Fact Sheet

INFORMATION TECHNOLOGY SECTOR BASELINE RISK ASSESSMENT

PURPOSE: The Information Technology (IT) Sector Baseline Risk Assessment provides an evaluation of risk to the IT Sector infrastructure, specifically critical IT Sector functions. The IT Sector Risk Assessment (ITSRA) provides an all-hazards risk profile that public and private IT Sector partners can use to inform resource allocation for research and development and other protective measures, which enhance the security and resiliency of the critical IT Sector functions. By increasing the awareness of risks across the public and private sectors, the Baseline Risk Assessment is the foundation for ongoing national-level collaboration to enhance the security and resiliency of the critical IT Sector functions.

APPROACH: The ITSRA utilized a top-down and functions-based approach to develop a national-level understanding of, and baseline for managing risk to the sector and to prioritize risk for the six critical IT Sector functions:

- Producing and providing IT products and services;
- Providing incident management capabilities;
- Providing domain name resolution services;
- Providing identity management and associated trust services;
- Providing Internet-based content, information and communications services; and
- Providing Internet routing, access and connection services.

FINDINGS: The ITSRA validated the resiliency and redundancy of key elements of the IT Sector's infrastructure while also providing a process by which public and private sector owners and operators can continually update their risk management programs. The assessment further identified significant interdependencies between critical functions. While the assessment noted several "high" risks to critical IT functions, the ITSRA also determined that it is unlikely that any of these risks would lead to the complete failure of any critical IT Sector functions.

PROCESS: Subject matter experts from public and private sector entities engaged in a collaborative and iterative process to develop, pilot, and revise a methodology to jointly assess risk, identify national level consequences to the critical functions, conduct consequences and vulnerability analysis, and use the results to write the ITSRA. The public-private collaboration on the ITSRA represents a significant achievement through the Department of Homeland Security's National Infrastructure Protection Plan (NIPP) partnership model. The IT Sector will evaluate lessons learned and will continue to update the ITSRA. The IT Sector is already using the results

of the ITSRA to inform work in other areas such as R&D, development of protective programs and the establishment of metrics to measure the IT Sector's security posture.

BACKGROUND: Homeland Security Presidential Directive-7 established a national policy for Federal departments and agencies to identify and prioritize critical infrastructure and key resources (CIKR) throughout the United States and to protect those resources from attack. DHS' National Cyber Security Division (NCSD) serves as the Sector Specific Agency for the IT sector.