National Monuments & Icons

Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan

May 2007

Homeland Security

Department of the Interior

National Monuments and Icons Sector Government Coordinating Council Letter of Agreement and Support

The National Infrastructure Protection Plan (NIPP) provides the unifying structure for the integration of critical infrastructure and key resources (CI/KR) protection efforts as part of a coordinated national program. The NIPP provides the overarching framework for integrating protective programs and activities that are underway in the various sectors, as well as new and developing CI/KR protection efforts. The NIPP includes 17 sector-specific plans (SSPs) that detail the application of the overall risk management framework for each specific sector.

The National Monuments and Icons (NMI) SSP describes a collaborative effort among the various Federal government agencies that have equities within the NMI Sector and will result in the prioritization of protection initiatives and recommended investments within the NMI Sector as a whole. This plan will not, however, interfere with the internal budget deliberations by the various Federal agencies, nor will it overrule internal, agency specific decisions on priorities of protection initiatives and recommended investments. This prioritization ensures that resources are applied where they contribute the most to risk mitigation by lessening vulnerabilities, deterring threats, and minimizing the consequences of terrorist attacks and other natural and manmade hazards. As the sector matures and more assets are added, this collaborative effort will expand to include the private sector; state, territorial, local and tribal governments; and nongovernmental organizations.

By signing this letter of agreement and support, the departments and agencies that constitute the NMI Government Coordinating Council (GCC) commit to:

- Support the NMI SSP concepts and processes, and carry out their assigned functional responsibilities regarding the protection of the NMI CI/KR as described herein;
- Work with the Department of the Interior (DOI), the NMI Sector Specific Agency (SSA), and the Secretary of Homeland Security, as appropriate and consistent with their own agency-specific authorities, resources, and programs, to coordinate funding and implementation of programs that enhance NMI CI/KR protection;

- Cooperate and coordinate with DOI and the Secretary of Homeland Security, in accordance with guidance provided in Homeland Security Presidential Directive (HSPD) -7, as appropriate and consistent with their own agency-specific authorities, resources, and programs, to facilitate NMI CI/KR protection;
- Develop or modify existing interagency and agency-specific CI/KR plans, as appropriate, to facilitate compliance with the NMI SSP;
- Develop and maintain partnerships for CI/KR protection with appropriate state regional, local, tribal, and international entities; the private sector; and nongovernmental organizations (NGO); and
- Protect critical infrastructure information according to the Protected Critical Infrastructure Information (PCII) program or other appropriate guidelines, and share CI/KR protection-related information, as appropriate and consistent with their own agency-specific authorities and the process described herein.

Salvatore R. Lauro, Chairperson
Assistant Director
Office of Law Enforcement, Security, and Emergency Management
U.S. Department of the Interior

Table of Contents

List of Figures

List of Tables

Executive Summary

The National Monuments and Icons (NMI) Sector-Specific Plan (SSP) was created to complement the National Infrastructure Protection Plan (NIPP) in improving protection of the NMI Sector in an all-hazard environment. The NMI SSP is designed to establish a collaborative partnership at all levels of government and the private sector to foster the cooperation necessary to improve the protection of NMI critical infrastructure and key resources (CI/KR). The NMI SSP is a pathway to identify and prioritize assets, assess risk, implement protective programs, and measure the effectiveness of protective programs. This document represents the collaborative efforts of partners from the private sector and government, all dedicated to the protection of CI/KR within the NMI Sector.

1. Sector Profile and Goals

The NMI Sector encompasses a diverse array of assets, systems, networks, and functions located throughout the United States and its Territories. Many of these NMI assets are listed in either the National Register of Historic Places or the List of National Historic Landmarks.

NMI Sector assets that are categorized as "National Critical":

- Are monuments, physical structures, or objects; and
- Are recognized both nationally and internationally as representing the Nation's heritage, traditions, and/or values or are recognized for their national, cultural, religious, historical, or political significance; and
- Serve the primary purpose of memorializing or representing significant aspects of our Nation's heritage, traditions, or values and to serve as points of interest for visitors and educational activities. They generally do not have a purpose or function that fits under the responsibility of another sector.

NMI Sector assets that do not meet these criteria are categorized as "National Significant," "Regional Critical," or "Local Significant."

NMI Sector assets are essentially physical structures and include the operational staff and visitors who may be impacted by a terrorist attack or all-hazard incident. Sector assets do not include famous people or technology applications, and there are minimal cyber and telecommunications issues associated with this sector due to the nature of the assets.

The NMI Sector is committed to ensuring that the symbols of our Nation remain protected and intact for future generations. In the course of protecting U.S. landmarks, the sector will ensure that staff and visitors are protected from harm. Because access to monuments and icons is a hallmark of life in a free and open society, the sector will strive for an appropriate balance between

security, public access, and aesthetics. The sector will take protective measures to prevent adversaries from affecting the national psyche by damaging or destroying these important symbols.

The NMI SSP represents the goals established by the NMI Sector to facilitate the incorporation of protective measures to improve awareness, protection, response, and recovery. The sector goals are driven by a desire to reduce risk to critical assets within the NMI Sector and to promote the continued use and enjoyment of these infrastructures.

The goals of the NMI Sector are as follows:

Goal 1: Establish clear criteria to define assets as National Critical versus National Significant, Regional Critical, or Local Significant.

Goal 2: Clearly delineate and define roles and responsibilities for all the sector's security partners.

Goal 3: Perform risk assessments on National Critical assets.

Goal 4: Develop rapid and robust communications between intelligence and law enforcement agencies and Federal, State, local, tribal, and private security partners.

Goal 5: Ensure seamless coordination among Federal, State, and local agencies as well as any private sector entities that own or operate sector assets.

Goal 6: Maintain cross-sector coordination with regard to NMI assets whose primary protective responsibility resides in another sector.

Goal 7: Integrate robust security technology and practices while preserving the appearance and accessibility of NMI sites.

Goal 8: Develop flexible security programs to adjust to seasonal and event-specific security challenges.

Goal 9: Protect against insider threats.

Goal 10: Develop contingency response programs.

2. Identify Assets, Systems, Networks, and Functions

The identification of assets, systems, networks, and functions is necessary to define the NMI Sector and to develop an inventory of CI/KR that can be further analyzed with respect to vulnerabilities and the protective actions required to achieve the goals set forth in section 1.

The process for identifying sector assets, systems, networks, and functions will be a collaborative effort between the U.S. Department of the Interior (DOI), the U.S. Department of Homeland Security (DHS), and other supporting and lead Sector-Specific Agencies (SSAs). DOI will work closely with DHS in establishing relationships with the private sector to ensure maximum information exchange within and outside the Federal Government.

A number of NMI assets, systems, networks, and functions are listed on the National Register of Historic Places or the List of National Historic Landmarks. These listings have been used as a starting point to determine National Critical NMI assets. Through DHS and State offices of homeland security, DOI will work at the Federal, State, local, and tribal government levels and with the private sector to identify other NMI assets that may be included within the sector.

3. Assess Risk

The NIPP affirms that risk assessments are essential to the appropriate distribution of the limited funds allocated for infrastructure protection. There is no overarching regulatory authority within the NMI Sector that mandates risk assessments. However, most National Critical assets are owned by government agencies and are covered by internal requirements mandating risk assessments.

The initial step in the risk assessment process is the characterization of the sector assets and consists of the following two elements:

- A ranking system based on the uniqueness of the asset and its significance as a national symbol; and
- Consequence categories encompassing DHS SSP guidance.

This step is independent of the threat scenario and is a measure of the impact to the national morale and public confidence caused by damage or destruction of a significant monument or icon. The ranking system will determine if a monument or icon is a National Critical NMI asset or the responsibility of a lower authority. The monument or icon will be ranked as National Critical, National Significant, Regional Critical, or Local Significant. The National Significant, Regional Critical, and Local Significant categories are added for application of the methodology by other Federal Government, State, regional, and local authorities.

The remaining steps in the process utilize the DHS SSP guidance regarding criteria for consequence, vulnerability, and risk and result in a numerical ranking based on a postulated, worst-case scenario.

The risk calculations will be used to prioritize the National Critical NMI assets to facilitate implementing appropriate protective measures and program requirements. DOI will conduct risk calculations for its own facilities and encourage other asset owners to implement the methodology presented herein or a similar methodology. The results can be normalized with other DHS methodologies for those NMI assets not owned or operated by DOI. Furthermore, DOI will make the methodology available to other sector stakeholders, with the expectation that stakeholders and State and local authorities will follow the same methodology guidance with support from sector resources as needed.

4. Prioritize Infrastructure

Prioritization for CI/KR is used to focus planning, foster coordination, and support effective resource allocation and incident management. The NMI Sector's CI/KR will be prioritized to ensure that resources are applied where they contribute most to the mitigation of identified risks.

Assets designated as National Critical will be subjected to the NMI risk assessment methodology to develop a numerical score based on the vulnerabilities associated with each asset. DOI will conduct the assessment for those assets it owns and will work with the owners of other assets to ensure that the assessment is conducted.

5. Develop and Implement Protective Programs

Protective programs involve measures designed to prevent, detect, deter, and mitigate the threat; reduce vulnerability to a terrorist attack or all-hazards incident; minimize consequences; and enable timely, efficient response and restoration in a post-event situation, whether a terrorist attack, natural disaster, or other incident.

DOI, key stakeholders, and asset-specific law enforcement have developed and implemented protective programs on an accelerated basis since the terrorist attacks against the United States on September 11, 2001. A mix of new regulations, congressional mandates, actual and perceived threat information, and vulnerabilities is driving these programs.

DOI will use a methodical, disciplined approach to match limited resources with National Critical NMI assets and to share validated protective measures currently in use throughout DOI with other stakeholders. Since National Critical NMI assets cut

across different Federal agencies the participation of all entities is paramount to ensuring the highest level of protection for the Nation's NMI assets.

Because other NMI assets are not owned by the Federal Government, and there is no regulatory authority to require compliance with protective program measures, DOI will work with DHS and other agencies to promote cooperation and involvement of stakeholders in implementation of this plan. The SSA's role under this initiative is to share information with stakeholders and encourage involvement.

6. Measure Progress

A partnership at all levels of government collaborated to create a comprehensive set of goals to enhance the protection of CI/KR within the NMI Sector. A set of objectives and initial metrics was also developed to measure the progress of the protection efforts. By measuring the effectiveness of the protective programs and actions, the sector can continually improve CI/KR mitigation actions at the sector level and improve the overall performance at the national level.

7. CI/KR Protection R&D

Research and development (R&D) is one of the key tools the sector uses to improve knowledge pertaining to threats, vulnerabilities, consequences, and subsequent risks associated with sector assets when subject to terrorist attacks or all-hazards incidents.

The DOI NMI Sector liaison will confer with the DHS Science and Technology Directorate (S&T) and the Executive Office of the President's Office of Science and Technology Policy (OSTP) on a periodic basis to identify current R&D initiatives that have applicability to the sector. DOI will share this information with sector stakeholders through the NMI Government Coordinating Council to gather input relative to those initiatives of most value to the sector.

8. Manage and Coordinate SSA Responsibilities

Because of staffing and funding limitations, DOI has been unable to create a separate program office to manage NIPP-related responsibilities as the SSA for the NMI Sector.

The DOI SSA responsibility will be delegated to a Special Agent assigned in the Security Division of the Office of Law Enforcement, Security, and Emergency Management. When necessary the Special Agent will be assisted by the Assistant Director of the Security Division.

The SSA will capitalize on the cooperation and coordination that already exists among sector partners to accomplish the numerous tasks assigned to the SSA and ensure that the sector meets its goals and objectives.

Introduction

Protecting the critical infrastructure and key resources (CI/KR) of the United States is essential to the Nation's security, economic vitality, and way of life. CI/KR include the assets, systems, networks, and functions that provide vital services to the Nation. Terrorist attacks on CI/KR and other natural and man-made hazards could significantly disrupt the functioning of government and business alike and produce cascading effects far beyond the affected CI/KR sector and physical location of the incident. Direct attacks could result in large-scale human casualties, property destruction, and economic damage, and also profoundly damage national prestige, morale, and confidence. Terrorist attacks that use components of the Nation's CI/KR as weapons of mass destruction[1] could have even more devastating physical, psychological, and economic consequences.

The protection of CI/KR is, therefore, an essential component of the homeland security mission to make America safer, more secure, and more resilient from terrorist attacks and all-hazards incidents. Protection includes actions to guard or shield CI/KR assets, systems, networks, or their interconnecting links from exposure, injury, destruction, incapacitation, or exploitation. In the context of the National Infrastructure Protection Plan (NIPP), this includes actions to deter, mitigate, or neutralize the threat, vulnerability, or consequences associated with a terrorist attack or all-hazards incident. Protection can include a wide range of activities, including hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, promoting personal surety programs, and implementing cyber security measures. The NIPP provides the framework for the unprecedented cooperation that is needed to develop, implement, and maintain a coordinated national effort that brings together government at all levels, the private sector, and international organizations and allies.

The NIPP and its complementary Sector-Specific Plans (SSPs) provide a consistent, unifying structure for integrating both existing and future CI/KR protection efforts. It also provides the core processes and mechanisms to enable government and private sector security partners to work together to implement CI/KR protection initiatives. Homeland Security Presidential Directive 7 (HSPD-7) outlines 17 CI/KR sectors in recognition that each sector possesses unique characteristics and operating methods. The U.S. Department of the Interior (DOI) has been designated as the Sector-Specific Agency (SSA) for the National Monuments and Icons (NMI) Sector and is responsible for developing the SSP for this sector.

The purpose of the SSPs is to detail the application of the NIPP risk management framework to each of these 17 CI/KR sectors. The SSPs are developed by the designated Federal SSAs in coordination with relevant sector security partners. The SSP for each sector should align with the processes established in the NIPP, most notably the risk management framework. Each SSP should support the planning assumptions outlined in the NIPP, as well as sector-specific planning assumptions that are relevant to protection of that sector's CI/KR. This document presents the SSP for the NMI Sector.

[1] (1) Any explosive, incendiary, or poison gas (i) bomb, (ii) grenade, (iii) rocket having a propellant charge of more than 4 ounces, (iv) missile having an explosive or incendiary charge of more than one-quarter ounce, or (v) mine or (vi) similar device; (2) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors; (3) any weapon involving a disease organism; or (4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life (18 U.S.C. 2332a).

The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, published in February 2003, defined the NMI Sector as the "diverse array of national monuments, symbols, and icons that represent our Nation's heritage, traditions and values, and political power. They include a wide variety of sites and structures such as prominent historical attractions, monuments, cultural icons, and centers of government and commerce." In addition, the U.S. Department of Homeland Security's (DHS) *Guidance for Developing Sector-Specific Plans* states that "icons can be considered to include any structure, system, or resource that has cultural, historic, psychological, or political significance at the local, regional or national level if compromised or destroyed." Terrorists perceive NMI assets as internationally recognized symbols of American power, culture, and democratic tradition. Terrorist targets most frequently represent a confluence of these factors and the pragmatic concerns of loss of life, continuous live media coverage, strategic economic impact, and potential for infrastructure interdependency.

Many of the assets included in this sector are monuments and icons ranked as National Critical, such as those located in the Nation's capital as well as others such as the Statue of Liberty, Independence Hall, the Liberty Bell, and Mount Rushmore National Monument owned by DOI. This sector also encompasses buildings, institutions, and landmark architectural structures that are not owned or operated by DOI.

The NMI Sector also includes monuments and symbols ranked as National Significant, Regional Critical, and Local Significant. However, the responsibility for protecting those assets lies primarily with the owner. DOI as the SSA intends to work with DHS to establish appropriate mechanisms to enhance outreach and improve information sharing regarding threats, best practices, and protective measures with all stakeholders of sector assets, including those at the State, regional, and local levels.

Assets with iconic value that best fit in one of the other sectors, such as Dams, Commercial Facilities, and Government Facilities, will not be assessed within the NMI SSP. However, DOI will support other SSAs to ensure appropriate risk ranking and implementation of protective programs for those assets.

To protect assets across all sectors, the NIPP risk management framework includes the following activities:

- **Set Security Goals:** Define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective protective posture.
- **Identify Infrastructures:** Develop an inventory of assets, systems, and networks that make up the Nation's CI/KR and the critical functionality they provide, including infrastructure located outside the United States, and collect information pertinent to risk management.
- **Assess Risks:** Determine risk by combining potential direct and indirect consequences of a terrorist attack or all-hazards incident (including dependencies and interdependencies associated with each identified asset, system, or network), known vulnerabilities to various potential attack vectors, and general or specific threat information.
- **Prioritize:** Aggregate and analyze assessment results to determine asset, system, and network criticality, and present a comprehensive picture of national CI/KR risk to establish priorities and provide the basis for planning and allocating resources.
- **Implement Protective Programs:** Select appropriate protective actions or programs to reduce the risks identified and secure the resources needed to address priorities.
- **Measure Effectiveness:** Use metrics and other evaluation procedures at the national and sector levels to measure progress and assess the effectiveness of the national CI/KR protection program.

Enhancing critical infrastructure for the NMI Sector will require the following:

- Identification of National Critical NMI assets through collaboration with sector stakeholders;
- Assessment of the vulnerabilities and interdependencies of NMI assets and analysis of potential risks based on their associated threats and consequences;

- Prioritization of the NMI assets based on overall risk ranking;
- Development of sustainable protective programs and new protection technologies for prioritized implementation that also can be shared with and implemented by State, regional, and local stakeholders; and
- Evaluation of the effectiveness of the protective programs, as well as overall SSP implementation, using predefined performance metrics.

The NMI SSP will provide the impetus for collaboration with stakeholders who share responsibility for protecting the Nation's NMI assets, including State and local governments and the private sector.

A number of key limitations affect the environment in which DOI operates as it develops programs to protect NMI assets:

- First, except for monuments and icon sites managed by the National Park Service (NPS), DOI has no existing or historical regulatory or oversight relationships with any entities within the sector. The NPS maintains the National Register of Historic Places and the List of National Historic Landmarks, but this does not imply ownership by DOI.
- Second, changes designed to enhance security may face severe limitations because of the historic nature of many assets and their surrounding areas. An example is the icons on the National Mall in Washington, DC. The NPS must submit proposed security enhancements to the National Capitol Planning Commission and the Fine Arts Commission for review and approval. Although this is a critical process that maintains the visual and historical integrity of the assets and surrounding areas, the review frequently results in disapproval or modification of the proposed security enhancements.
- Finally, by their very nature, most assets within this sector are designed and managed as open sites that welcome visitors from this country and from around the world. These sites are intended to be visited and enjoyed, to provide areas for learning and contemplation, and to connect current and future generations to historical events and locations in the Nation's past. Maintaining the open design of these sites while addressing the current need to improve security leads to conflicting considerations, both internally and externally, concerning the level and type of security measures to be used at each site.

1. Sector Profile and Goals

1.1 Sector Profile

Overall, the NMI Sector encompasses a diverse array of assets located throughout the United States and its Territories. Many of these NMI assets are listed on either the National Register of Historic Places or the List of National Historic Landmarks.

NMI Sector assets that are categorized as "National Critical":

- Are monuments, physical structures, or objects; and
- Are recognized both nationally and internationally as representing the Nation's heritage, traditions, and/or values or are recognized for their national, cultural, religious, historical, or political significance; and
- Serve the primary purpose of memorializing or representing significant aspects of our Nation's heritage, traditions, or values and to serve as points of interest for visitors and educational activities. They generally do not have a purpose or function that fits under the responsibility of another sector.

Some physical structures that could be considered as monuments or icons (e.g., Golden Gate Bridge, Sears Tower, Hoover Dam, and the U.S. Capitol) have been determined to be more appropriately assigned to other sectors, such as Transportation Services, Commercial Facilities, Dams, or Government Facilities, based on their primary purposes. This sector assignment is intended to ensure a better level of security based on application of more appropriate protective measures and programs. DOI, as the SSA, will confer with other SSAs and Government Coordinating Councils (GCCs) during the asset identification process to ensure that assets are assigned to the appropriate authority.

NMI assets are primarily physical structures. Included as part of each asset are the operational staff and visitors that may be impacted by a terrorist attack or all-hazards incident. Sector assets do not include famous people or technology applications, although they may contain holdings of significant importance to the Nation's history. There are minimal cyber and telecommunications issues associated with this sector due to the nature of the assets. Some information technology (IT) or telecommunications systems may be used at a few of the assets, and these will be considered during the process of conducting the vulnerability assessment and implementing protective programs as appropriate. The section on protective programs addresses in detail the three key areas of security programs: physical, personnel, and cyber/information.

The Bureau Chief Information Officer (CIO) is responsible for providing security for the cyber-based information systems located at DOI-owned NMI assets; however, that responsibility may be delegated to the system owner. In conjunction with the system security manager, the system owner is responsible for the overall security of the IT system including certification and accreditation, categorization of systems as general support systems or major applications, and preparation of system security plans. DOI policy applies to all IT systems that process Sensitive But Unclassified (SBU) data (all unclassified DOI systems are considered SBU).

Certain national holidays, such as the Fourth of July, Memorial Day, and Labor Day, represent an especially important factor for this sector, when visitation at selected NMI assets is particularly high. Special date events will be discussed with respect to the development of protective programs in section 5.

Although a diverse array of NMI assets are scattered across the United States and its Territories, this SSP focuses primarily on identifying, prioritizing, assessing, and protecting National Critical NMIs that may be attractive targets for terrorists. The process for narrowing the NMI asset list to those of national criticality and for which DOI will retain SSA authority will be further discussed in section 2.

1.2 Security Partners

Recognizing that each infrastructure sector possesses its own unique characteristics and operating models, HSPD-7 has designated SSAs in each critical infrastructure sector that have primary responsibility for leading protective program efforts for the assets in that sector. In accordance with the guidance provided by HSPD-7, as the SSA for NMI assets, DOI will do the following:

- Work with the owners of National Critical NMI assets to identify, prioritize, and coordinate protecting them to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them;
- Collaborate with relevant Federal departments and agencies;
- Conduct vulnerability assessments of DOI-owned assets and facilitate or support similar assessments of non-DOI-owned assets; and
- Encourage adoption of risk management strategies to protect against and mitigate the effects of attacks against CI/KR.

1.2.1 Sector-Specific Agency

Department of the Interior. DOI was created by an act of Congress in 1849 to manage public lands. DOI has long been involved in the protection of NMI assets, such as the Washington Monument and the Statue of Liberty. DOI manages the third largest Federal law enforcement force, with approximately 4,400 commissioned law enforcement personnel spread among the Bureau of Indian Affairs, Bureau of Land Management, Bureau of Reclamation (BOR), Fish and Wildlife Service, and the NPS. In addition, approximately 1,300 tribal and contract law enforcement personnel serve on Indian country lands. DOI is responsible for the safety and security of 70,000 employees and 200,000 volunteers, 1.3 million daily visitors, and more than 507 million acres of public lands that include historic or nationally significant sites as well as dams and reservoirs. Over the last several years, BOR has completed security vulnerability assessments (VAs) of its dams, power plants, and canals in the 17 Western States. In addition, DOI assists in providing security for oil and gas production and transmission facilities on Federal and Indian trust lands, including 4,000 offshore oil and gas production facilities, 22,000 miles of active pipeline, and 35,000 petroleum workers in the Gulf of Mexico.

All DOI cyber systems fall under the responsibility of the CIO, who monitors the performance of IT programs and activities including cyber security. The CIO consults with the Department's Chief Financial Officer to ensure that IT programs and activities at DOI are carried out in a cost-effective manner and that financial and related program information is reliable, consistent, and timely. The CIO confers with top-level officials in the Office of Management and Budget and other Federal agencies, providing testimony before congressional committees as necessary.

All cyber systems within DOI are required to comply with regulations outlined in the Federal Information Security Management Act (FISMA) and must be certified and accredited. Each must follow the standardized approach of DOI's certification and accreditation (C&A) process that is based on the National Institute of Standards and Technology's (NIST) Special

Publication 800 series. Additional requirements of the C&A process involve methods to identify and prioritize cyber systems, discover and remediate vulnerabilities, and test protective measures.

DOI is an active partner in multiagency task forces that facilitate the sharing of information, developing security protocols, and identifying protective measures designed to prevent and respond to real and potential terrorist attacks. In the wake of 9/11, DOI's efforts were intensified to match the increased threat environment.

1.2.2 Federal Departments and Agencies

Smithsonian Institution (SI). In 1826, James Smithson, a British scientist, drew up his last will and testament, naming his nephew as beneficiary. Smithson stipulated that if his nephew should die without heirs (as he would in 1835), the estate should go "to the United States of America, to found at Washington, under the name of the Smithsonian Institution, an establishment for the increase and diffusion of knowledge among men."

Smithson died in 1829, and 6 years later, President Andrew Jackson announced the bequest to the U.S. Congress. On July 1, 1836, Congress accepted the legacy bequeathed to the Nation and pledged the faith of the United States to the charitable trust. An act of Congress signed by President James K. Polk on August 10, 1846, established the Smithsonian Institution as a trust to be administered by a board of regents and a secretary of the Smithsonian.

The Smithsonian Institution's Office of Protection Services (OPS) provides security services and operates programs for security management and criminal investigations at the Smithsonian Institution (SI) facilities on and near the National Mall in Washington, DC, in New York City, and in Panama. OPS provides technical assistance and advisory services to SI bureaus, offices, and facilities. It serves SI employees and volunteers, and more than 25 million visitors each year. The United States Code (40 U.S.C. 6301-6307) provided OPS the authority to police the buildings and grounds of the Smithsonian Institution.

National Archives and Records Administration (NARA). The mission of NARA is to take cost-effective steps to protect the holdings of our archival and records center in an appropriate space, ensure protection and preservation of records, and expand storage capacities to meet growing demands. NARA's authority is codified principally under 44 U.S.C. Chapters 21-33.

NARA also ensures that the President, Congress, the courts, public servants, and citizens continue to have access to the essential evidence that documents the rights of American citizens and the actions of Federal officials, promotes civic education, and facilitates a historical understanding of our national experience. NARA sets the minimum structural, environmental, property, and life-safety standards that a records storage facility must meet in order to be used to safeguard and preserve the records of our government and ensure that the people can discover, use, and learn from this documentary heritage.

Federal Bureau of Investigation (FBI). The FBI is the investigative arm of the U.S. Department of Justice. The FBI's investigative authority is explained in 28 U.S.C. 533. The USA PATRIOT Act signed October 26, 2001, granted the FBI new provisions to address the threat of terrorism. The FBI is the lead Federal agency in combating terrorism and investigating acts of terrorism.

U.S. Secret Service (USSS). When an event is designated as a National Special Security Event (NSSE), the USSS assumes its mandated role as the lead agency for the design and implementation of the operational security plan. An NSSE venue may be located at an NMI asset. The USSS has significant responsibility for White House security in coordination with the Executive Office of the President.

Department of Homeland Security (DHS). As set forth in HSPD-7, DHS is responsible for coordinating the overall national effort to enhance protection of the CI/KR of the United States. DHS also is responsible for establishing uniform policies, approaches, guidelines, and methodologies for integrating Federal infrastructure protection and risk management activities within and across sectors along with metrics and criteria for related programs and activities. DHS has overseen the development of the NIPP and will be responsible for approving SSP approaches and methodologies. During implementation, DHS will lead, integrate, and coordinate the efforts among Federal departments and agencies, State and local governments, and the private sector.

Specifically within DHS, the Office of Infrastructure Protection will provide oversight of the NMI SSP and the Science and Technology Directorate (S&T) will provide support. DHS will assist DOI in establishing relationships with the private sector to ensure maximum information exchange within and outside the Federal Government.

The mutual collaboration and agreement between DOI and DHS is critical regarding overlaps and interdependencies where the type and character of the NMI asset falls primarily into a CI/KR sector for which DHS is the SSA. DOI will confer with DHS and the other SSAs to clearly identify these overlaps and interdependencies and will reach consensus on responsibilities for these NMI assets within the respective sectors. For example, there will be overlaps between DOI's NMI and DHS's CI/KR sectors with respect to the following:

- DHS's Transportation Systems Sector, with respect to bridges, locks, dams, and canals (e.g., Golden Gate Bridge);
- DHS's Dams key resource category (e.g., Hoover Dam);
- DHS's Government Facilities key resource category (e.g., U.S. Capitol); and
- DHS's Commercial Facilities key resource category (e.g., Empire State Building).

DOI will confer with DHS to clearly delineate lead and support roles and responsibilities. In its support role, DOI will assist DHS with respect to the overall protection of these assets.

Department of Defense (DOD). DOD is responsible for defending the Nation. DOD owns buildings, structures, and systems that could be categorized as NMI assets (e.g., the Pentagon). The U.S. Army Corps of Engineers (USACE) is responsible for maintaining the Nation's commercial waterways and operates the dams and locks on our Nation's inland waterways. These examples would fall within the Government Facilities and Dams sectors, respectively, and DHS would be the lead SSA. As previously stated, DOI will work with DHS and DOD to delineate lead and support roles and responsibilities.

Office of Science and Technology Policy (OSTP). The OSTP has a broad mandate to advise the President and others within the Executive Office of the President on the effects of science and technology on domestic and international affairs. The office also is authorized to lead an interagency effort to develop and implement sound science and technology policies and budgets and to work with the private sector, State and local governments, the science and higher education communities, and other nations toward this end.

The OSTP will support DOI in developing the NMI SSP and will be included as appropriate in policy development, protective program plans and related technology development, operational discussions, and coordination meetings. DOI, as the SSA, will coordinate with the OSTP Assistant Director for Homeland Security to take advantage of available support resources.

Other Federal Agencies. Although not listed in the DHS guidance document, other Federal agencies own or are responsible for buildings, structures, and systems that could be categorized as NMI assets. The assets under the responsibility of these Federal agencies would be included as CI/KR under Government Facilities or Transportation Systems, and DHS would be the lead SSA. DOI, as the SSA, will work with DHS and other Federal agencies to clearly delineate lead and support roles and responsibilities.

1.2.3 State, Local, and Tribal Governments

State Offices of Homeland Security. States have designated homeland security advisors that work with DHS in coordinated and integrated law enforcement, domestic security, emergency response and recovery, policy development, and implementation of programs to better align resources to protect public and private ventures and secure the homeland. DOI intends to work with these advisors through DHS to develop a list of assets that may be categorized within this sector.

In addition, DHS has begun staffing new positions, known as Protective Security Advisors (PSAs), to support CI/KR stakeholders. These PSAs are highly experienced security specialists who are being placed in neighborhoods throughout the country to assist local efforts in protecting critical assets and to provide a local perspective that will contribute to the national threat picture.

State and Local Law Enforcement. State police agencies are responsible for public safety and domestic security, providing law enforcement and investigative services in cooperation with county and municipal agencies. These State-level agencies link the Federal Government and local agencies by providing statewide jurisdictional administration for law enforcement, domestic security, and antiterrorism issues. State police agencies provide assistance and cross-jurisdictional management of incidents that affect multiple local agencies.

Generally, State police agencies are responsible for antiterrorism and have initial jurisdiction over any terrorist act. They are responsible for providing a State's support of national domestic security efforts. State police agencies are generally responsible for developing comprehensive strategies to secure the State and protect residents and visitors from acts of terrorism. In supporting national security efforts, State police agencies are at least partially responsible for developing programs to prevent and respond to terrorist incidents. The national strategy emphasizes preparedness at all levels (statewide, regional, and local). In support of this strategy, all States are mandated to develop principles of mutual aid and oversight. State police agencies play a significant role in this effort.

Most State police agencies provide the following services:

- State antiterrorism and domestic security programs;
- Statewide traffic services to keep State roadways safe;
- Statewide emergency response services and support services to the public and the criminal justice community (in conjunction with State emergency management);
- Investigation of criminal activities on State-owned and leased property; and
- Security for the governor and other State officials.

Relationships With State, Local, and Tribal Governments

State, local, and tribal authorities typically own or regulate regional and local NMI assets. DOI, as the SSA for the NMI Sector, will work closely with DHS in establishing relationships with State Offices of Homeland Security to ensure maximum information exchange within and outside the Federal Government. These State offices, in conjunction with DHS, will develop a close working relationship with other State and local agencies responsible for NMI assets as a major part of outreach efforts. As part of the asset identification process, DOI will engage DHS and the State Offices of Homeland Security to gather information from agencies and organizations within each State.

Generally, if monuments and symbols under State, local, or tribal control are considered nationally significant NMI assets, they would be included within the key resource categories of Commercial Facilities or Government Facilities. DHS is the lead SSA. DOI will work with DHS to delineate lead and support roles and responsibilities.

1.2.4 Private Sector

Private sector firms function as an adjunct to but not a replacement for public law enforcement by helping to reduce and prevent crime. They protect individuals, property, and proprietary information, and provide protection for banks, hospitals, research and development (R&D) centers, manufacturing facilities, defense and aerospace contractors, high technology businesses, nuclear power plants, chemical companies, oil and gas refineries, airports, communication facilities and operations, office complexes, schools, private universities, residential properties, apartment complexes, gated communities, museums, sporting events, and theme parks. Private sector security and law enforcement entities derive their authority from State, regional, and local laws in effect for their jurisdictions or areas of responsibility. Many assets within the NMI Sector utilize private security guards under contract, both armed and unarmed, as their sole security force or to supplement their law enforcement and security staffs.

Relationships with Private Sector Owner/Operators and Organizations

Relationships with private sector facilities currently exist but are limited. Some information on those facilities is available on the National Register of Historic Places or the List of National Historic Landmarks, but other private sector facilities also exist that have not registered or did not meet the criteria for designation. DOI, as the SSA for the NMI Sector, will rely on the DHS Infrastructure Partnership Division's relationships with private sector entities such as the Commercial Facilities Sector Coordinating Council (SCC) and others to ensure information exchange with organizations outside the Federal Government.

Generally, if private sector assets are considered National Critical NMI assets, they will be included within the Commercial Facilities key resource category, with DHS as the lead SSA. DOI will work with DHS and the private sector to delineate lead and support roles and responsibilities.

Relationships between DOI cyber system owners and private sector organizations vary among bureaus and offices. With the diverse nature of the existing cyber system environment, expectations vary but have common underlying policy requirements outlined in FISMA and DOI policy. Each IT security manager is responsible for certifying and documenting system interconnections and information-sharing arrangements at the installation that have been approved and configured securely. One vital role the DHS National Cyber Security Division (NCSD) will play is to facilitate communications and develop common approaches for working with the private sector. The Federal Government has successfully developed processes through NIST for C&A of cyber systems. Aligning these with private sector policies and procedures would greatly enhance the cooperation and understanding between both entities.

1.3 Sector Security Goals

Sector security goals state the comprehensive protective posture that the government and nongovernmental owners and operators are working together to achieve and will help lead to a steady state of protection.

These goals were developed using the full spectrum of protective activities (i.e., awareness, prevention, protection, response, and recovery). These five areas correspond to the five goals established in the DHS Strategic Plan.

Awareness

Threats

Following 9/11, DOI initiated a review of security policies at hundreds of DOI-owned assets meeting the criteria as monuments or icons. Conscious of the need to expedite implementation of enhanced security measures, DOI quickly initiated efforts to identify monument or icon assets at risk of terrorist attack. In doing so, the Department focused specific attention on those assets commonly recognized within the national or international community as being symbolic or iconic of the United States. At the conclusion of this effort, DOI identified monument or icon assets warranting special protective measures. These assets came to be referred to as National Icon Parks. Since completing the initial identification effort, DOI has reevaluated this assessment to ensure that each asset continues to be appropriately designated. The reevaluation effort resulted in adjustments to the original list of National Icon Parks.

DOI is working with its Federal partners and DHS to contact State, local, and private asset owners to determine if any of their assets should be included.

Vulnerability

The priority assets were then subjected to VAs that ranked each asset based on the nature of the threat as well as the consequences of a terrorist attack. DOI will work with DHS and other partners of the NMI Sector to develop a ranking structure for assets within the sector.

Impacts

Unlike other assets that have numerous interdependencies, NMI assets are basically stand-alone assets. The loss of or damage to an NMI asset generally will not have a cascading effect on other assets within the NMI Sector, or other sectors, such as Energy, Transportation, Food, and so on. Damage to an NMI asset could undoubtedly result in a drastic increase in security, and possible closure, of other NMI assets. Also, the economic impact of an attack may significantly affect the local and national tourism industry. However, the greatest potential impact will be on the national psyche. An attack on a National Critical asset could result in significant loss of life and intense media coverage with visual reminders of the death and destruction. It could also reduce public confidence in our Nation's ability to protect its citizens and resources against attack.

Prevention

Detection

The ability of intelligence agencies to detect potential terrorist attacks has been enhanced significantly in recent years. A critical component of any attack is prior surveillance of the target. This is also one of the points where our adversaries are the most vulnerable. A robust and effective countersurveillance program is critical to detecting the preattack indicators.

Countersurveillance relies heavily on the law enforcement and security staffs at or near an asset. An often overlooked component of countersurveillance is the observations of non-law enforcement personnel at the site, such as maintenance workers, interpretive staff, and volunteers. These individuals are thoroughly familiar with the area and may be cognizant of anything or anyone who seems out of place. By reporting their observations to law enforcement, they have a major impact on deterring an attack.

Deterrence

The results of a VA will demonstrate where each asset is most susceptible to an attack. Combined with a risk assessment, the VA will determine the measures that must be taken for each asset, and in what order, to reduce the risk of an attack to an acceptable level.

Depending on the assessments, as well as the particular situation at each site, the increased protective measures could be as simple as restricting parking adjacent to the facility or as complex as building an effective vehicle deterrence system. In some cases small, low-cost changes can have a significant impact on deterring potential attacks.

In many instances, implementing certain protective measures at the asset will not be feasible due to costs or other influences involving the historic footprint of the site. In these cases, the mitigation of a potential attack would receive added emphasis.

Mitigation

Because of the accessible nature of this sector's assets, many of the detection and deterrence measures used in other sectors are not available or are not acceptable to asset owners, oversight committees, or the public. For those threats that cannot be deterred, an effective mitigation plan must be established. In many cases, this will mean close coordination with local emergency services agencies to ensure a quick and effective response to any incident.

Protection

The concept of protection differs within the NMI Sector as compared to other sectors due to the accessibility of most sites. Whereas other sectors can institute protective measures that restrict access to the asset, the NMI Sector must use protective measures that do not unnecessarily impede access and are not overly visible.

In the post-9/11 era, citizens are more accepting of protective measures but only to a point. Protection of many of our assets requires spending significant resources to convince legislative staff, regulatory and advisory agencies, and the public of the need for enhanced protective measures. For some of the sector's high-profile targets, such as the Statue of Liberty and the Washington Monument, the use of magnetometers and x-ray machines to screen visitors has been successfully implemented. In other more open sites, such as the Lincoln Memorial and Mount Rushmore National Monument, screening visitors is not occurring.

Vehicle-borne improvised explosive devices (VBIED) are an area of concern at many sites. Some sites have little or no standoff distance from major roadways and are extremely vulnerable to VBIEDs, highlighting the need for innovative approaches to reducing this vulnerability.

The release of a chemical, biological, radiological, or nuclear agent is also a concern at many sites. Some sites have detection sensors in place, while others are connected to area-wide networks, but many have no detection equipment in place. The cost of responding to false alarms is problematic. In many instances, the expense needed to adequately safeguard against these types of attacks does not justify the additional margin of protection.

Response

In the case of threats that NMI assets cannot adequately protect against, the capability must be in place to mitigate the effects of a potential attack.

A key issue related to several potential attack scenarios is the ability to respond quickly with onsite security personnel to prevent the attack or minimize the effects. For those sites where onsite security is adequate for general activities but insufficient to deal with an attack, it is critical that local first responders be available to quickly supplement the onsite assets.

Recovery

Most NMI assets do not have interdependencies with other sectors and are not a critical component to the operation of other sectors. The time needed to restore the sites following an attack or all-hazards incident is not as critical as it is in other sectors. In some cases, the best course of action should an attack or all-hazard incident destroy an asset would be not to rebuild the asset.

The successful efforts taken to meet the goals and objectives in the sector, while addressing these five protective activities, will help the NMI Sector achieve a long-term security posture.

1.3.1 Elements and Characteristics of Sector Security Goals

Vision Statement for the National Monuments & Icons Sector

The NMI Sector is committed to ensuring that the symbols of our Nation remain protected and intact for future generations. In the course of protecting our landmarks, the sector will ensure that staff and visitors are protected from harm. Because citizen access to these monuments and icons is a hallmark of life in a free and open society, the sector will strive for an appropriate balance between security, ease of public access, and aesthetics. However, the sector's ultimate goal is to provide the appropriate security posture that will discourage America's adversaries from choosing our NMI assets as opportune targets.

Sector Security Goals

The NMI Sector will work toward the following goals:

Goal 1: Establish clear criteria to define nationally critical versus State or locally critical assets. To comprehensively implement protective programs, the SSA will work with security partners at all levels of government and the private sector to distinguish National Critical assets from National Significant, Regional Critical, and Local Significant assets and to identify NMI assets whose primary protective responsibility falls within the scope of another sector.

Goal 2: Clearly delineate and define roles and responsibilities for all sector security partners. The NMI Sector will work with security partners to clarify the roles and responsibilities in providing security in the sector to achieve the following objectives:

- Allocate resources effectively;
- Integrate protection plans; and
- Coordinate a response in the event of an emergency.

Goal 3: Perform risk assessments on critical assets. The NMI Sector will conduct or facilitate risk assessments on a priority basis for National Critical monuments and icons.

Goal 4: Enable rapid and robust communications among intelligence and law enforcement agencies and Federal, State, local, and private security partners. To adapt security measures to emerging threats, the sector will develop secure information-sharing channels between DHS and State and local law enforcement agencies and the individuals operationally responsible for protecting the sector's assets.

Goal 5: Ensure seamless coordination among Federal, State, and local agencies as well as any private sector entities that own or operate sector assets. Effective implementation of sector security programs will require coordination among a wide range of security partners, including DOI, municipal governments, site-specific owners and operators, private sector owners, foundations, or nonprofit stewards of sites and symbols.

Goal 6: Implement cross-sector coordination with regard to NMI assets whose primary protective responsibility resides in another sector. The sector will work with other CI/KR sectors to ensure that protective programs reflect the multi-use nature of certain critical NMI assets. Such cross-sector coordination would include Dams, Transportation Services, Government Facilities, and Commercial Facilities.

Goal 7: Integrate robust security technology and practices while preserving the appearance and accessibility of NMI sites. Monuments and icons are important symbols of our Nation's heritage and identity. It is imperative to the sector and to the Nation that these assets remain open and accessible to the public. NMI security measures will thus limit, to the extent possible, restrictions on public access or degradation in the scenic appeal of sector assets.

Goal 8: Develop flexible security programs to adjust to seasonal and event-specific security challenges. Many NMI assets experience dramatic seasonal or holiday-specific fluctuations in visitor volume (e.g., Fourth of July celebration on the National Mall), while a special event might increase the public attention given to a monument or icon. These variables can increase the threat, vulnerability, and/or consequences associated with an attack on the asset. Sector security measures must be flexible enough to enable appropriate responses to seasonal and event-driven increases in risk.

Goal 9: Protect against insider threats. NMI security partners will work together to develop guidelines for protecting against insider threats, such as vetting and credentialing security personnel, enhancing surveillance capabilities, and conducting employee background checks as appropriate.

Goal 10: Develop contingency response programs. NMI security partners will create contingency response programs to ensure the safety and control of visitors at critical sites in the event of a terrorist attack or all-hazards incident.

1.3.2 Process to Establish Sector Security Goals

The initial process for establishing security goals for the NMI Sector involved obtaining asset data from other Federal, State, local, tribal, and private entities and determining what information should be included in the data set. The next step was to reach consensus as to which of the assets would be better served by another SSA that more closely mirrors the assets' function (such as the Golden Gate Bridge, which has iconic value, being listed under the Transportation Services Sector) and which of the assets fit into the definition of a National Critical NMI asset.

Once DOI had a clear understanding of the assets that would be included within the NMI Sector, a determination was made as to which assets should be considered "assets of consequence." Most of DOI's focus will be directed toward effectively securing these sites. As assets belonging to State, local, tribal, or private entities are identified, they will be ranked and a determination will be made concerning whether they rise to the level for inclusion within the NMI Sector.

NMI Sector sites encourage visitation and generally strive to present an open and accessible posture. To further complicate the issue, many assets must obtain approval from advisory or preservation groups before any modifications can be made to the site, whether security related or not.

The types of assets within this sector, and the outside influences on each asset, make it impossible to create one security plan to fit all. Some of these outside influences include the following:

- **Property around an asset belonging to another entity or jurisdiction:** An example of this would be at Independence National Historical Park where a city street divides Independence Hall and the Liberty Bell pavilion. The city's reluctance to close the roadway permanently has created security challenges.
- **Location in a remote area:** At Mount Rushmore National Monument, for instance, the nearest available emergency responder in the event of a terrorist attack or all-hazards incident would be more than 30 minutes away. As a result, the staffing levels have been increased to stabilize an incident until additional resources can arrive.
- **An asset belonging to another agency located on DOI property:** The USS Constitution, a designated National Icon, is located in Boston National Historical Park. The vessel is commissioned as a U.S. Navy warship and is staffed by Navy personnel but open to the public. This creates unique challenges for the NPS and the Navy as they jointly manage and protect the asset.

These challenges have resulted in different security plans being developed at each site. They do, however, have the same basic detection and deterrence methods underlying the plans.

1.4 Value Proposition

All of the assets in the sector designated as National Critical are government owned. They do not generate income nor are they intended to do so. The asset owner and operators are limited in the actions they can take to protect the assets by available funding allocated through Federal, State, and local budget processes. In most cases, funding for infrastructure protection programs is in direct competition with funding for operational needs within each agency.

An additional impediment to an effective infrastructure protection program in this sector is the desire to maintain the accessibility of the assets.

Security officials charged with protecting the asset must justify proposed protective measures to their agency decision makers, commissions or boards with architectural oversight authority (e.g., fine arts commissions and regional and local planning commissions), and, to a lesser extent, the visiting public. Therefore, it is imperative that emerging security and protection technology be cost effective and unobtrusive.

In addition, because of acute staffing shortages, emerging security and protective technology that is cost effective and can act as a force multiplier would be readily accepted. This is a key challenge to be addressed by future technology.

The value of working within the NMI Sector will be the ability to develop best practices to protect our assets and to partner with outside commissions and agencies. Federally owned assets are self insured, the destruction of the asset will more than likely result in extreme pressure to replace the asset. Rebuilding costs will greatly exceed the cost to adequately protect the asset.

2. Identify Assets, Systems, Networks, and Functions

The process for identifying NMI assets will be a collaborative effort between DOI, DHS, the NMI GCC, and other supporting and lead SSAs. DOI will work closely with DHS in establishing relationships with the private sector to ensure maximum information exchange within and outside the Federal Government.

2.1 Defining Information Parameters

A number of NMI assets located within the United States and its Territories (e.g., Puerto Rico and the Northern Mariana Islands) are listed on the National Register of Historic Places or the List of National Historic Landmarks. The National Register of Historic Places is the Nation's official list of cultural resources reserved for preservation. The National Historic Landmarks are significant historic places designated by the Secretary of the Interior for their exceptional value or quality in illustrating or interpreting the heritage of the United States. Currently, fewer than 2,500 historic places bear this national distinction. The criteria applied to evaluate properties for possible designation as National Historic Landmarks are delineated in the Code of Federal Regulations (36 CFR 65.4, National Historic Landmark Criteria).

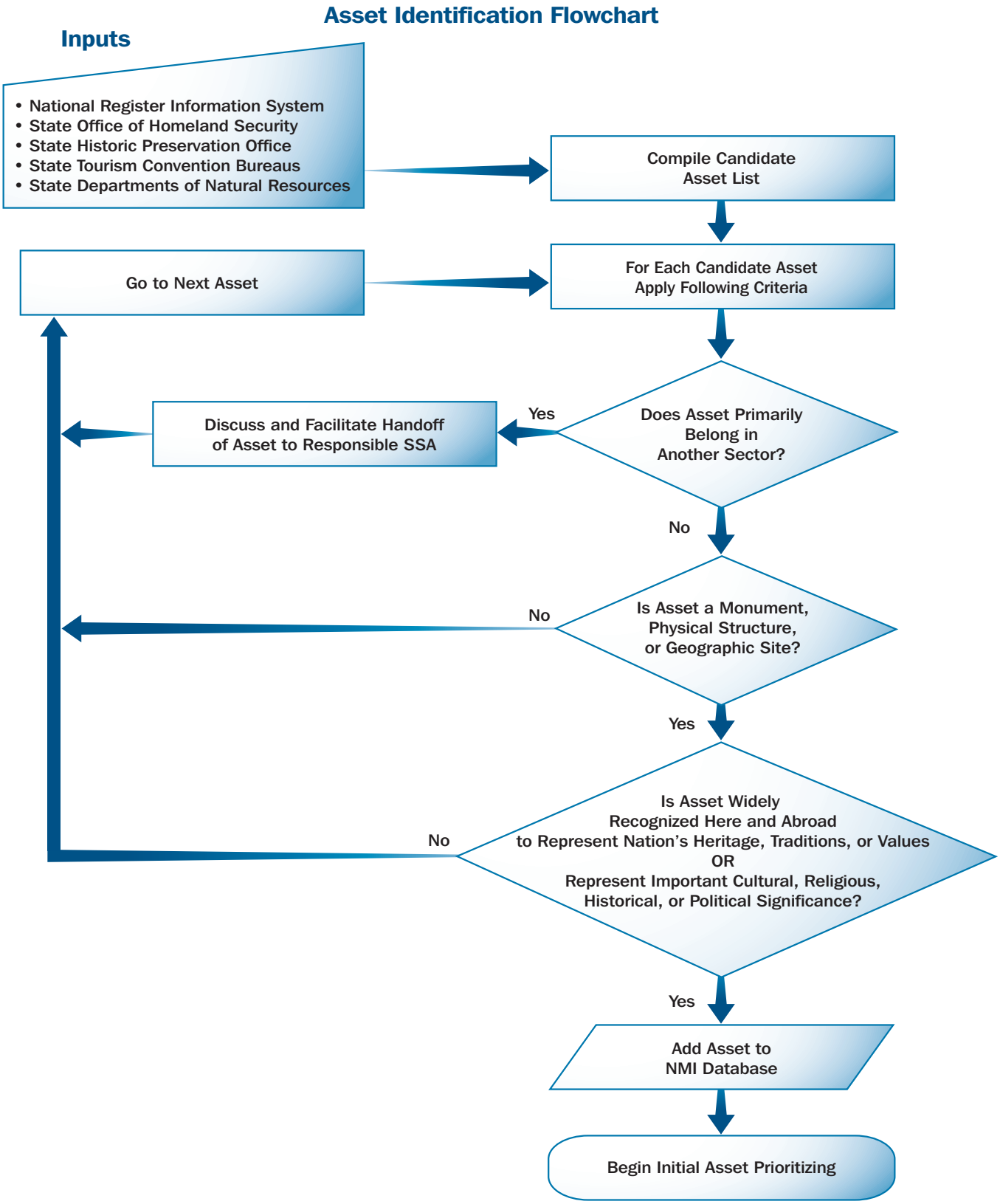
In addition, DHS developed the National Asset Database (NADB), which is being populated with input from various Federal, State, local, and tribal governments. The NMI Sector has worked closely to define the appropriate data fields to be included within the NMI section of the NADB.

These major listings will be used as a starting point to determine National Critical assets in the NMI Sector. Through DHS and State Offices of Homeland Security, DOI will work at the Federal, State, local, and tribal government levels, and with the private sector, to identify other NMI assets that may not be on either list but should be considered as National Critical.

Based on information gathered at the State level, DHS and State Offices of Homeland Security will reach out to local governments and the private sector as necessary to obtain information on National Critical NMI assets.

Once an asset is considered for the NMI category, a formal process will be used to determine whether it qualifies for inclusion in the NMI Sector. The process focuses on identifying assets that are the primary responsibility of the NMI Sector, which include monuments, physical structures, and objects of national importance. Specifically, the goal is to capture those physical assets that are widely recognized as having national cultural, religious, historical, or political significance. Figure 2-1 illustrates the process flow for identifying NMI assets.

Figure 2-1: NMI Asset Identification Flowchart



DOI has worked with DHS to develop a set of asset descriptors, or data fields, that will be collected for each NMI asset.

DOI will develop a template for collecting asset information that will help ensure consistency in data collection across the sector and from diverse stakeholders. The template also will ensure that data can be captured for integration and comparison within the NADB.

The taxonomy developed for the NMI Sector breaks down the assets into the following categories:

- National Monument/Icon Structures:
  - Buildings;
  - Monuments; and
  - Other Monument/Icon Structures;
- National Monument/Icon Geographic Areas:
  - Parks; and
  - Historical Areas;
- National Monument/Icon Documents and Objects:
  - Historical/Significant Documents;
  - Historical/Significant Objects; and
  - Other National Monuments/Icons.

Specific data to be collected for each of the National Critical NMI assets will include the following:

- Asset name and address or general description of location;
- Responsible entity/owner and address;
- Category of asset within the sector (e.g., monument, building, museum, etc.);
- Purpose and basis for asset's criticality;
- Relationship to other sectors (e.g., Energy, Government Facility, Transportation, Commercial);
- Seasonality/frequency of use;
- Annual visitors/maximum daily visitors;
- Number of operations staff on site;
- Average/maximum number of visitors within 100 meters;
- Large-scale special events/schedules;
- Nearby population base/population density;
- Annual revenues including associated area economic impact (e.g., vendor revenues);
- What the asset depends on to function (e.g., computers, IT systems, telecommunications, utilities, and other dependencies);
- Interdependencies (i.e., what depends on asset operability) (people, physical, IT, telecommunications, economics, and other sectors);

- Security measures in place;
- VA completion status (annual updates contingent on available funding and as warranted);
- Ongoing threat status mechanism;
- Impact to area in cases of loss or failure (e.g., economic, public health and welfare, public psyche);
- Interface with local law enforcement agencies/mutual aid agreements; and
- Critical interdependencies with other infrastructure sectors.

Assets determined to be National Significant, Regional Critical, or Local Significant will not be specifically assessed by DOI as part of the implementation process for this SSP. However, all information and protective programs developed by the implementation of this SSP for the National Critical NMI assets will be shared with State, regional, and local stakeholders for application to their specific assets.

Once the data on National Critical NMI assets have been collected and consolidated, DOI will then assist DHS and site owners/operators in implementing a process for assessing the potential consequences that may result if the asset were compromised. The intent of the assessment is to provide a baseline screening of the assets within the sector to determine their criticality and whether they are a potential candidate for additional protective actions beyond what is currently being provided. DOI will develop a systematic and standardized process to assess the worst-case consequences of a successful terrorist attack or all-hazards incident that in turn will facilitate ranking and prioritizing the National Critical NMI assets.

2.2 Collecting Infrastructure Information

As previously discussed, other than information contained in the National Register of Historic Places and the List of National Historic Landmarks, DOI has limited information concerning assets that it does not own. DOI will work with the DHS Office of State and Local Government Coordination and Office of Infrastructure Protection to determine the assets within each State that could be considered for inclusion as a National Critical monument and/or icon.

Once the initial list has been established, DOI will compile the necessary data through checklists or questionnaires sent to the asset owners.

Some stakeholder information may contain confidential, proprietary, or business-sensitive data. The information is exempt from public disclosure in accordance with the Protected Critical Infrastructure Information (PCII) program, implemented by 6 CFR Part 29. The PCII program requires rigorous safeguarding and handling procedures to prevent unauthorized access to information submitted under the program. This information must be voluntarily submitted directly to DHS and be accompanied by an Express Statement requesting protection under the Critical Infrastructure Information Act of 2002. All information requests to NMI asset stakeholders will be developed in close coordination with the DOI legal staff and DHS PCII program representatives to ensure that the PCII program requirements are met.

Once the checklist and instructions are developed, the information request will be sent to participating government agencies and private sector entities.

Information collection, control, and consolidation into a database will be an essential element following the return of NMI asset information from the participating government agencies and private sector entities. DHS will formulate and implement project procedures to ensure that the asset data are managed properly and securely. As outlined in the NIPP, DHS will maintain the NADB and will include information concerning all CI/KR.

During the NMI asset identification and data collection phase, DOI will not compile a list of NMI assets that fall within other CI/KR sectors. However, DOI will support other SSAs through information sharing and the development of protection programs that address preservation of the asset's iconic value. DOI will encourage other SSAs having assets with iconic value and other NMI Sector stakeholders to be involved in the communication and information-sharing functions of the NMI Sector. Of critical importance to establishing this collaborative relationship is recognition that one of the primary goals is to preserve public accessibility to National Critical assets to the maximum extent possible. DOI will confer with the lead SSA to ensure that this goal is maintained in conjunction with high standards of protection for assets that are the primary responsibility of another sector.

DOI has performed an analysis of cyber assets in accordance with DHS NCSD guidance. The results of this analysis indicate that the sector's cyber assets are not sufficiently critical that damaging or destroying them would interfere with the continued operation of NMI assets. Cyber assets are used primarily for security (e.g., video scanning technology), and redundant physical systems are in place as backup in the event that the cyber systems fail.

2.3 Verifying Infrastructure Information

Additional verification of National Critical NMI information from DOI-owned assets will likely be minimal. For additional assets deemed appropriate for inclusion within this sector, DOI will work through the NMI GCC to verify the data. Depending on the asset and resources available, site visits to selected non-DOI-owned assets may be necessary to verify the information.

2.4 Updating Infrastructure Information

DOI will review the data on National Critical NMI assets and coordinate with the GCC for updates on an annual basis. In addition, stakeholders will be requested to update their asset profiles as soon as possible whenever a significant change occurs in their security posture or operating characteristics (e.g., addition of a new visitor's center).

DOI will collect the information and forward it to DHS. DOI will work closely with DHS to ensure that the information is protected and develop appropriate sharing mechanisms to facilitate accessibility to sector stakeholders.

3. Assess Risks

DOI and the other NMI Sector partners have risk assessments in place for their assets. Several discussions have occurred with DHS concerning normalizing these risk assessments with Risk Analysis and Management for Critical Asset Protection (RAMCAP) to establish a common threat picture across all sectors. It is believed that this will be possible without any difficulty. The NMI Sector will work closely with DHS in the coming months to accomplish this.

3.1 Risk Assessment in the Sector

The initial step in determining asset risk within the NMI Sector is to ascertain which assets pose a significant concern and warrant further analysis. A terrorist attack on an NMI asset could impact national morale and confidence; cause significant loss of life and casualties, political and economic disruption, or environmental damage; and, in some instances, have a negative impact on other CI/KR sectors. Due to these potential consequences, the vulnerabilities of our Nation's NMI assets and the threat of an attack must be assessed so measures and programs can be implemented to protect these symbols of national culture and heritage. The risk assessments of the NMI assets address physical structures, personnel, cyber/IT, and other dependencies.

Because cross-sector impacts of a terrorist attack on an NMI asset would be limited, and because most of the assets stand-alone entities that are not tied to each other in any way, the risk assessments will be done for each specific asset and not as part of a network or system.

No overarching regulatory authority within the sector mandates risk assessments. However, most assets are owned by government agencies and are covered by internal requirements mandating risk assessments. This is true within DOI where risk assessments are mandated for all icon parks.

In addition, the NIPP requires that the SSAs lead sector-specific risk management programs as part of the overall effort to ensure a steady state of protection within and across the CI/KR sectors.

3.2 Screening Infrastructure

The initial step in the risk assessment process is the characterization of the sector assets and comprises the following two elements:

- A ranking system based on the uniqueness of the asset and its significance as a national symbol; and
- Consequence categories encompassing SSP guidance from DHS.

The first step in the risk assessment process is independent of the threat scenario and is a measure of the impact on the national morale and public confidence caused by damage or destruction of a significant monument or icon. The ranking system will determine if a monument or icon is a National Critical, National Significant, Regional Critical, or Local Significant NMI asset.

The concept is defined in table 3-1. For purposes of consistency and standardization, the National Significant, Regional Critical, and Local Significant categories are added for application of the methodology by State, regional, and local authorities. The NMI SSP will assess those assets designated as National Critical. Other assets will be assessed by the requisite authority, with support as necessary from DHS and DOI.

Table 3-1: Tier Levels

Tier level	NMI Asset Characteristics	Point Value
National Critical	Assets of unique quality, widely recognized both nationally and internationally to be symbolic of the United States.	
National Significant	Assets generally recognized nationally to be significant symbols of the United States.	
Regional Critical	Assets of unique quality, widely recognized as having significance on a regional level.	
Local Significant	Assets generally recognized as significant on a local level.	

3.3 Assessing Consequences

The second step of the process uses the SSP guidance developed by DHS regarding criteria for consequence categories and results in a numerical ranking based on postulated, worst-case scenarios. The estimates used in the following exhibits are derived from modeling and elicitation of expert opinions. The consequence categories are defined as follows.

- **Loss of Life and/or Casualties:** A measure of the number of individuals (under normal/average visitation) that could be killed or wounded in and around the asset's immediate area;
- **Economic Impact:** A measure of overall dollar-cost impact including direct and indirect loss of business and tourism revenue, economic impacts on overlapping sectors, costs of emergency response, costs of environmental cleanup, and so on;
- **Length of Outage/Disruption:** A measure of the length of time it would take to resume normal operations;
- **Impact to Other Sectors:** A measure of asset interdependency reflected in a correlate loss of function in other sectors; and
- **Environmental Impact:** A measure of the acreage impacted including direct and indirect effects on natural resources and wildlife, loss of use due to environmental damage and associated remediation, and so on.

Due to the irreplaceable value of NMI assets and their unique importance to our culture and national heritage, the overall consequence calculation is weighted higher (by a factor of two to one) in the tier-ranking exercise in section 3.2 than the impacts based on the categories outlined in this section: casualties, economic impact, length of outage/disruption, impact to other sectors, and environmental impact. This results in a prioritization based on symbolic value and impact on the public morale and confidence as the prime considerations for the NMI Sector.

Once the impact of the threat scenarios is determined and the tier consequence value is established, the total consequence ranking for each threat scenario as applied to an asset can be calculated. The consequence ranking for each threat scenario is determined by the sum of the individual numerical rankings from each consequence category. The calculation may be expressed in a numerical equation as follows:

$$C_{\text{Attack Scenario Total}} = (2 \times C_{\text{Tier Level}}) + C_{\text{Casualties}} + C_{\text{Economic Impact}} + C_{\text{Length of Outage/Disruption}} + C_{\text{Impact to Other Sectors}} + C_{\text{Environmental Impact}}$$

Each of these consequence categories will include a numerical ranking that assigns the impact of the scenario into bins of consequences. Appropriate technical expertise, specifically DHS-NCSD, will be utilized as required during the performance and review of initial consequence assessments for NMI components. See table 3-2 for an example of the consequence value table.

This worst-case consequence assessment provides an initial prioritization of National Critical NMI assets and establishes the basis for the subsequent detailed analysis of consequences.

Table 3-2: Consequence Values

Attack Scenario	Asset Tier Level	Number of Casualties	Economic Impact	Length of Outage	Impact to Other Sectors	Environment Impact	Total Consequence Value
	Tier Level + Casualties + Economic + Outage + Other Sectors + Environmental = Attack Scenario Total						
						Overall Consequence Value for Asset	

3.4 Assessing Vulnerabilities

This section outlines the process of how National Critical NMI assets (including critical information and telecommunications components) will be assessed to identify vulnerabilities to possible terrorist events. The section also presents the methodology for determining the overall risk of attack. DOI will use the risk calculations to prioritize the National Critical NMI assets to facilitate appropriate implementation of protective measures and program requirements. DOI will conduct risk calculations for its own facilities and encourage other asset owners to implement the methodology presented herein for those NMI assets not owned or operated by DOI. DOI will make the methodology available to other sector stakeholders, including State and local authorities, which will be expected to follow the same methodology guidance with support from sector resources as needed.

3.4.1 Assessing Security System Effectiveness

In the initial step of the risk assessment process, a standard VA approach is used to identify security weaknesses of the asset. The weaknesses are determined based on an assessment of the effectiveness of the asset's existing security systems and procedures to prevent or mitigate the specified attack scenarios being considered. In order to measure each security system's effectiveness against a specific attack scenario, "effectiveness" has been divided into five levels, each of which is assigned a corresponding point value ranging from 0.1 to 0.9. For example, if an assessment of the asset's vulnerability to an improvised explosive device (IED) attack determines that existing security systems and procedures are likely to prevent or mitigate the attack to a level resulting in little or no damage, the system would be considered Fully Effective and assigned a point value of 0.9. See table 3-3 for a description of the effectiveness characteristics of the security system.

Table 3-3: Security System Effectiveness

Security System Effectiveness	Security System Characteristics	Point Value
Fully Effective [Very High]	The system presents an obstacle expected to prevent an adversary from achieving the attack scenario objective.	0.9
Effective [High]	The system presents an obstacle that would require a high level of effort to overcome in order for an adversary to achieve the attack scenario objective.	0.7
Somewhat Effective [Moderate]	The system presents an obstacle that would require moderate effort to overcome in order for an adversary to achieve the attack scenario objective.	0.5
Minimally Effective [Low]	The system presents an obstacle that would require minimal effort to overcome in order for an adversary to achieve the attack scenario objective.	0.3
Ineffective [Very Low]	The system presents no obstacle to prevent an adversary from achieving the attack scenario objective.	0.1

3.4.2 Gauging the Likelihood of Successful Attack

After establishing the effectiveness of the security systems to prevent or mitigate the specified attack scenarios, the assessment process gauges the likelihood of success for each attack scenario. This is accomplished by establishing the likelihood of a specific attack occurring and the effectiveness (or ineffectiveness) of the security system to protect against that attack. In order to develop a baseline risk value, it is assumed that each of the specified attack scenarios is credible and has an equal probability of occurrence. Given this parameter, the likelihood of an adversary successfully executing a specific attack scenario can essentially be measured as the inverse of the Security System Effectiveness point value for that attack scenario.

Likelihood of Successful Attack = 1 - System Effectiveness → $L_A = (1 - S_E)$

For example, if the asset's security system is considered Fully Effective (a point value of 0.9) against an attack scenario, the likelihood of a successful attack being carried out would be considered Very Low (a point value of 0.1).

The point values assigned to the System Effectiveness and Likelihood of Successful Attack categories are developed using available documentation, concurrent site surveys, interviews with security personnel familiar with the asset and its operation, and onsite reviews. These resources provide the survey team with a snapshot of the asset's current security posture from which to assess each attack scenario.

3.4.3 Calculating Risk Values

Once the effectiveness of the asset's security systems and the likelihood of successful attack have been determined for each scenario, the process of calculating risk values can proceed. Using the Total Consequence Value developed for each scenario during the Consequence Assessment Phase (section 3.3) and the corresponding values for the Likelihood of Successful Attack (section 3.4.2), the risk associated with each scenario can be quantified. The Risk Value is derived by multiplying the Total Consequence Value by its corresponding Likelihood of Successful Attack Value.

Risk Value = Likelihood of Successful Attack x Total Consequence Value → $R_{TS} = L_A (1 - S_E) \times C_{\text{Attack Scenario Total}}$

As a final step, the risk values for each scenario are added together to derive the asset's Overall Risk Value. The Overall Risk Value can be translated into a corresponding asset vulnerability rating of High, Medium, or Low. The Overall Risk Value provides a means of evaluating the effects of improvements such as security hardware enhancements, operational changes, and staffing increases in reducing an asset's security vulnerabilities and allows for the relative ranking of all NMI assets. Overall Risk Value can be calculated using table 3-4.

The System Effectiveness, Likelihood of Successful Attack, Total Consequence Value, and Risk Value can be shown in the table. Combining these factors produces the Overall Risk Value score.

Table 3-4: Overall Risk Value

Attack Scenario	System Effectiveness	Likelihood of Successful Attack	Total Consequence Value	Risk Value
	$S_E + L_A (1-S_E) \times C_{\text{Attack Scenario Total}} = R_{TS}$			
			Overall Risk Value for Asset	

3.5 Assessing Threats

The threat scenarios considered for the NMI Sector are high level and are considered applicable for all assets. The threat of each potential attack scenario is based on an understanding of the adversary's intent and an assessment of the adversary's capability.

Although a general threat underlies the sector due to the open accessibility of NMI assets, each asset has its own distinct vulnerabilities, due to location, surrounding geography, structure, and so on. Close collaboration with responsible law enforcement and security personnel is necessary to facilitate understanding and assessing the threat level faced.

DOI will work internally through its intelligence units, and externally with other intelligence agencies as well as DHS's Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), to assess the overall threat to the sector and individual assets whenever specific information is available.

4. Prioritize Infrastructure

When a determination is made that an asset belongs within the NMI Sector, the first step in the prioritization process is to place the asset into a specific tier level bin (National Critical, National Significant, Regional Critical, or Local Significant) as described in section 3.2. To date, DOI has completed this initial prioritization. As the sector matures, the NMI GCC will be responsible for determining the bin into which an asset falls.

DOI will subject assets designated as National Critical to the NMI risk assessment methodologies described in sections 3.3 and 3.4 to develop a numerical score based on the consequences and vulnerabilities of each asset. DOI will conduct the assessment for those assets it owns and will work with the owners of other assets to ensure that the assessment is conducted.

DOI will work through the NMI GCC and with the Government Facilities Sector to ensure that owners of assets categorized as National Significant, Regional Critical, and Local Significant have access to the methodology. DOI will not assist in the actual assessments due to staffing and funding limitations.

Once priorities are established, they will become the basis for resource allocation and protective program development.

Reassessments of DOI-owned National Critical assets will be conducted on a biannual basis. In the event that the security posture changes significantly, a reassessment may be conducted to accurately address any new risks.

5. Develop and Implement Protective Programs

5.1 Overview of Sector Protective Programs

The NMI Sector has several distinguishing risk management characteristics that aid in defining the sector's end state:

- The sector's structures, locations, and artifacts are recognized worldwide as unique historical and cultural symbols of American values, history, and national identity. Many of these assets are inherently irreplaceable, physically and psychologically, and a successful terrorist attack on the sector could have dramatic consequences for public morale. Accordingly, the risk management focus in the sector is heavily weighted toward prevention and protection.
- NMI assets are typically stand-alone assets or sites located in urban and rural settings, such as bridges, ships, documents, artwork, monuments, estates, and mountains. Although the assets are by nature static and defined (e.g., the Washington Monument), the environment surrounding the asset is dynamic (e.g., the National Mall) and, therefore, challenging from a security standpoint. Operational and protective requirements may also vary depending on the season and/or occurrence of a special event.
- NMI assets must be open to the public and attention must be paid to preserve the historic or artistic value of the site as a whole. Protective measures are thus set in the context of community standards on accessibility and the desire to maintain the aesthetics of the site. The intrinsically public nature of the sector and the limitations imposed on its protective measures makes NMI assets more challenging to protect from potential attacks.
- Monuments and icons attract large numbers of visitors and present attractive targets for adversaries. Protective measures must ensure the security of the site itself and plan for the safety of visitors in an emergency situation.
- National icons may also serve other critical infrastructure needs and fall primarily under the protective domain of other sectors (e.g., Hoover Dam is under the oversight of the Dams Sector, while the Sears Tower is classified in the Commercial Facilities Sector).
- Funding for public safety and security programs generally comes from operational funds, especially for those assets owned by DOI. This creates competition for available funding between operational and security programs.

5.2 Determining Protective Program Needs

Because of the highly distributed nature of the assets in the NMI Sector, the responsibility for protection is shared among affected Federal, State, local, and tribal governments, as well as the private sector.

DOI, key stakeholders, and asset-specific law enforcement have developed and implemented protective programs on an accelerated basis since 9/11. A mix of new regulations, congressional mandates, actual and perceived threat information, and vulnerabilities is driving these programs. DOI's approach to protecting natural and historic sites and 1.3 million visitors daily provides a solid foundation for the NMI protection program. The following three capabilities can be leveraged to address other sector assets:

- Experience DOI gained in conducting risk-based VAs on iconic national monuments, including threat assessments and recommended security upgrades;
- Significant experience in identifying, implementing, and evaluating physical protection strategies for visitors to national parks; and
- Access to VAs, security plans, and response plans from law enforcement agencies that are currently protecting some of the high-risk NMI assets.

DOI, in consultation with DHS, is following a systematic, threat-based approach to develop protective programs across the entire sector.

In addition, many of the sector partners have programs in place to mitigate the effects of natural disasters that may impact their assets. DOI, through several of its bureaus, is heavily involved in monitoring earthquakes and volcanoes, and works closely with several other Federal agencies to track hurricanes. A wide spectrum of Federal, State, local, and tribal government agencies, as well as the private sector, routinely share this information.

5.3 Protective Program Implementation

DOI recognizes the need for a systematic approach in developing protective programs to ensure a consistent, efficient, and effective level of protection across the NMI Sector. In addition, DOI is responsible for most assets within the sector designated as National Critical and has a long history and extensive experience in protecting NMI assets.

DOI will use a methodical, disciplined approach to match limited resources with National Critical NMI assets and share validated protective measures currently in use throughout DOI with other stakeholders. Because National Critical NMI assets crosscut different Federal agencies, the participation of all entities is paramount to ensuring the highest level of protection for our Nation's NMI assets.

DOI has developed a chapter in its departmental manual that describes the minimum required protective measures that must be in place at all DOI-owned critical infrastructure (see appendix 3). The standards capture best practices from a security perspective and outline minimum recommended measures for each asset. The Department has identified baseline physical security standards as well as additional, more rigorous standards for implementation as the threat level against an asset or the sector increases.

NMI assets are designed to attract and encourage visitation. Security at NMI assets must be unobtrusive and flexible to accommodate large numbers of visitors but still provide security commensurate with the level of risk identified. Following completion of the vulnerability and risk assessments (as discussed in section 3), DOI will continue to coordinate development and implementation of physical security protection for NMI assets.

DOI will do the following:

- Identify security strengths and weaknesses based on asset characteristics;
- Evaluate risks based on seasonal and holiday considerations and adjacent critical infrastructures;
- Develop a matrix with asset characteristics and vulnerabilities;

- Develop risk-prioritized listing of sector assets to facilitate application of protective measures using a graded approach;
- Develop a set of minimum-security standards for each tier of NMI assets; and
- Develop a set of recommended security enhancements for elevated threat or alert levels.

DOI leadership will determine whether the risk assessments warrant action and whether the recommended courses of action are feasible based on available resources and other factors. At this juncture, the risks associated with DOI-owned NMI assets are known, and the decision concerning what level of risk is acceptable will be made.

Because many NMI assets are not owned by the Federal Government, and there is no regulatory authority to require compliance with protective program measures, DOI will work with DHS and other agencies to promote cooperation and involvement of stakeholders in implementing this plan. The SSA's role under this initiative is to share information with stakeholders and encourage involvement.

Because many NMI assets are located in urban settings and have become an integral part of the fabric of city life, a critical component of the decisionmaking process is to develop a strong dialogue with civic leaders, community groups, historic preservation officials, architects, and others regarding the proposed measures.

The following are examples of security-related measures that have been implemented at DOI-owned assets to improve protective measures by leveraging scarce resources:

- DOI officials at the Statue of Liberty have partnered with DOD research units to test emerging technologies that may eventually be used to protect military personnel and facilities. The partnership has provided the Statue of Liberty with cutting-edge protective technology at no cost to DOI and has facilitated product testing in a real-world application.
- DOI officials at Mount Rushmore National Monument have manipulated the natural landscape palette to augment the existing perimeter control barrier surrounding the asset. They have leveraged the passive use of the physical environment to effectively reduce the risk of a VBIED attack at the asset.
- DOI officials at NMI assets are incorporating appropriate security awareness messages in printings of park newspapers and brochures disseminated to visitors.

The following paragraphs describe broad protective measures and programs in all facets of the security spectrum:

Awareness

DOI has assessed risk, vulnerability, and threat information for DOI-owned assets to establish a readiness standard. In addition, with stakeholder participation, DOI will catalog critical NMI assets, including their vulnerabilities across the threat spectrum.

Prevention/Protection

DOI's prevention and protection strategy is based on employing best practices, developing standards, providing guidance, and issuing internal DOI security directives. DOI will share the best practices, standards, lessons learned, and other aspects developed through stakeholder interaction. DOI also may conduct annual exercises at DOI-owned assets to test specific plans and to assess the strength, viability, and level of preparedness. DOI will use a readiness assessment system to measure the industry's security posture in response to the threat level established by DHS.

Specific Protective Measures

DOI will develop a menu of protective items to facilitate selecting the best protective practices applicable to a specific situation. The process will be as open as possible to enable the individual asset owners and operators to select the solution best tailored to their needs based on the results of the risk assessments conducted for their assets.

- Protective measures can be specific to a single asset or applicable across the sector. DOI will ensure that there is crosscut among types of NMI assets to ensure maximum use of these specific measures and sharing of best practices;
- Measures will be best practices within the industry that properly weigh risk avoidance or mitigation against cost; and
- Measures will be identified within industry, the private sector, and other relevant entities planning guidance.

Security Plans

DOI will coordinate the structure and maintenance of security plans for DOI-owned NMI assets to ensure consistency and compatibility. Plans will address domain awareness, prevention, preparedness, response, and recovery efforts. DOI will provide guidance to stakeholders to encourage functional equivalency within the asset category and consistency with the National Response Plan (NRP) and the National Incident Management System (NIMS) when preparing plans.

- DOI will develop risk-based plans for its internal assets.
- DOI will conduct rigorous plan reviews for DOI-owned assets. For other National Critical assets, DOI will provide assistance to other Federal agencies in reviewing plans and recommendations for improvements. For assets categorized as National Significant, Regional Critical, and Local Significant, DOI will encourage certification within the framework of the program and work with DHS and the GCC to develop mechanisms for sharing information within the sector.
- A portion of the protection and mitigation measures for NMI assets are borne by owners outside of DOI and must be considered when developing programs. DOI will consider the use of conferences, symposiums, public forums, and stakeholder outreach when crafting programs.

Protection of Supporting Infrastructure

DOI will coordinate with DHS in protecting other infrastructure sectors that support NMI assets (e.g., cyber, power, and telecommunications) or are the responsibility of DHS or another sector. Based on guidance from DHS/NCSD, DOI will provide this information to NMI asset owners as part of its guidance on implementing protective programs for the sector.

SSA Relationships With State and Local Agencies

State and local authorities may be the first on the scene of an attack on an NMI asset. DOI will work closely with Federal officials and regional preparedness agencies in coordinating recovery efforts and restoring public confidence after an attack on a DOI-owned NMI asset. State and local authorities constitute the front line of defense for some of DOI's critical assets, and in some cases, are the owners or operators of a historic landmark. Public safety agencies such as law enforcement, fire/rescue, emergency medical services, and emergency management are an integral part of prevention, mitigation, response, and recovery.

Resource Management

To effectively coordinate actions to prevent, deter, and mitigate attacks on an NMI asset, awareness of the security resources available across the Federal, State, and local governments; Territories; and private sector jurisdictions is critical. Developed under the requirements of HSPD-5, the NRP outlines the mechanisms for resource sharing at the Federal, State, and local levels. These mechanisms include memoranda of agreement, mutual aid agreements, mutual aid pacts, and similar protocols. Federal resources can be deployed to temporarily provide protection to critical national infrastructure. During high threat conditions, DOI and DHS may coordinate deployment.

Response Preparedness

Preparedness encompasses actions taken before a terrorist attack or all-hazards incident occurs and includes prestaging resources, exercising with first responders, and planning for restoration of NMI assets. Response preparedness also presumes that despite best efforts, an attack or all-hazards incident may still occur. DOI will coordinate efforts with multiple jurisdictions as necessary, including Federal, State, and local stakeholders; nongovernmental organizations; and the private sector if an attack

or all-hazards incident occurs at a DOI-owned asset. In addition, DOI will work with the FBI and other law enforcement agencies to investigate the cause of the incident, protect any evidence, and use the information to improve prevention measures.

Response Plans

DOI will use NIMS to manage a response to an attack in accordance with HSPD-5. NIMS will provide unity of command, a manageable span of control, the use of common terminology, and a scalable management structure to mitigate the immediate effects of an attack. If an incident occurs, DOI will coordinate with the Principal Federal Official with incident response. DOI will also conduct an investigation of the event to identify areas where response preparedness and prevention standards could be strengthened.

Cyber Security Considerations

The February 2003 presidential report *National Strategy to Secure Cyberspace* provides DOI with a framework for approaching cyber security for the NMI Sector. IT and telecommunication networks directly support the operation of all sectors of our economy—energy (electric power, oil, gas), transportation (highway, rail, air, merchant marine), finance and banking, information and communications, public health, emergency services, water, chemicals, defense industrial base, food and agriculture, and postal and shipping services.

The cyber threat has been identified as a potential attack scenario. IT and telecommunication systems are important to the operations of a limited number of NMI assets, and an attack on those systems could affect the availability, function, or mission of an asset.

DOI will consider the following principles for protecting IT and telecommunication systems, whether used operationally or for physical security:

- Reduce cyber threats and deter malicious actors through effective programs to identify and punish them;
- Identify and address those existing vulnerabilities that could create the most damage to critical systems if exploited;
- Develop new systems with less vulnerability and assess emerging technologies for vulnerabilities; and
- Initiate workforce surety measures through implementation of a standard identity credential for secure and reliable identification and authentication of Federal Government employees and contractors as specified in Federal Information Processing Standards (FIPS) Publication 201 and its supporting authorities.

The implementation of these principles into the protection program will include four major actions:

- Enhance cyber security awareness training programs;
- Reduce cyber vulnerabilities;
- Respond to cyber security threats; and
- Establish NMI cyber security working groups.

5.4 Protective Program Performance

DOI will assess protective programs at DOI-owned assets on a continual basis, and formal reassessments of National Critical NMI assets will be conducted on a biannual basis.

DOI will assist the owners and operators of non-DOI-owned assets in periodically assessing the protective posture at their assets and making recommendations for measures that can be implemented to counter emerging threats.

6. Measure Progress

6.1 CI/KR Performance Measurement

The NMI Sector's CI/KR protection activities will support the achievement of overall CI/KR protection goals and the primary sector goal of ensuring that those National Critical NMI assets remain intact and accessible to the public at all times (or at least not closed for security reasons). DOI will use these goals as the standard to measure progress and will direct resources toward those activities that best support accomplishing the goals. Activities that do not advance the goals will be redesigned or eliminated over time. The goals will continue to evolve as the sector matures.

CI/KR protection metrics have been subdivided into the following two categories: core CI/KR protection metrics and CI/KR protection metrics that are sector specific. Core metrics will be tracked across each sector to enable comparison and analysis between different types of critical infrastructure.

NMI metrics will be more focused on monitoring progress within the sector. The metrics discussed below are expected to evolve as DHS and sector stakeholders become more aware of their specific CI/KR protection challenges.

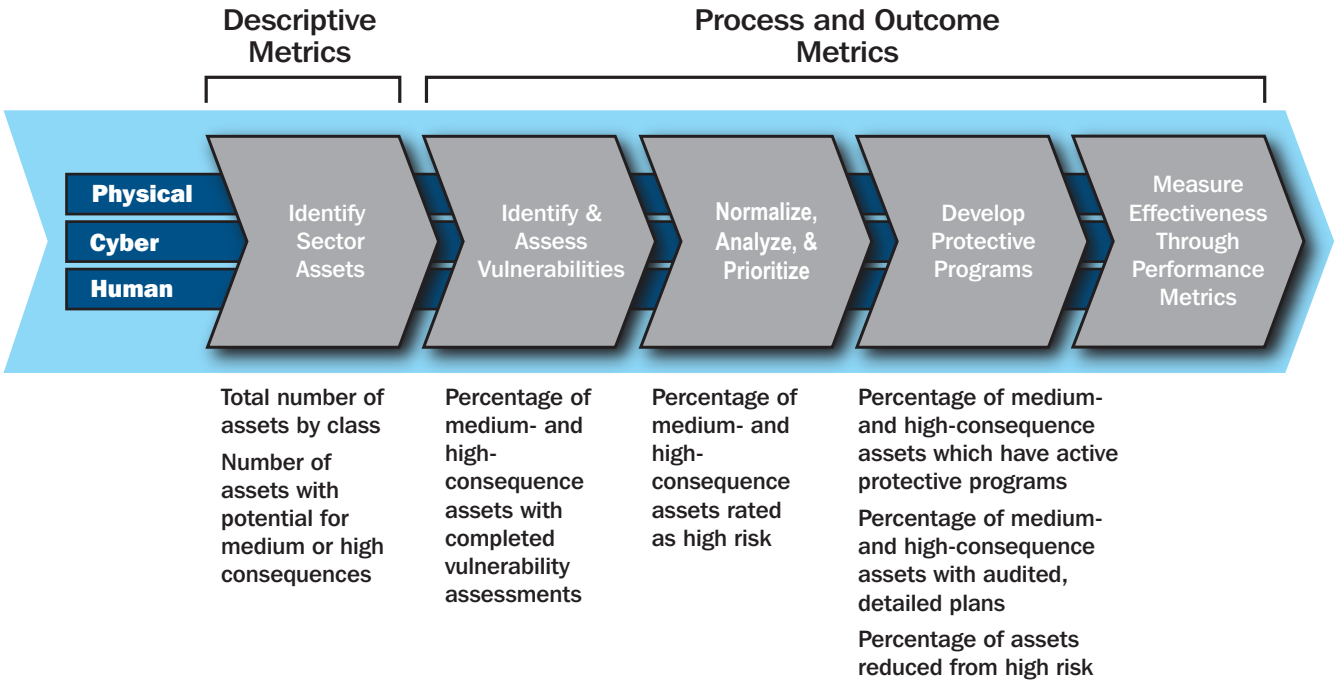
DOI will track three types of metrics to ensure that program goals are being met: descriptive metrics, process metrics, and outcome metrics.

- **Descriptive metrics** are necessary to understand sector resources and activity but do not reflect CI/KR protection performance. For instance, a typical descriptive measure would identify how many assets there are by tier or the number of assets with high or medium consequence value.
- **Process (i.e., output) metrics** measure whether specific activities were performed as planned, track the progression of a task, or report on the output of a process such as creating an inventory of assets. Examples of process metrics include the percentage of medium- and high-consequence assets with completed VAs. Process metrics have an important role, showing progress made in performing the activities necessary to achieve the goals of the CI/KR protection program. Process metrics build a comprehensive picture of CI/KR protection status and activities.
- **Outcome metrics** track progress toward a strategic goal in terms of beneficial results rather than level of activity. An example of an outcome metric may be the change in number of medium- and high-consequence assets rated as "high" risk. Outcome metrics are the most valuable because they indicate progress toward specific objectives. As the NIPP matures, process metrics will be deemphasized in favor of outcome metrics.

6.1.1 Developing Sector-Specific Metrics

Core CI/KR protection metrics are a set of seven descriptive, process, and outcome metrics used to measure initial progress in the implementation of the NMI SSP. Core metrics will be common across all sectors and are aligned with the key steps in the NIPP risk management framework, as illustrated in figure 6-1.

Figure 6-1: Alignment of Metrics to NIPP Risk Management Framework



The metrics do not specifically address cyber components of NMI assets because they are integral to the VAs and protective programs and are not separate assets themselves. If cyber issues become a significant factor for the NMI Sector, then appropriate metrics will be added. The core metrics for the NMI Sector are listed in table 6-1.

Table 6-1: NMI Sector Core Metrics

Type of Metric	Metric	Description
Descriptive	1. Total number of assets by tier.	Assessed for each asset tier and category of monument and icon by DOI, in conjunction with the GCC and SCC.
Descriptive	2. Number of assets with medium or high consequence values.	Assessed for National Critical assets as identified by DOI, in conjunction with the GCC and SCC. This metric will help determine what assets are in the most need of assessing vulnerabilities and if there are particularly critical ones. The identification of medium- and high-consequence assets is called for in section 2.
Process	3. Percentage of medium- and high-consequence assets with completed VAs.	Assessed for National Critical assets as identified by DOI. This measure will help determine progress against VA goals.
Outcome	4. Percentage of medium- and high-consequence assets rated as high risk.	Assessed for National Critical assets as identified by DOI. Tracking this metric will help determine which sector programs require increase protection. It can help focus government and private sector resources on those sectors, regions, and industries with the highest identified risks. This is called for in section 3.
Process	5. Percentage of medium- and high-consequence assets that have active protective programs to measurably reduce risk.	Assessed for National Critical assets. This metric, in conjunction with other measures, will help determine where there are potential gaps in program coverage for critical infrastructure assets determined to be high risk.
Process	6. Percentage of medium- and high-consequence assets that have been assessed for readiness, response, and recovery capability.	Metrics should be applied to National Critical assets as identified by DOI. This measure will provide insight into the degree to which readiness, response, and recovery planning are in place for the more important assets.
Outcome	7. Percentage of assets reduced from high risk.	Measures should be applied to all National Critical assets. This measure will provide insight into the effectiveness of the risk reduction programs, such as creating a better response and recovery capability, increasing the difficulty of attacking critical infrastructure assets, etc.

In addition to the core CI/KR protection metrics, the sector-specific metrics unique to the NMI Sector shown in table 6-2 will be part of the overall approach to performance management. These sector-specific metrics, together with the core CI/KR metrics, constitute the sector's approach to monitoring the performance of major processes and activities within the NMI Sector that are aimed at reducing risk.

Table 6-2: NMI Sector-Specific Metrics

Type of Metric	Metric	Description
Descriptive	1. Percentage of assets by tier that is fully accessible to the public and not closed or greatly restricted due to security concerns.	Assessed for National Critical assets and information collected by DOI, in conjunction with the GCC and SCC.
Descriptive	2. Attendance trends for NMI Sector sites (increasing, constant, or decreasing).	Assessed for National Critical assets. This metric will help determine which sites are experiencing changes to their customer base. Special large-scale events on national holidays may necessitate additional review.
Process	3. Percentage of medium- and high-consequence assets completed in accordance with their VA.	Assessed for National Critical assets as identified by DOI. Tracking this measure will help determine progress against protection system upgrades identified in the VAs.
Descriptive	4. Percentage of participation at NMI conferences, and SSP implementation.	Will allow some measure of success for reliability of data on location, ownership, and status of assets. It can help focus government and private sector resources on those NMI assets with the highest identified risks first.
Outcome	5. Percentage of medium- and high-consequence assets that have active protective programs to reduce risk and associated impacts when threat levels are increased.	In conjunction with other measures, will help determine where cost-effective changes are possible or whether the sector is meeting its primary goal of keeping the asset accessible to the public.

6.1.2 Information Collection and Verification

Because there are no existing processes for collecting this information, DOI will work closely with its sector partners through the GCC in the initial development and collection of metrics information.

For DOI-owned assets, the Department's Office of Law Enforcement, Security, and Emergency Management will work with the NPS and United States Park Police to collect the metrics information and verify its accuracy.

For non-DOI-owned Federal Government assets, DOI will work with the responsible Federal agency on collection and verification of the metric information.

For non-Federal Government-owned assets, DOI will work closely with the Government Facilities Sector SSA to collect and verify the needed information.

6.1.3 Reporting

DOI will update the information in both the core metrics and sector-specific metrics prior to the annual July 1 deadline for reporting sector CI/KR data as required by the NIPP. The information will be gathered internally, through the GCC and the Government Facilities Sector.

DOI will compile and report the information in accordance with DHS guidance.

6.2 Implementation Actions

The NIPP contains recommended implementation actions for security partners as well as other responsibilities and requirements dispersed throughout the base plan (see table 6-3). This SSP consolidates applicable actions and combines them with NMI sector-specific actions necessary to support sector initiatives, objectives, and goals.

Table 6-3: NIPP Implementation Actions

NIPP Implementation Actions for the NMI Sector SSA	Date
No Later Than 90 Days After NIPP Approval Review NIPP and establish processes needed to support implementation. Establish NMI Sector GCC. Identify sector-level information-sharing mechanisms and ensure that information protection practices comply with appropriate guidance for protection of classified or sensitive information. Provide initial NIPP awareness training to security partners.	9/30/06
No Later Than 180 Days After NIPP Approval Incorporate NIPP into strategies for cooperation with foreign countries and organizations. Develop sector-specific CI/KR inventory guidance. Review existing methodologies for risk assessment for compatibility with NIPP criteria. Establish timeline for developing sector-specific risk methodologies and conducting consequence-based top screening for assets. Coordinate SSP development in collaboration with security partners and submit to DHS with appropriate documentation of concurrence. Review and revise CI/KR-related plans as needed to reinforce linkage between NIPP steady-state CI/KR protection and NRP incident management requirements. Review current CI/KR protection measures to ensure alignment with Homeland Security Advisory System (HSAS) threat conditions and specific threat vectors and scenarios. Develop and implement a comprehensive national CI/KR protection awareness program. Review and revise, as appropriate, training programs to ensure consistency with NIPP requirements. Advise State, local, and tribal governments of SSA grant programs or other sources that can support the NIPP.	12/31/06
No Later Than 365 Days After NIPP Approval Conduct and validate, or facilitate, consequence assessments of priority CI/KR as identified by the top screening process. Conduct or facilitate VAs for priority CI/KR and identify cross-sector vulnerabilities. Conduct the first annual review of the NIPP and SSP.	6/30/07
Annually on a Specific Date Communicate requirements for CI/KR-related R&D to DHS for use in the national R&D planning effort. Submit sector's annual report on CI/KR protection to DHS.	7/1 (Annually)

The activities described within the SSP implementation plan also provide a means to measure progress toward sector goals. Each of the actions detailed within the implementation plan is benchmarked to a specific period of time following the SSP release. This ensures that security partners establish the necessary protocols to implement the NMI SSP and enables the SSA to measure progress toward SSP implementation. The SSP implementation plan also provides a means for security partners to translate the strategic goals and processes outlined in the SSP into specific activities that can be carried out at the tactical level.

6.3 Challenges and Continuous Improvement

As stated previously, DOI has no regulatory authority over non-DOI assets within the NMI Sector. In addition, since all National Critical assets within the sector are federally owned, the only funding source available is the Federal budget process. In many instances, this results in a situation in which funding for security needs competes with other departmental program priorities. Federal managers must then determine the cost-benefit ratio of implementing a security measure versus the amount of risk associated with not expending those funds. If the risk is determined to be acceptable, in many cases the funding will be used for non-security-related priorities.

Significant progress has been made within this sector since 9/11. In many cases, agencies had appropriated funds specifically targeted to CI/KR protection, resulting in a more robust security posture at NMI Sector assets.

The sector now faces the challenges of maintaining this level of security, continuing to justify the need for additional funding for improvements, and developing strategies and protective measures to deal with emerging threats.

The metrics described previously in this section will help determine where funding should be focused to achieve measurable and justifiable improvements.

7. CI/KR Protection R&D

7.1 Overview of Sector R&D

Federal R&D planning for CI/KR protection is based on the NIPP and HSPD-7, which state the following:

"In coordination with the Director of the Office of Science and Technology Policy, the Secretary shall prepare, on an annual basis, a Federal Research and Development Plan in support of this directive."

In addition to the NIPP, HSPD-7 establishes an annual requirement for the National Critical Infrastructure Protection Research and Development Plan (NCI/KR R&D Plan). As the primary R&D arm of DHS, S&T supports the Secretary of Homeland Security by preparing the annual NCI/KR R&D Plan in partnership with the Executive Office of the President's OSTP. The long-term vision of the NCI/KR R&D Plan is set out in three strategic goals:

- A national, common operating picture for critical infrastructures;
- A next-generation Internet architecture with "designed-in" security inherent in all elements rather than added after the fact; and
- Resilient, self-diagnosing, and self-healing physical and cyber infrastructure systems.

HSPD-7 also instructs OSTP and DHS to coordinate interagency R&D to enhance the protection of CI/KR. Planning needs to be collaborative so cross-sector priorities can be identified and R&D solutions developed to meet the needs of a specific infrastructure sector can be made available to all sectors. To assist the agencies and sector industries in coordinating their R&D, S&T and OSTP organized the NCI/KR R&D Plan into nine research theme areas:

- Detection and Sensor Systems;
- Protection;
- Entry Portals;
- Insider Threats;
- Analysis and Decision-Support Methods;
- Response, Recovery, and Reconstitution;
- New and Emerging Threats and Vulnerabilities;
- Advanced Infrastructure Architectures and System Designs; and
- Human/Social Issues.

Each theme area includes both physical and cyber R&D, and each theme area supports the three NCI/KR R&D strategic goals.

7.2 Sector R&D Requirements

Assets included in the NMI Sector offer challenges to effective security enhancement due to a number of factors, such as the need to maintain public access, recognition, and significant visitation. Emerging technologies may offer benefits for enhancing the security of these assets.

However, due to continuing concern over terrorist activity, ongoing advancements in technologies to reduce vulnerabilities to terrorism, and continuing need for enhanced protection equipment, commercial off-the-shelf (COTS) security equipment solutions may not be enough. DOI will work with DHS, OSTP, and the GCC to stay ahead of the multivariate threats to NMI assets and the complex and interdependent systems, subsystems, and components of the infrastructure that support them. Total solutions to this multifaceted problem will include conventional security measures, COTS, and emerging technologies.

The primary technology requirements of the NMI Sector are for unobtrusive security technologies that maintain the aesthetic qualities of the assets while allowing enhanced security when required. These could include any of the following:

- Technologies for maintaining a controlled perimeter;
- New techniques for visitor screening to maintain accessibility for the anticipated number of visitors and unobtrusive surveillance techniques, including biometric technology applications for access and control;
- Unobtrusive internal and external security technologies (e.g., buried lines, seismic pressure sensors, magnetic sensors, electric field sensors, coaxial cable, passive infrared technology, chemical/biological/radiological sensors, face recognition technology) that meet the physical security objectives of the protection program strategies; and
- Research projects that develop unobtrusive physical security technologies, architecture that enhances security through environmental design, and studies that provide innovative ways to protect NMI assets.

7.2.1 Physical Protection R&D

Physical protection R&D projects are needed to develop standardized methodologies and decision aids for VAs as well as to introduce new approaches for protecting elements critical to assets and infrastructure. These elements include the asset and control centers, power generation and transmission systems, and transportation and communication systems. By understanding the dynamics of support systems, asset managers will be able to develop secure operating methodologies and strategies to prevent or mitigate security issues. DOI will evaluate and incorporate R&D of new technologies into the implementation of new equipment and the development of common standards and best practices.

7.2.2 Cyber Security R&D

Cyber security R&D projects are needed to focus on preventing or mitigating threats to computer networks and are an important aspect of the operation and safety of NMI assets. Modern systems increasingly rely on new technologies, computer networks, and the Internet to conduct business, manage operational activities, engage in communications, and perform other daily functions. The complexity and sophistication of information technologies and widespread integration in other infrastructures increase the likelihood of vulnerabilities, creating opportunities for criminals, terrorists, and hostile foreign agents to invade information systems or cause vital infrastructure elements to cease operations. This research will provide detection, prevention, response, and alert capabilities to counter such attacks and harden computer systems.

7.3 Sector R&D Plan

There are currently no known R&D initiatives specific to the NMI Sector. The DOI liaison from the NMI Sector will confer with S&T/OSTP on a periodic basis to identify current Federal R&D initiatives that may be applicable to the sector. DOI will share this information with sector stakeholders through the GCC to gather input relative to those initiatives of most value to the sector.

7.4 R&D Management Processes

The DOI liaison from the NMI Sector will confer with S&T/OSTP to conduct a gap analysis between current R&D initiatives and those deemed necessary for the sector. DOI also will solicit input from NMI Sector stakeholders through the Department's information-sharing Web site to identify R&D needs.

8. Manage and Coordinate SSA Responsibilities

8.1 Program Management Approach

As the SSA for the NMI Sector, DOI has been unable to create a separate program office to manage NIPP-related responsibilities due to limitations on staffing and funding.

Within DOI, the SSA responsibility will be delegated to a Special Agent assigned in the Security Division of the Office of Law Enforcement, Security, and Emergency Management. When necessary, the Assistant Director of the Security Division will assist the Special Agent. As appropriate and necessary, they will work closely with other personnel assigned primarily with the NPS and the U.S. Park Police, which are the two agencies within DOI with primary responsibility for NMI assets.

8.2 Processes and Responsibilities

8.2.1 SSP Maintenance and Update

As the SSA, DOI will work with the GCC to determine when a change within the sector warrants updating the SSP. In addition, while compiling the annual report with the GCC partners, DOI will highlight any outstanding issues that may warrant changes. DOI will discuss proposed changes with all GCC partners and seek their concurrence prior to implementation.

DOI will review the SSP and update it triennially in conjunction with the review of the NIPP Base Plan in coordination with DHS.

8.2.2 Annual Reporting

Upon receipt of the annual guidance from DHS, DOI will initiate a call for data from all assets within the sector. Once the information is received, DOI will develop a draft report. All GCC partners then will have the opportunity to review the draft and provide comments.

8.2.3 Resources and Budgets

Currently all assets identified within the NMI Sector are federally owned. Therefore, each department or agency within the sector will manage its own budget through the Federal budget process. The sector can play a role in obtaining additional resources by identifying gaps in the agencies' budgets within the NMI annual report. This practice may assist agencies in their attempts to obtain additional resources through the Office of Management and Budget. As the SSA, DOI will not interfere with the internal budgeting processes of other Federal agencies but will attempt to advocate for them through the annual report.

Because the assets within the sector are all federally owned, they are ineligible for grants distributed through DHS. They can, however, benefit indirectly through training and exercises that DHS funds for State and local agencies.

8.2.4 Training and Education

Successful implementation of the national risk management framework relies on building and maintaining individual and organizational expertise in CI/KR protection. Training and education at a variety of levels and in a variety of subject areas are necessary to achieve and sustain an optimal level of expertise. Section 6.2 of the NIPP Base Plan discusses some of the areas of expertise where training is recommended, as well as examples of the types of training currently being offered and other general information on training and education related to CI/KR protection.

Individual and organizational training as well as tabletop exercises are integral to improving the NMI Sector's overall security posture. Training facility staff on how to identify suspicious activity could dramatically reduce the likelihood of a terrorist attack. Red-team exercises that test an asset's security measures using teams of trained adversaries can help gauge the effectiveness of an asset's security program and prepare staff to respond efficiently in the event of an actual incident. Tabletop exercises can also be used to measure an asset's state of readiness for an actual attack.

DOI will encourage NMI sector partners to participate in security-related training and educational opportunities. In addition, DOI will work with its partners to identify security-related training and educational opportunities.

8.3 Implementing the Sector Partnership Model

8.3.1 NIPP Coordinating Councils

The Sector Partnership Model is the framework proposed in the NIPP Base Plan to promote and facilitate sector and cross-sector planning, coordination, collaboration, and information sharing for CI/KR protection involving all levels of government and the private sector. The model encourages formation of GCCs to harmonize government efforts and SCCs to coordinate private sector efforts. DHS provides guidance, tools, and support to enable the councils to carry out their respective roles and responsibilities. The goals of the councils are to establish the context, framework, and support for activities required to implement and sustain the national CI/KR protection effort.

8.3.2 NMI Sector SCC

The NMI Sector has partnered with the Government Facilities Sector to coordinate outreach to State, local, and tribal entities through its SCC.

8.3.3 NMI Sector GCC

The NMI Sector GCC provides an effective mechanism for coordinating CI/KR strategies and activities, policy, and communication across the government and between the government and the NMI Sector to support the Nation's homeland security mission.

The GCC will accomplish its objectives through the following activities:

- Identifying issues that require government coordination and communication. The GCC brings together diverse Federal and State interests to identify and develop collaborative strategies that advance critical infrastructure protection.
- Identifying needs and gaps in plans, programs, policies, procedures, and strategies.
- Acknowledging successful programs and practices. The GCC will facilitate the sharing of experiences, ideas, effective practices, and innovative approaches related to protecting critical infrastructure.
- Leveraging complementary resources within government and between government and industry.

The GCC meets quarterly or more frequently if required. The members of the NMI Sector GCC are representatives from the following agencies:

- U.S. Department of the Interior:
  - Office of Law Enforcement, Security, and Emergency Management;
  - National Park Service; and
  - United States Park Police;
- Department of Homeland Security:
  - Office of Infrastructure Protection;
  - Federal Protective Service; and
  - United States Secret Service;
- Department of Justice:
  - Federal Bureau of Investigation;
- Smithsonian Institution;
- National Archives and Records Administration;
- United States Capitol Police; and
- Department of Defense.

8.4 Joint GCC-SCC Activities

The NMI Sector has partnered with the Government Facilities Sector's SCC to provide outreach to State, local, and tribal entities. Information sharing with the NMI Sector GCC and from this body to the Government Facilities Sector's SCC will be facilitated through quarterly meetings and electronic message exchanges.

8.5 Information Sharing and Protection

The lack of historical interactions within this sector, except for those assets owned by DOI, highlights the need for a structured method to disseminate information within the sector in a timely manner. This is a critical gap that needs to be addressed quickly across the entire sector.

Most sector assets rely on the information-sharing processes that the responsible law enforcement or security entity has in place. For critical operational information, the procedures currently in place within the law enforcement community should continue to be utilized and improved. The Critical Infrastructure Warning Information Network should be utilized as applicable. For sector-specific information of a less critical nature, the Homeland Security Information Network (HSIN) system should be used.

The NMI Sector developed its own HSIN portal to enable sector partners to share information quickly concerning threats and potential protective measures that have been used successfully. A key component of this information system will be the ability of DHS's HITRAC to quickly disseminate developing threat information or evolving patterns of attack to all NMI Sector partners.

The information used by the NMI Sector and its security partners to manage risk and secure CI/KR may contain sensitive data as well as proprietary or sensitive business information. As a result, information protection is a significant concern for those partners who are supplying this sensitive information. The NMI Sector will protect this information to the maximum extent possible.

Pursuant to the Critical Infrastructure Information Act of 2002, information that satisfies the requirements of the Act will be protected from public disclosure to the maximum extent permitted by law. The PCII Program managed by DHS is an outgrowth of the Act. The rules governing the PCII Program are available at 6 CFR Part 29.

Appendix 1: List of Acronyms and Abbreviations

BOR	Bureau of Reclamation
C&A	Certification and Accreditation
CFR	Code of Federal Regulations
CI/KR	Critical Infrastructure and Key Resources
CIO	Chief Information Officer
COTS	Commercial Off-the-Shelf
DHS	Department of Homeland Security
DOD	Department of Defense
DOI	Department of the Interior
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GCC	Government Coordinating Council
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HSIN	Homeland Security Information Network
HSPD-7	Homeland Security Presidential Directive 7
IED	Improvised Explosive Device
IT	Information Technology
NADB	National Asset Database
NARA	National Archives and Records Administration
NCSD	National Cyber Security Division
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NMI	National Monuments and Icons
NPS	National Park Service
NRP	National Response Plan
NSSE	National Special Security Event
OSTP	Office of Science and Technology Policy
PCII	Protected Critical Infrastructure Information
PSA	Protective Security Advisor
R&D	Research and Development
S&T	Science and Technology
SBU	Sensitive But Unclassified
SCC	Sector Coordinating Council
SSA	Sector-Specific Agency
SSP	Sector-Specific Plan
USSS	United States Secret Service
VA	Vulnerability Assessment
VBIED	Vehicle-Borne Improvised Explosive Device

Appendix 2: Authorities

The assets currently identified as falling within the National Monuments and Icons (NMI) Sector are all federally owned. These include a number of monuments and memorials under the jurisdiction of the National Park Service (NPS), a number of Smithsonian Institution buildings, and the National Archives and Records Administration (NARA) building, includeing many of its contents. Most of these assets have their own dedicated law enforcement or security forces on site, but many rely on State or local law enforcement agencies to respond and provide support during special events or large incidents. It is imperative that the asset managers have agreements in place, preferably written, detailing the assistance available and the mechanics of how the assistance will flow in a smooth and orderly manner.

The U.S. Department of the Interior (DOI), as the Sector-Specific Agency (SSA), has no statutory or regulatory authority for collecting and sharing asset information (except for those assets under the NPS), completing vulnerability and risk assessments, or implementing protective programs. DOI must work with the asset owners, some of whom already have working relationships with bureaus within DOI, to gain voluntary compliance and cooperation.

The following specific authorities apply to the various partners of the NMI Sector:

- **DOI**
  - **Antiquities Act of 1906:** Congress passed the Antiquities Act of 1906, which authorized the President "to declare by public proclamation (as national monuments) historic landmarks, historic and prehistoric structures, and other objects of historic or scientific interest" (16 U.S.C. 431). The act also stated that any person who shall appropriate, excavate, injure, or destroy any historic monument without the permission of the Secretary of the Interior is in violation of Federal law.
  - **16 U.S.C. 1, National Park Service Organic Act:** In 1916, Congress created the NPS within DOI to "promote and regulate the use of the Federal areas known as national parks, monuments, and reservations." The interrelated provisions of the NPS Organic Act of 1916 established the NPS under DOI and the NPS General Authorities Act of 1970, including amendments to the latter law enacted in 1978 that reiterated the provisions of the Organic Act. The congressional report accompanying the 1978 amendment (Redwood Amendment) stated, "The Secretary has an absolute duty, which is not to be compromised, to fulfill the mandate of the 1916 Act to take whatever actions and seek whatever relief as will safeguard the units of the national park system."
  - **16 U.S.C. 1a-6, General Authorities Act of 1970 (Public Law 91-383, as amended by Public Law 94-458):** The Act stated the following: (a) The Secretary of the Interior (SOI) is authorized to designate, pursuant to standards prescribed in regulations by the Secretary, certain officer or employees of DOI who shall maintain law and order and protect persons and property within areas of the NPS. (b) SOI is hereby authorized to (1) "designate officers and employees of any other Federal agency or law enforcement personnel of any State or political subdivision thereof, when deemed economical and in the public interest and with the concurrence of that agency or that State or subdivision, to act as special policemen in areas [of

the National Park Service] when supplemental law enforcement personnel may be needed" and to exercise the powers and authority provided by paragraphs (1), (2), and (3) of subsection (a) of this section. On October 13, 1976, pursuant to 16 U.S.C. 1a-6(b), the Director of the NPS designated "all United States Park Police officers" to maintain law and order and protect persons and property within areas of the National Park System," as published in the Federal Register (41 FR 44876).

- **16 U.S.C. 1a-6, 43 U.S.C. 1733, 16 U.S.C. 7421, DOI Cross-Designation Agreements-Interagency Agreement:** "Pursuant to ... Titles 16 U.S.C. 1a-6, 43 U.S.C. 1733, 16 U.S.C. 7421(b), 25 U.S.C. Chapter 30 ... it has been determined by all parties that the cross-designation of law enforcement officers...[may be] mutually beneficial, economical, and advantageous to the public interest."
- **36 CFR 2.32:** 36 CFR 2.32 (a) (2) provides that authorized park employees may assert a lawful order to close or limit public access to park areas during law enforcement actions and emergency operations that involve a threat to public safety or park resources, or where the control of public movement and activities is necessary to maintain order and public safety.
- **16 U.S.C. 461, National Historic Sites Act of 1935:** This act declared it national policy to preserve for public use historic sites, buildings, and objects of national significance for the inspiration and benefit of the people of the United States. The regulation sets forth the criteria for establishing national significance and the procedures used by DOI for conducting the National Historic Landmarks Program.
- **16 U.S.C. 470, National Historic Preservation Act of 1966:** This act requires the Secretary of the Interior to promulgate regulations for the following: (1) approving and overseeing State historic preservation programs, (2) certifying local governments to carry out the purposes of the act, (3) ensuring that applicable State Historic Preservation Officers allocate a share of grants received under the act to certified local governments, and (4) assisting Indian tribes in preserving their particular historic properties.

- **Smithsonian Institution**
  - **40 U.S.C. 6301-6307:** This section provides the Smithsonian Institution's Office of Protection Services the authority to police the buildings and grounds of the Smithsonian Institution.
- **FBI**
  - **28 U.S.C. 533:** This section grants the FBI its investigative authority.
  - **USA PATRIOT Act:** This act granted the FBI new provisions to address the threat of terrorism.
- **USSS**
  - **United States Secret Service:** USSS was established as a law enforcement agency in 1865. Although most people associate the Secret Service with Presidential protection, its original mandate was to investigate the counterfeiting of U.S. currency.
  - **18 U.S.C. 3056:** This authorizes agents and officers of the United States Secret Service to carry firearms; execute warrants issued under the laws of the United States; make arrests without warrants for any offense against the United States committed in their presence, or for any felony recognizable under the laws of the United States if they have reasonable grounds to believe that the person to be arrested has committed such felony; offer and pay rewards for services and information leading to the apprehension of persons involved in the violation of the law that the Secret Service is authorized to enforce; investigate fraud in connection with identification documents, fraudulent commerce, fictitious instruments and foreign securities; and perform other functions and duties authorized by law. The Secret Service works closely with the United States Attorney's Office in both protective and investigative matters.
  - **18 U.S.C. 871:** This authorizes the USSS to provide security for the President, the Vice President, (or other individuals next in order of succession to the Office of the President), the President-elect, and Vice President-elect; the immediate fami-

lies of the above individuals; former Presidents, their spouses for their lifetimes, except when the spouse remarries, and children of former presidents until age 16; visiting heads of foreign states or governments and their spouses traveling with them, other distinguished foreign visitors to the United States, and official representatives of the United States performing special missions abroad; and major Presidential and Vice Presidential candidates and their spouses within 120 days of a general Presidential election.

– **18 U.S.C. 1030:** This authorizes the USSS to safeguard the payment and financial systems of the United States. Historically, the USSS accomplished this through enforcement of the counterfeiting statutes to preserve the integrity of United States currency, coin, and financial obligations. Since 1984, the investigative responsibilities have expanded to include crimes that involve financial institution fraud, computer and telecommunications fraud, false identification documents, access device fraud, advance fee fraud, electronic funds transfers, and money laundering as it relates to USSS core violations.

Appendix 3: Minimum Security Requirements for DOI CI/KR Assets

Security Personnel	
Minimum Requirement	**Definition/Description**
Dedicated/trained onsite Security Manager	Specific protective measures provided to NMI partners
360-degree visual coverage	Specific protective measures provided to NMI partners
24-hour presence	Specific protective measures provided to NMI partners
Periodic roving patrols	Specific protective measures provided to NMI partners
Armed security force	Specific protective measures provided to NMI partners
Reliable 24-hour communication system	Specific protective measures provided to NMI partners
Access to Explosive Ordnance Detection (EOD) K-9 unit on a 24-hour basis	Specific protective measures provided to NMI partners

Perimeter Security	
Minimum Requirement	**Definition/Description**
Physical perimeter with barriers preventing unauthorized vehicular access	Specific protective measures provided to NMI partners
Identification system and procedures for authorized parking within the security perimeter	Specific protective measures provided to NMI partners
Posted "No Parking" signs and arrangements for towing unauthorized vehicles	Specific protective measures provided to NMI partners
Closed-circuit television (CCTV) surveillance cameras (360-degree coverage)	Specific protective measures provided to NMI partners
Monitoring the CCTV system on a 24-hour basis	Specific protective measures provided to NMI partners
External lighting with 360-degree coverage	Specific protective measures provided to NMI partners
Emergency lighting in critical areas	Specific protective measures provided to NMI partners
Lighting meets minimum standards for the CCTV system	Specific protective measures provided to NMI partners
Secure exterior utility systems and fuel sources	Specific protective measures provided to NMI partners

Access Control Security—Receiving/Shipping	
Minimum Requirement	**Definition/Description**
Review/Implement receiving/shipping procedures	Specific protective measures provided to NMI partners
Restrict delivery access area to authorized personnel/vehicles	Specific protective measures provided to NMI partners
Post or secure receiving/shipping areas	Specific protective measures provided to NMI partners
Screen, search, and/or x-ray all incoming packages	Specific protective measures provided to NMI partners
Provide security training for all mailroom personnel	Specific protective measures provided to NMI partners

Access Control Security—Entrance/Exit	
Minimum Requirement	**Definition/Description**
Armed security personnel located (posted) at all open access points	Specific protective measures provided to NMI partners
X-ray and magnetometer equipment at public entrances with trained operators	Specific protective measures provided to NMI partners
Required inspection of vehicles entering the facility	Specific protective measures provided to NMI partners
Intrusion detection system (IDs) with 24-hour central monitoring capability	Specific protective measures provided to NMI partners
IDs using line supervision and backup power	Specific protective measures provided to NMI partners
IDs covering all access points	Specific protective measures provided to NMI partners
HSPD-12-compliant card readers	Specific protective measures provided to NMI partners
Central database containing the location and serial numbers of all keys	Specific protective measures provided to NMI partners
High-security locks and secure door hinges	Specific protective measures provided to NMI partners

Interior Security	
Minimum Requirement	**Definition/Description**
Establish employee/contract employee identification authority	Specific protective measures provided to NMI partners
Agency photo ID for all employees displayed at all times	Specific protective measures provided to NMI partners
Visitor control system	Specific protective measures provided to NMI partners
Visitor identification accountability system	Specific protective measures provided to NMI partners
Secure interior utility areas	Specific protective measures provided to NMI partners
Emergency power for critical systems	Specific protective measures provided to NMI partners
Ability to close air intake system	Specific protective measures provided to NMI partners
Designated and trained occupant emergency plan official (refer to CFR 41-2.101-20.103.4)	Specific protective measures provided to NMI partners
Examine, update, and practice occupant emergency plans and contingency procedures once per year	Specific protective measures provided to NMI partners
Contacts for local police, fire department, HAZMAT teams, EOD team, etc.	Specific protective measures provided to NMI partners
All official computers in compliance with current DOJ security standards	Specific protective measures provided to NMI partners
Presence of a building emergency public address system	Specific protective measures provided to NMI partners
Established “shelter-in-place” plan	Specific protective measures provided to NMI partners

Security Planning	
Minimum Requirement	**Definition/Description**
Current law enforcement agency/security intelligence liaison contacts	Specific protective measures provided to NMI partners
Procedures in place for intelligence receipt/dissemination	Specific protective measures provided to NMI partners
Establish unusual facility incident reporting system	Specific protective measures provided to NMI partners
Conduct and document annual security awareness training for all employees	Specific protective measures provided to NMI partners
Standardized security force qualifications/training requirements	Specific protective measures provided to NMI partners
Implement/review construction projects for security enhancements	Specific protective measures provided to NMI partners
Establish employee access protocols	Specific protective measures provided to NMI partners
Establish security control procedures for service contract personnel	Specific protective measures provided to NMI partners

Homeland Security

Department of the Interior