

# Appendix 3B: Existing Protective Programs and Other In-Place Measures

This appendix provides examples of the Federal protective programs that currently support NIPP implementation. The examples provided herein generally cut across sectors and have national significance. These Federal programs augment the extensive State, local, tribal, and private sector protective programs that constitute important efforts already being implemented in support of the NIPP. The SSPs address sector-specific programs that are conducted under the leadership of the SSAs, and include selected protection programs undertaken by other security partners that apply broadly across the sector.

## 3B.1 Protective Programs and Initiatives

**Assistance Visits:** This activity refers to facility-level security assessments conducted by a federally led team and facility owners and operators that are designed to facilitate vulnerability identification and mitigation discussions between security partners and individual CI/KR owners and operators.

**Buffer Zone Protection Program:** The BZPP is a grant program designed to provide resources to State, local, and tribal law enforcement and other security professionals to enhance security of priority CI/KR facilities, thereby making it more difficult for terrorists to conduct surveillance or successfully launch an attack from the immediate vicinity of a potential target.

**Comprehensive Reviews:** DHS is leading an interagency effort to develop and conduct comprehensive reviews of select potentially high-risk CI/KR. The Comprehensive Review Program spans multiple CI/KR sectors. Working collaboratively with private sector owners and operators, State and local law enforcement and first-responders, and other security partners, a DHS-led interagency team first collects data available from multiple agencies; invites owners and operators to provide additional data; and, if required, visits specific locations to gather additional information that is needed. The team then evaluates the potential

consequences and vulnerabilities of a given asset or group of like assets from high-consequence and/or high-risk sectors within a specific geographical area, as well as the protective and response capabilities associated with the facility and the surrounding community.

Comprehensive reviews will assist State and local jurisdictions in identifying vulnerabilities and capability gaps so they may be addressed in State and local homeland security strategies and CI/KR protection programs.

As the comprehensive review process matures, DHS and the SSAs expect to learn a great deal about the development and execution of joint programs and to employ these lessons in building partnerships, thereby increasing the efficiency of Federal CI/KR protection activities and reinforcing the value of a coordinated approach. Federal agencies with sector-based security responsibilities should plan and budget for participation in the Comprehensive Review Program.

**Control Systems Security Initiative:** DHS sponsors programs to increase the security of control systems. A control system is an interconnection of components (designed to maintain operation of a process or system) connected or related in such a manner as to command, monitor, direct, or regulate itself or another system. Control systems are embedded throughout the Nation's CI/KR and may be vulnerable to increasing cyber threats that could have a devastating impact on national security, economic security, public health and safety, and the environment. The DHS Control Systems Security Initiative provides coordination among Federal, State, local, and tribal governments, as well as control system owners, operators, and vendors to improve control system security within and across all CI/KR sectors.

**Federal Cyber System Security Programs:** DHS established the GFIRST to facilitate interagency information sharing and cooperation across Federal agencies responsible for cyber system readiness and response. The members work together to understand and manage computer security incidents and to encourage proactive and preventive security practices. Other examples of Federal agency cyber security access control, certification, and policy enforcement tools include:

- The General Services Administration (GSA) is responsible for developing and implementing an infrastructure for authentication services, as well as an automated risk assessment tool for government-wide use in certifying and accrediting its eAuthentication gateway. GSA is creating a list of approved solution providers that supply smart cards based on Federal Public Key Infrastructure standards and that include a new electronic authentication policy specification.
- The National Oceanic and Atmospheric Agency has implemented enterprise-wide vulnerability assessments and virus-detection software, an intrusion-detection system, anti-virus scanning gateways, and a patch management policy.

**Federal Hazard Mitigation Programs:** FEMA administers three programs that provide funds for activities that reduce losses from future disasters or help prevent the occurrence of catastrophes. These hazard mitigation programs include the Flood Mitigation Assistance Program, the Hazard Mitigation Grant Program, and the Pre-Disaster Mitigation Program. These programs enable grant recipients to undertake activities such as the elevation of structures in floodplains, relocation of structures from floodplains, construction of structural enhancements to facilities and buildings in earthquake-prone areas (also known as retrofitting), and modifications to land-use plans to ensure that future construction ameliorates, and does not exacerbate, hazardous conditions.

**International Outreach Program:** DHS works with the Department of State and other security partners to conduct international outreach with foreign countries and international organizations to encourage the promotion and adoption of best practices, training, and other programs, as needed, to improve the protection of overseas assets and the reliability of the foreign infrastructure on which the United States depends.

**Internet Disruption Contingency Planning:** DHS formed a strategic partnership through the Internet Disruption Working Group in January 2005 to assist the NCRCG, the US-CERT, and the private sector to coordinate contingency plans for recovering Internet functions in the event of a cyber-related incident. This working group collaborates with major security partners to identify and prioritize the short-term protective measures necessary to prevent major disruptions of the Internet or reduce their consequences and to identify responsive/reconstitution measures for contingency plans in the event of a major disruption.

**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.

**National Cyber Response Coordination Group:** This entity facilitates coordination of the Federal Government's efforts to prepare for, respond to, and recover from cyber incidents and physical attacks that have significant cyber consequences (collectively known as cyber incidents). The NCRCG serves as the Federal Government's principal interagency mechanism for operational information sharing and coordination of the Federal Government's response and recovery efforts during a cyber crisis. It uses established relationships with the private sector and State and local governments to help manage a cyber crisis, develop courses of action, and devise appropriate response and recovery strategies.

**Protective Community Support Program:** Specific advisory support is provided to the protective community (e.g., law enforcement, first-responders), including training and exercise support.

**Protective Security Advisor Program:** DHS protection specialists are assigned as liaisons between DHS and the protective community at the State, local, and private sector levels in geographical areas representing major concentrations of CI/KR across the United States. The PSAs are responsible for sharing risk information and providing technical assistance to local law enforcement and CI/KR owners and operators of CI/KR within those areas.

**Software Assurance:** DHS is developing best practices and new technologies to promote integrity, security, and reliability in software development. Focused on shifting away from the current security paradigm of patch management, DHS is leading the Software Assurance Program, a comprehensive strategy that addresses processes, technology, and acquisition throughout the software life cycle to result in secure and reliable software that supports critical mission requirements.

**Training Programs:** DHS training programs are designed to provide security partners with a source from which they can obtain specialized training to enhance CI/KR protection. Subject matter, course length, and location of training can be tailored to security partner needs.

## 3B.2 Guidelines, Reports, and Planning

**Cyber Security Planning:** DHS recognizes that each sector will have a unique reliance on cyber systems and will, therefore, assist SSAs in considering a range of effective and appropriate cyber protective measures. The sector-level approaches to cyber security will be documented in the respective SSPs.

**Educational Reports:** DHS provides several types of informational reports to support efforts to protect CI/KR. They cover subjects such as CI/KR common vulnerabilities, potential indicators of terrorist activity, and best practices for protective measures. As they are developed, these reports are distributed to all State and Territorial Homeland Security Offices with the guidance that they should be shared with CI/KR owners and operators, the law enforcement community, and captains of the ports in their respective jurisdictions.

**Risk Management Manuals:** In response to the September 11, 2001, attacks, FEMA's role was expanded to include activities to reduce the vulnerability of buildings to terrorist attacks. In support of this, FEMA created the Risk Management Series, a collection of publications directed at providing design guidance to mitigate the consequences of manmade disasters.

To date, the series includes the following manuals:

- FEMA 155, Building Design for Homeland Security
- FEMA 426, Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings
- FEMA 427, Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks

- FEMA 428, Primer to Design Safe School Projects in Case of Terrorist Attacks
- FEMA 429, Insurance, Finance, and Regulation Primer for Terrorism Risk Management in Buildings
- FEMA 430, Primer for Incorporating Building Security Components in Architectural Design
- FEMA 452, Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings
- FEMA 453, Multihazard Shelter (Safe Havens) Design

### 3B.3 Information-Sharing Programs That Support CI/KR Protection

Federal agencies and the law enforcement community provide information-sharing services and programs that support CI/KR protection information sharing. These include:

- **DHS Homeland Security Information Network:** HSIN is a national, Web-based communications platform that allows DHS; SSAs; State, local, and tribal government entities; and other security partners to obtain, analyze, and share information based on a common operating picture of strategic risk and the evolving incident landscape. The network is designed to provide a robust, dynamic information-sharing capability that supports both NIPP-related steady-state CI/KR protection and NRP-related incident management activities, and to provide the information-sharing processes that form the bridge between these two homeland security missions. HSIN will be one part of the ISE called for by the Intelligence Reform and Terrorism Prevention Act of 2004; as specified in the act, it will provide users with access to terrorism information that is matched to their roles, responsibilities, and missions in a timely and responsive manner. HSIN is discussed in detail in chapter 4.
- **FBI's InfraGard:** InfraGard is an information-sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector. InfraGard is an association of businesses, academic institutions, State and local law enforcement agencies, and other participants dedicated to sharing information and intelligence related to the protection of U.S. CI/KR from both physical and cyber threats. InfraGard chapters are geographically linked with FBI Field Office territories. Each InfraGard chapter has an FBI Special Agent Coordinator who works closely with Supervisory Special Agent Program Managers in the Cyber Division at FBI Headquarters.
- **Interagency Cyber Security Efforts:** Interagency cooperation and information sharing are essential to improving national counterintelligence and law enforcement capabilities pertaining to cyber security. The intelligence and law enforcement communities have various official and unofficial information-sharing mechanisms in place. Examples include:
  - **U.S. Secret Service's Electronic Crimes Task Forces:** U.S. Secret Service's ECTFs provide interagency coordination on cyber-based attacks and intrusions. At present, 15 ECTFs are in operation, with an expansion planned.
  - **FBI's Inter-Agency Coordination Cell:** The Inter-Agency Coordination Cell is a multi-agency group focused on sharing law enforcement information on cyber-related investigations.
  - **Computer Crime and Intellectual Property Section:** DOJ, Criminal Division, Computer Crime and Intellectual Property Section is responsible for prosecuting nationally significant cases of cyber crime and intellectual property crime. In addition to its direct litigation responsibilities, the division formulates and implements criminal enforcement policy and provides advice and assistance.
  - **Cybercop Portal:** The DHS-sponsored Cybercop portal is a secure Internet-based information-sharing mechanism that connects more than 5,300 members of the law enforcement community worldwide (including bank investigators and the network security community) involved in electronic crimes investigations.

- **Law Enforcement Online:** The FBI provides LEO as national focal point for electronic communications, education, and information sharing for the law enforcement community. LEO, which can be accessed by any approved employee of a Federal, State, or local law enforcement agency, or approved member of an authorized law enforcement special interest group, is intended to provide a communications mechanism to link all levels of law enforcement throughout the United States.
- **Regional Information Sharing Systems:** The RISS Program is a federally funded program administered by DOJ, Office of Justice Programs, Bureau of Justice Assistance. RISS serves more than 7,300 member law enforcement agencies in 50 States, the District of Columbia, Guam, Puerto Rico, the U.S. Virgin Islands, Australia, Canada, and the United Kingdom. The program is comprised of six regional centers that share intelligence and coordinate efforts against criminal networks that operate in many locations across jurisdictional lines. Typical targets of RISS activities are terrorism, drug trafficking, violent crime, cyber crime, gang activity, and organized criminal activities. The majority of the member agencies are at the municipal and county levels; however, more than 485 State agencies and more than 920 Federal agencies also participate. The Drug Enforcement Administration; FBI; U.S. Attorneys' Offices; Internal Revenue Service; Secret Service; U.S. Immigration and Customs Enforcement; and the Bureau of Alcohol, Tobacco, Firearms, and Explosives are among the Federal agencies participating in the RISS Program.
- **Sharing National Security Information:** The ability to share relevant classified information poses a number of challenges, particularly when the majority of industry facilities are neither designed for nor accredited to receive, store, and dispose of these materials. Ultimately, HSIN may be used to more efficiently share appropriate classified national security information with cleared private sector owners and operators during incidents, times of heightened threat, or on an as-needed basis. While supporting technologies and policies are identified to satisfy this requirement, DHS will continue to expand its initiative to sponsor security clearances for designated private sector owners and operators, sharing classified information using currently available methods.
- **Web-Based Services for Citizens:** A variety of Web-based information services are available to enhance the general awareness and preparedness of American citizens. These include CitizenCorps.gov, FirstGov.gov, Ready.gov, and USAonwatch.org.

