

APPENDIX 2: INFORMATION TECHNOLOGY SECTOR

Sector Description

Information Technology (IT) in today's society enables a variety of routine functions and services across all walks of life. While many aspects of IT often overlap with the telecommunications, IT is considered a separate sector. The Information Technology Sector produces hardware, software, and services that enable other sectors to function. For example, the IT Sector produces laptops, operating systems, and Internet search engines. These IT Sector products are consumed across other critical infrastructure sectors and the government. The *production* of hardware, software, and services therefore comprises the IT Sector; the IT Sector may be considered as the "IT Industrial Base." The Internet is a Key Resource in which the IT Sector and the Telecommunications Sector have a shared responsibility. Other infrastructure sectors also contain IT resources that may or may not be integrated with telecommunication resources. Those cyber⁹ resources enable functionality of assets within all sectors. Standard security concepts (e.g., confidentiality, integrity, and availability) must be maintained for all cyber-based infrastructures in each sector. By viewing IT as its own sector, the people, facilities, and cyber-based systems that make IT possible will be assured protection.

Results of Infrastructure Interruptions

- Control System failures.
- Computer Hardware, Software, Application, Database failures.
- Network component, power related issues.
- Facility access, security related issues.
- Banking and Finance network (direct deposit, ATMs, credit/debit cards) failures.
- Cascading impact on many telecommunications services.
- 911 Dispatch would be inoperable.
- Many government functions would halt.
- Citizens of Region 6 will not be able to contact government agencies or each other.

Regional Service Providers Active in CIP

- Cingular Wireless
- City of Bellevue
- City of Kent
- City of Redmond
- City of Renton
- City of Seattle
- Global Telematics

⁹ **Cyber** - Electronic information and communications systems and the information contained therein. Information and communication systems are comprised of all the hardware and/or software that processes, stores, and communicates (or any combination thereof) information. *Processing* includes the creation, modification, and destruction of information; *Storage* includes all media types (paper, magnetic, and electronic); *Communication* includes sharing and distribution of information.

- King County
- Microsoft
- Qwest Communications
- Westin Building

Current Information Sharing Mechanisms

- Information Technology - Information Sharing and Analysis Center, (<http://www.it-isac.org>)
- ACCIS of the State of Washington, (<http://www.accis-wa.org>)
- Association of Contingency Planners (ACP), Washington State Chapter, (<http://www.acp-wa-state.org/>)
- Information Processing Management Association (IPMA), (<http://www.ipma-wa.com>)
- InfraGard, (<http://infraguard.net/>)
- Pacific Northwest Economic Region (PNWER), (<http://www.pnwer.org>)
- NWWARN, (<https://www.nwwarn.gov>)

Common Vulnerability Assessment Tools

- Disaster Recovery Institute (DRI) International Vulnerability Assessment Guidelines
- Business Continuity Institute (BCI) Guidelines
- International Standards Organization (ISO) 17799 and its predecessor British Standard 7700. British Standard 7799 became ISO/IEC 17799 on November 30, 2000.
- CARVER + Shock VAM, The CARVER + Shock methodology. CARVER was originally developed by the US Special Forces.
- HLS-CAM, HLS-CAM Criticality developed by the West Virginia National Guard based on the DTRA JSIVA model modified to the civilian sector along with the Florida Domestic Security Task Force Comprehensive Vulnerability Assessment.
- IAPVA, IAP VA methodology developed by the Joint Program Office – Special Technology Countermeasures.
- State Vulnerability Assessment Methodology, The State Vulnerability Assessment (VA) Methodology developed by Argonne National Laboratory for the Department of Homeland Security (DHS) (2003).
- SVA-Pro, developed by Dyadem International Ltd. (2003).
- Terrorism VSAT, Developed by the North Carolina Department of Agriculture and Consumer Services for the North Carolina agri-business community.
- VAF, prepared under contract for the Critical Infrastructure Assurance Office by KPMG Peat Marwick LLP (1998).