

Appendix 5B: Recommended Homeland Security Practices for Use by the Private Sector

This appendix provides a summary of practices that may be adopted by private sector owners and operators to improve the efficiency and effectiveness of their CI/KR protection programs. The recommendations herein are based on best practices currently in use by various sectors and other groupings. The NIPP encourages private sector owners and operators to adopt and implement those practices that are appropriate and applicable at the specific sector enterprise and individual facility levels:

- **Asset, System, Network, and Function Identification:**

- Incorporate the NIPP framework for the assets, systems, and networks under their control; and
- Voluntarily provide CI/KR-related data to DHS to facilitate national CI/KR protection program implementation with appropriate information protections.

- **Assessment, Monitoring, and Reduction of Risks/Vulnerabilities:**

- Conduct appropriate risk and vulnerability assessment activities using tools or methods that are rigorous, well-documented, and based on accepted practices in industry or government;
- Implement measures to reduce risk and mitigate deficiencies and vulnerabilities corresponding to the physical, cyber, and human security elements of CI/KR protection;
- Maintain the tools, capabilities, and protocols necessary to provide an appropriate level of monitoring of networks, systems, or a facility and its immediate surroundings to detect possible insider and external threats;
- Develop and implement personnel screening programs to the extent feasible for personnel working in sensitive positions; and

- Manage the security of computer and information systems while maintaining awareness of vulnerabilities and consequences to ensure that systems are not used to enable attacks against CI/KR.
- **Information Sharing:**
 - Connect with and participate in the appropriate national, State, regional, local, and sector information-sharing mechanisms (e.g., HSIN-CS and the sector information-sharing mechanism);
 - Develop and maintain close working relationships with local (and, as appropriate, Federal, State, Territorial, and tribal) law enforcement and first-responder organizations relevant to the company’s facilities to promote communications, with appropriate protections, and cooperation related to prevention, remediation, and response to a natural disaster or terrorist event;
 - Provide applicable information on threats, assets, and vulnerabilities to appropriate government authorities, with appropriate information protections;
 - Share threat and other appropriate information with other CI/KR owners and operators;
 - Participate in activities or initiatives developed and sponsored by relevant NIPP SCC or entity that provides the sector coordinating function;
 - Participate in, share information with (with appropriate protections), and support State and local CI/KR protection programs, including coordinating and planning with Local Emergency Planning Committees;
 - Collaborate with other CI/KR owners and operators on security issues of mutual concern; and
 - Use appropriate measures to safeguard information that could pose a threat and maintain open and effective communications regarding security measures and issues, as appropriate, with employees, suppliers, customers, government officials, and others.
- **Planning and Awareness:**
 - Develop and exercise appropriate emergency response, mitigation, and business continuity-of-operations plans;
 - Participate in Federal, State, local, or company exercises and other activities to enhance individual, organization, and sector preparedness;
 - Demonstrate continuous commitment to security and resilience across the entire company;
 - Develop an appropriate security protocol corresponding to each level of the HSAS. These plans and protocols are additive so that as the threat level increases for company facilities, the company can quickly implement its plans to enhance physical or cyber security measures in operation at those facilities and modify them as the threat level decreases;
 - Utilize National Fire Protection Association 1600 Standard on Disaster/Emergency Management and Business Continuity Programs, endorsed by DHS and Congress, when developing Emergency Response and Business Continuity-of-Operations Plans if the sector has not developed its own standard;
 - Document the key elements of security programs, actions, and periodic reviews as part of a commitment to sustain a consistent, reliable, and comprehensive program over time;
 - Enhance security awareness and capabilities through periodic training, drills, and guidance that involve all employees annually to some extent and, when appropriate, involve others such as emergency response agencies or neighboring facilities;

- Perform periodic assessments or audits to measure the effectiveness of planned physical and cyber security measures. These audits and verifications should be reported directly to the CEO or his/her designee for review and action;
- Promote emergency response training, such as the Community Emergency Response Team training offered by the U.S. Citizen Corps,³⁸ for employees;
- Consider including programs for developing highly secure and trustworthy operating systems in near-term acquisition or R&D priorities;
- Create a culture of preparedness, reaching every level of the organization’s workforce, which ingrains in each employee the importance of awareness and empowers those with responsibilities as first-line defenders within the organization and community;
- As the organization performs R&D or acquires new or upgraded systems, consider only those that are highly secure and trustworthy;
- Encourage employee participation in community preparedness efforts, such as Citizen Corps, schools, Red Cross, Second Harvest, etc.;
- Work with others locally, including government, nongovernmental organizations, and private sector entities, both within and outside its sector, to identify and resolve gaps that could occur in the context of a terrorist incident, natural disaster, or other emergency;
- Work with the DHS to improve cooperation regarding personnel screening and information protection; and
- Identify supply chain and “neighbor” issues that could cause workforce or production disruptions for the company.

³⁸ The U.S. Citizen Corps is a national organization that brings citizen groups together and focuses the efforts of individuals through education, training, and volunteer service to help make communities safer, stronger, and better prepared to address the threats of terrorism, crime, public health issues, and disasters of all kinds. It works through a national network of State, local, and tribal Citizen Corps Councils that include leaders from law enforcement, fire, emergency medical, emergency management, volunteer organizations, local elected officials, the private sector, and other community stakeholders. More information is available on the internet at www.CitizenCorps.gov.