



National Infrastructure Protection Plan

Information Technology Sector

The Information Technology (IT) Sector is one of 18 critical infrastructure sectors established under the authority of Homeland Security Presidential Directive 7 (HSPD-7). Each sector is managed by a Sector-Specific Agency (SSA) that provides sector-level performance feedback to the Department of Homeland Security (DHS) to enable assessment of national, cross-sector critical infrastructure protection and resilience programs. In accordance with the National Infrastructure Protection Plan (NIPP), each SSA is responsible for developing and implementing a Sector-Specific Plan (SSP), in collaboration with public and private sector partners, and for encouraging the development of appropriate information-sharing and analysis mechanisms.

Sector Overview

The IT Sector is central to the Nation's security, economy, 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 sector's complex and dynamic environment makes identifying threats and assessing vulnerabilities difficult and requires that these tasks be addressed in a collaborative and creative fashion. The IT Sector functions are operated by a collaboration of entities—often owners and operators and their respective associations—that maintain and reconstitute the network, including the Internet. Although the IT infrastructure has a certain level of inherent resilience, its interdependent and interconnected structure presents challenges as well as opportunities for coordinating public and private sector preparedness and protection activities.

Sector Partnerships

The IT Sector implements the NIPP by ensuring the Internet infrastructure and the Nation's IT infrastructure

are secure through collaboration with sector partners, including IT Sector associations and agencies spanning all levels of government.

The IT Sector Government Coordinating Council (GCC) and the IT Sector Coordinating Council (SCC) are the primary bodies for communicating their respective public and private perspectives, and developing collaborative policies, strategies, and security efforts to advance critical infrastructure protection. Formally chartered in January 2006, the IT SCC consists of private companies and associations from across the sector, as well as the IT Information Sharing and Analysis Center. The IT SCC is self-organized, self-run, and self-governed. Chaired by DHS and established in April 2005, the IT GCC includes representatives from DHS and the Departments of Commerce, Defense, Justice, State, and Treasury; the National Institute of Standards and Technology; and the Office of the Director of National Intelligence. In addition, representatives from State and local governments, including the National Association of State Chief Information Officers and the State, Local, Tribal, and Territorial Government Coordinating Council, participate in the IT GCC.

In March 2006, DHS established the Critical Infrastructure

Partnership Advisory Council to facilitate coordination and dialogue between SCC and GCC representatives to share experiences, ideas, best practices, and innovative approaches related to critical infrastructure protection and risk management for their respective sectors.

Critical Infrastructure 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 partners from the public and private sectors are actively engaged to ensure the resilience of the sector and prevent and protect against incidents that could have negative economic consequences or degrade public confidence.

IT Sector Risk Assessment and Risk Management Activities

Public and private sector owners and operators completed the first-ever functions-based IT Sector Baseline Risk Assessment in August 2009. This assessment describes risks from manmade deliberate, manmade unintentional, and natural threats to producers and providers of IT hardware, software, and services using threat, vulnerability, and consequence frameworks. The IT Sector Risk Assessment (ITSRA) resulted in an IT Sector Risk Profile that identifies national-level risks of concern for the IT Sector. Public and private sector partners collaboratively developed the assessment, which reflects the expertise of participating subject matter experts (SMEs).

Using the risks identified in the ITSRA, IT Sector partners are systematically developing sector-level responses to risks of concern for each critical function by engaging in risk management analyses. These responses will identify a portfolio of risk management activities identified by sector SMEs to yield the greatest potential reduction in evaluated risks, to be promoted across the IT Sector.

Critical IT Sector Functions

- IT products and services
- Incident management capabilities
- Domain name resolution services
- Identity management and associated trust support services
- Internet-based content, information, and communications services
- Internet routing, access, and connection services

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



Homeland
Security