

Planning and Coordination

The Government Facilities SSP details the means by which the NIPP risk management framework is implemented in the sector. It provides guidance to sector security partners to enhance the steady state of preparedness across all government facilities. It is specifically tailored to:

- address unique characteristics and risk landscapes of the sector;
- define sector security partners, and their roles, responsibilities and authorities;
- establish (or document existing) procedures for sector interaction, information sharing, coordination and partnership;
- describe the sector-specific mechanisms used to identify assets, understand threats, assess vulnerabilities and consequences and prioritize investments based on costs and benefits so that they are applied where they offer the greatest mitigation of risk; and
- provide consistency for protective programs and investments across the sector.

FPS coordinates activities for the Government Facilities Sector in conjunction with its Government Coordinating Council. FPS represents the sector as a member of the NIPP Federal Senior Leadership Council and through coordination with other sectors.



Contact Information

Government Facilities Sector
Federal Protective Service
nipp_gfs@dhs.gov

For questions or more information regarding NIPP,
please contact NIPP@dhs.gov or visit www.dhs.gov/nipp

For more information regarding FPS or ICE,
please visit: www.ice.gov

Enhancing the Protection of Critical Government Facilities

Government Facilities Sector
National Infrastructure Protection Plan



U.S. Immigration
and Customs
Enforcement

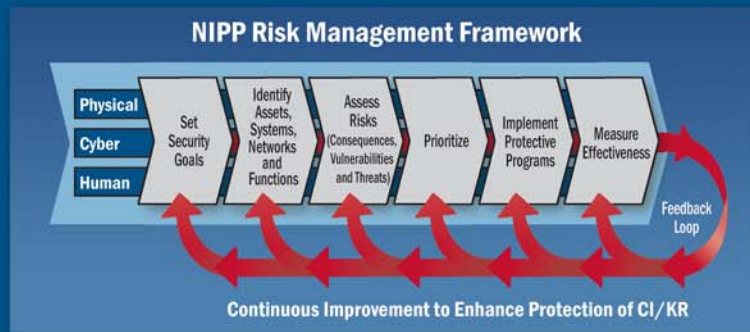
Report Suspicious Activity:
1-866-DHS-2-ICE
1-866-DHS-2423
www.ice.gov



U.S. Immigration
and Customs
Enforcement

Building a Safer, More Secure and More Resilient America

The National Infrastructure Protection Plan (NIPP) sets forth a comprehensive risk management framework and clearly defines critical infrastructure protection roles and responsibilities. The NIPP provides the coordinated approach that will be used to establish national priorities, goals and requirements for infrastructure protection so that funding and resources are applied in the most effective manner.



Homeland Security Presidential Directive-7 (HSPD-7) identified 17 critical infrastructures and key resources (CI/KR) sectors and designated federal government Sector-Specific Agencies (SSAs) for each of the sectors. SSAs are responsible for working with the Department of Homeland Security (DHS) to implement the NIPP sector partnership model and risk management framework, develop protective programs and related requirements and provide sector-level CI/KR protection guidance in line with the overarching guidance established by DHS pursuant to HSPD-7.

Working in collaboration with security partners, they are also responsible for developing and submitting a Sector-Specific Plan (SSP) and sector-level performance feedback to DHS to enable national cross-sector CI/KR protection program gap assessments.

The Federal Protective Service (FPS), a division of U.S. Immigration and Customs Enforcement (ICE), is designated in the NIPP as the SSA for the Government Facilities Sector. Building on its traditional role to provide

protection of General Services Administration (GSA) federally owned and federally operated facilities, this new responsibility requires that FPS coordinate the effort to identify, assess and enhance the protection of government facilities that are determined to be nationally critical.

Government Facilities Sector

The Government Facilities Sector includes a wide variety of buildings, owned or leased by federal, state, local or tribal



governments, located domestically and overseas. The sector's portfolio includes general use office buildings and special use military installations, embassies, courthouses, national laboratories, structures that may house critical equipment and systems, networks and functions and associated land. Many government facilities are open to the public for business activities, commercial transactions or recreational activities. Other buildings not open to the public may contain highly sensitive information, materials, processes and equipment.

The sector also includes the cyber elements that contribute to the protection of sector assets (e.g., access control systems and closed circuit television systems) and protection of individuals who possess tactical, operational or strategic knowledge or perform essential functions.

Many government facilities support essential government functions and services. Ensuring the continuity of these functions and services through protection of the associated assets is an important responsibility for this sector.

Situational Awareness and Readiness

Enhancing the protection of government facilities requires a strong partnership among all levels of government. The geographic scope of this effort is immense and depends on routine collaboration to share time- and security-sensitive information. The ability to increase situational awareness and readiness through real-time information exchange is essential for the protection of government facilities.



The Government Facilities Sector uses a secure Web-based portal, FPS Link, to collaborate and share information with sector security partners.

- FPS receives information from federal, state and local governments and continuously monitors open sources of information.
- This information is analyzed for relevance to government facility protection and shared with sector security partners based on the information's time and security sensitivity.
- Tactical information is relayed immediately to government facility owners and operators, law enforcement and emergency operations centers through alerts, secure messaging and a live synchronized chat, enabling quick and coordinated actions.
- Operational and strategic information is shared through compartmentalized collaboration tools including forum discussions, online briefings and surveys, a document library and a community calendar.