

Cyber security is a shared responsibility. Working together, we can secure America's cyberspace.