Supplemental Tool: NPPD Resources to Support Vulnerability Assessments

Homeland Security

NPPD Resources to Support Vulnerability Assessments

Assessing vulnerabilities of critical infrastructure is an important step in developing security solutions and managing critical infrastructure risk. The Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD) works with owners and operators to conduct vulnerability assessments of select critical infrastructure to inform its internal risk management processes and provide technical assistance to its State, local, tribal, and territorial (SLTT) and private sector partners to enable their own risk assessments and security plans. NPPD provides additional resources, typically in the form of informational material on known vulnerabilities, to help owners and operators understand vulnerabilities at a more general level.

The Homeland Security Act of 2002 and Presidential Policy Directive 21 (PPD-21) direct the DHS Secretary to conduct comprehensive assessments of the vulnerabilities of the Nation's critical infrastructure, in coordination with the Sector-Specific Agencies (SSAs) and in collaboration with SLTT entities and critical infrastructure owners and operators. This supplement provides information on Federal resources that are used by DHS and available to SLTT governments and critical infrastructure owners and operators to identify and assess critical infrastructure vulnerabilities.

Cyber Resilience Review (CRR)

The DHS Office of Cybersecurity and Communications conducts voluntary assessments to help evaluate and enhance cybersecurity capacities and capabilities within the critical infrastructure sectors and SLTT governments through its CRR process. The goal of the CRR is to understand and measure key cybersecurity capabilities and provide meaningful maturity indicators of an organization's operational resilience and ability to manage cyber risk to its critical services during normal operations and times of operational stress and crisis. To schedule a CRR, or to request additional information, please email the Cyber Security Evaluation program at **CSE@hq.dhs.gov**.

Enhanced Critical Infrastructure Protection (ECIP) Security Surveys

ECIP Security Surveys are voluntary, non-regulatory assessments of the overall security posture of the Nation's critical infrastructure. Security Surveys collect, process, and analyze facility data to develop a detailed assessment of physical security, security management, security force, information sharing, protective measures, dependencies, and preparedness. The resulting survey information is provided to owners and operators and may be shared with SSAs and other Federal, State, local, and private sector representatives, as appropriate, through interactive "dashboards." In addition to providing a facility and sector security overview, the dashboards highlight areas of potential concern and feature options

to view the impact of potential enhancements to protective and resilience measures. The DHS Office of Infrastructure Protection (IP) conducts Security Surveys at the request of the participating facility. More information can be obtained through the local Protective Security Advisor or by emailing **IPAssessments@hq.dhs.gov.**

Site Assistance Visits (SAVs)

SAVs are voluntary vulnerability assessments that assist owners and operators of critical infrastructure to identify and document vulnerabilities, protective measures, planning needs, and options to protection from a wide range of hazards. Like the Security Survey, SAVs provide owners and operators with interactive dashboards showing a facility and sector security overview, areas of potential concern, and options to view the impact of potential enhancements to protective and resilience measures. In addition, SAVs provide narrative reports by subject matter experts, which explain options to enhance a facility's security and resilience. IP conducts SAVs at the request of a participating facility and in coordination with other Federal and SLTT government entities. More information can be obtained through the local Protective Security Advisor or by emailing **IPAssessments@hq.dhs.gov**.

The Cyber Security Evaluation Tool (CSET™)

CSET is a self-contained software tool that runs on a desktop or laptop. It evaluates the cybersecurity of an automated, industrial control or business system using a hybrid risk and standards-based approach. CSET helps asset owners assess their information and operational systems' cybersecurity practices by asking a series of detailed questions about system components and architecture, as well as operational policies and procedures. These questions are based on accepted industry cybersecurity standards. Once the self-assessment questionnaire is complete, CSET provides a prioritized list of recommendations for increasing cybersecurity. You can access the CSET tool through the United States Computer Emergency Readiness Team's Website at **www.us-cert.gov/control_systems**.

Chemical Security Assessment Tool (CSAT) Security Vulnerability Assessment (SVA)

This tool is available only to chemical facilities that are subject to the Chemical Facility Anti-Terrorism Standards (CFATS) regulations. The CSAT SVA application:

- Collects basic facility identification information and information about the chemicals that a facility possesses.
- Collects information about assets at the facility that involve the chemicals of interest identified by DHS in Appendix A of the CFATS Authorization.

- Enables users to locate assets on an interactive map and apply DHS attack scenarios or define attack scenarios of their own to run against the facility's assets. This provides DHS with data on the vulnerability and potential consequences of such attacks. Users will assess the vulnerability of their facilities based on the security measures already in place at the facility.
- Collects information on relevant cyber systems that may affect the security of identified assets.

For additional information, the CSAT Help Desk has a toll-free number for questions regarding the CSAT SVA application: 866–323–2957, between 7:00 a.m. and 7:00 p.m. (Eastern Time), Monday through Friday. The CSAT Help Desk is closed on Federal holidays.

More details on CFATS, Chemical-Terrorism Vulnerability Information, and other related information is available on the DHS Website at **http://www.dhs.gov/chemicalsecurity**.

Infrastructure Protection Report Series

These reports identify common vulnerabilities by asset class within the sectors, as well as the types of terrorist activities that are likely to be successful in exploiting these vulnerabilities. They also identify security and preparedness best practices by asset class within the sectors. Brief integrated papers are currently available to Federal, SLTT, and private sector partners on the Homeland Security Information Network.

Homeland
Security