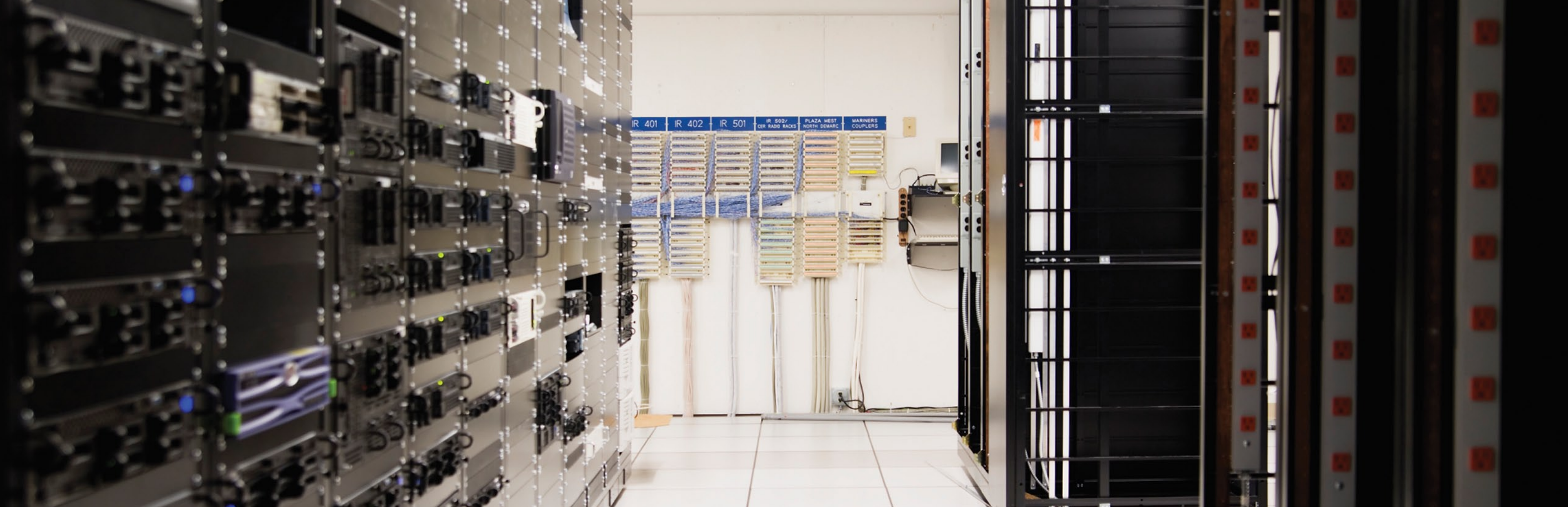

National Infrastructure Protection Plan

Information Technology Sector

Homeland Security Presidential Directive 7 (HSPD-7) identified 17 critical infrastructure and key resources (CIKR) sectors and designated Federal Government Sector-Specific Agencies (SSAs) for each of the sectors. Each sector is responsible for developing and implementing a Sector-Specific Plan (SSP) and providing sector-level performance feedback to the Department of Homeland Security (DHS) to enable gap assessments of national cross-sector CIKR protection programs. SSAs are responsible for collaborating with public and private sector security partners and encouraging the development of appropriate information-sharing and analysis mechanisms within the sector.

Sector Overview

The Information Technology (IT) Sector is central to the Nation's security, economy, and public health and safety. Businesses, governments, academia, and private citizens are increasingly dependent upon IT Sector functions. These virtual and distributed functions produce and provide hardware, software, and IT systems and services, and—in collaboration with the Communications Sector—the Internet. The IT Sector functions are operated by a combination of entities—often owners and operators and their respective associations—that maintain and reconstitute the network, including the Internet. The Internet encompasses the global infrastructure of packet-based networks and databases that use a common set of protocols to communicate. The networks are connected by various transports, and the availability of these networks and services is the collective responsibility of the IT and Communications Sectors. DHS is the SSA for the IT Sector.

Sector Partnerships

DHS recognizes that public-private partnerships provide the foundation for securing the IT Sector's infrastructure. The sector partnership model, as outlined in the NIPP, encourages collaboration through the respective private sector and government coordinating councils to coordinate CIKR protection activities.

Formally chartered in January 2006, the IT Sector Coordinating Council (SCC) consists of private companies and associations from across the sector, as well as the IT Information Sharing and Analysis Center (IT-ISAC). The IT SCC is self-organized, self-run, and self-governed. It enables owners and operators to coordinate on a wide range of sector-specific strategies, policies, activities, and issues across the public and private sectors.

Chaired by DHS and established in April 2005, the IT Government Coordinating Council (GCC) includes representatives from the Departments of Commerce, Defense, Homeland Security, Justice, State, and Treasury; the National Institute of Standards and Technology; the Office of the Director of National Intelligence; and the Office of Management and Budget. In addition, representatives from State and local governments, including the National Association of State Chief Information Officers and the Metropolitan Information Exchange, participate in the IT GCC.

CIKR Protection Issues

The IT Sector is a key enabler for U.S. and global economies, and its products and services are relied on by all critical infrastructure sectors. Because of this reliance, IT Sector public and private security partners are actively engaged to ensure the resiliency of the sector and prevent and protect against incidents that could have negative economic consequences or degrade public confidence.

Priority Programs

A number of programs contribute to securing cyberspace and support efforts to ensure a resilient and available IT infrastructure. Included among these are:

- **United States Computer Emergency Readiness Team (US-CERT):** Established in 2003 to protect the Nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the Nation. US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.
- **IT-ISAC:** For operations, analysis, and information sharing, the IT-ISAC is recognized and endorsed by the IT SCC as the lead for the IT private industry. The IT-ISAC has served since 2001 and will continue to serve as a vehicle for communicating information about threats, vulnerabilities, and incidents to private industry within the IT Sector.
- **National Cyber Exercises:** DHS conducts exercises to identify, test, and improve coordination of the cyber incident response community, including Federal, State, Territorial, local, tribal, and international government elements, as well as private sector corporations and coordinating councils. Cyber Storm II was the Nation's largest, most comprehensive cyber exercise. The exercise involved more than 2,500 participants worldwide representing 18 federal agencies, 40 U.S. companies, 9 states, 10 Information Sharing and Analysis Centers (ISACs), and 5 countries. Results of Cyber Storm II will be used to strengthen cyber security efforts across all CIKR sectors.

DHS, other Federal departments and agencies, State and local governments, academia, and the private sector manage a number of protective programs that support IT Sector situational awareness, risk management, and response, recovery, and reconstitution goals. The IT SSP provides greater detail about these key protective programs and identifies gaps where additional protective programs are needed to fully meet IT Sector goals.

Homeland Security

For questions or more information, please contact NIPP@dhs.gov or visit www.dhs.gov/nipp.