EXECUTIVE SUMMARY

This document defines the road ahead for a core mission area identified in the President's *National Strategy for Homeland Security*—reducing the Nation's vulnerability to acts of terrorism by protecting our critical infrastructures and key assets from physical attack.

This document, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, the *Strategy*, identifies a clear set of national goals and objectives and outlines the guiding principles that will underpin our efforts to secure the infrastructures and assets vital to our national security, governance, public health and safety, economy, and public confidence. This *Strategy* also provides a unifying organization and identifies specific initiatives to drive our near-term national protection priorities and inform the resource allocation process. Most importantly, it establishes a foundation for building and fostering the cooperative environment in which government, industry, and private citizens can carry out their respective protection responsibilities more effectively and efficiently.

This *Strategy* recognizes the many important steps that public and private entities across the country have taken in response to the September 11, 2001, attacks to improve the security of their critical facilities, systems, and functions. Building upon these efforts, this document provides direction to the federal departments and agencies that have a role in critical infrastructure and key asset protection. It also suggests steps that state and local governments, private sector entities, and concerned citizens across America can take to enhance our collective infrastructure and asset security. In this light, this *Strategy* belongs and applies to the Nation as a whole, not just to the federal government or its constituent departments and agencies.

A New Mission

The September 11 attacks demonstrated our national-level physical vulnerability to the threat posed by a formidable enemy-focused, mass destruction terrorism. The events of that day also validated how determined, patient, and sophisticated—in both planning and execution—our terrorist enemies have become. The basic nature of our free society greatly enables terrorist operations and tactics, while, at the same time, hinders our ability to predict, prevent, or mitigate the effects of terrorist acts. Given these realities, it is imperative to develop a comprehensive national approach to physical protection.

Defining the End State: Strategic Objectives

The strategic objectives that underpin our national critical infrastructure and key asset protection effort include:

- Identifying and assuring the protection of those infrastructures and assets that we deem most critical in terms of national-level public health and safety, governance, economic and national security, and public confidence consequences;
- Providing timely warning and assuring the protection of those infrastructures and assets that face a specific, imminent threat; and
- Assuring the protection of other infrastructures and assets that may become terrorist targets over time by pursuing specific initiatives and enabling a collaborative environment in which federal, state, and local governments and the private sector can better protect the infrastructures and assets they control.

Homeland Security and Infrastructure Protection: A Shared Responsibility

Protecting America's critical infrastructures and key assets calls for a transition to a new national cooperative paradigm. The basic tenets of *homeland security* are fundamentally different from the historically defined tenets of national security. Traditionally, *national security* has been recognized largely as the responsibility of the federal government. *National security* is underpinned by the collective efforts of the military, foreign policy establishment, and intelligence community in the defense of our airspace and national borders, as well as operations overseas to protect our national interests.

Homeland security, particularly in the context of critical infrastructure and key asset protection, is a shared responsibility that cannot be accomplished by the federal government alone. It requires coordinated action on the part of federal, state, and local governments; the private sector; and concerned citizens across the country.[1]

THE CASE FOR ACTION

To build and implement a robust strategy to protect our critical infrastructures and key assets from further terrorist exploitation, we must understand the motivations of our enemies as well as their preferred tactics and targets. We must complement this understanding with a comprehensive assessment of the infrastructures and assets to be protected, their vulnerabilities, and the challenges associated with eliminating or mitigating those vulnerabilities—a task that will require the concerted efforts of our entire Nation.

The Importance of Critical Infrastructures

America's critical infrastructure sectors provide the foundation for our national security, governance, economic vitality, and way of life. Furthermore, their continued reliability, robustness, and resiliency create a sense of confidence and form an important part of our national identity and purpose. Critical infrastructures frame our daily lives and enable us to enjoy one of the highest overall standards of living in the world.

The facilities, systems, and functions that comprise our critical infrastructures are highly sophisticated and complex. They include human assets and physical and cyber systems that work together in processes that are highly interdependent. They also consist of key nodes that, in turn, are essential to the operation of the critical infrastructures in which they function.

The Importance of Key Assets

Key assets and high profile events are individual targets whose attack—in the worst-case scenarios—could result in not only large-scale human casualties and property destruction, but also profound damage to our national prestige, morale, and confidence.

Individually, key assets like nuclear power plants and dams may not be vital to the continuity of critical services at the national level. However, a successful strike against such targets may result in a significant loss of life and property in addition to long-term, adverse public health and safety consequences. Other key assets are symbolically equated with traditional American values and institutions or U.S. political and economic power. Our national icons, monuments, and historical attractions preserve history, honor achievements, and represent the natural grandeur of our country. They celebrate our American ideals and way of life and present attractive targets for terrorists, particularly when coupled with high profile events and celebratory activities that bring together significant numbers of people.

Understanding the Threat

Characteristics of Terrorism

The September 11 attacks on the World Trade Center and the Pentagon underscore the determination of our terrorist enemies. Terrorists are relentless and patient, as evidenced by their persistent targeting of the World Trade Center towers over the years. Terrorists are also opportunistic and flexible. They learn from experience and modify their tactics and targets to exploit perceived vulnerabilities and avoid observed strengths. As security increases around more predictable targets, they shift their focus to less protected assets. Enhancing countermeasures for any one terrorist tactic or target, therefore, makes it more likely that terrorists will favor another.

The Nature of Possible Attacks

Terrorists' pursuit of their long-term strategic objectives includes attacks on critical infrastructures and key assets. Terrorists target critical infrastructures to achieve three general types of effects:

- *Direct infrastructure effects:* Cascading disruption or arrest of the functions of critical infrastructures or key assets through direct attacks on a critical node, system, or function.
- *Indirect infrastructure effects:* Cascading disruption and financial consequences for government, society, and economy through public- and private-sector reactions to an attack.
- *Exploitation of infrastructure:* Exploitation of elements of a particular infrastructure to disrupt or destroy another target.

NATIONAL POLICY AND GUIDING PRINCIPLES

This *Strategy* reaffirms our longstanding national policy regarding critical infrastructure and key asset protection. It also delineates a set of guiding principles that will underpin our domestic protection strategy.

Statement of National Policy

As a Nation we remain committed to protecting our critical infrastructures and key assets from acts of terrorism that would:

- Impair the federal government's ability to perform essential national and homeland security missions and ensure the general public's health and safety;
- Undermine state and local government capacities to maintain order and to deliver minimum essential public services;

- Damage the private sector's capability to ensure the orderly functioning of the economy and the delivery of essential services; and
- Undermine the public's morale and confidence in our national economic and political institutions.

We must work collaboratively to employ the tools necessary to implement such protection.

Guiding Principles

Eight guiding principles underpin this *Strategy*:

- Assure public safety, public confidence, and services;
- Establish responsibility and accountability;
- Encourage and facilitate partnering among all levels of government and between government and industry;
- Encourage market solutions wherever possible and compensate for market failure with focused government intervention;
- Facilitate meaningful information sharing;
- Foster international cooperation;
- Develop technologies and expertise to combat terrorist threats; and
- Safeguard privacy and constitutional freedoms.

ORGANIZING AND PARTNERING FOR CRITICAL INFRASTRUCTURE AND KEY ASSET PROTECTION

Implementing this *Strategy* requires a unifying organization, a clear purpose, a common understanding of roles and responsibilities, accountability, and a set of well-understood coordinating processes. A solid organizational scheme sets the stage for effective engagement and interaction between the public and private sectors at all levels. Without it, the tasks of coordinating and integrating domestic protection policy, planning, resource allocation, performance measurement, and enabling initiatives across federal, state, and local governments and the private sector are virtually impossible to accomplish. Our strategy for action must provide the foundation these entities can use to achieve common objectives, applying their core capabilities, expertise, and experience as necessary to meet the threat at hand.

Federal Government Responsibilities

The federal government has the capacity to organize, convene, and coordinate broadly across governmental jurisdictions and the private sector. It has the responsibility to develop coherent national policies, strategies, and programs for implementation. In the context of homeland security, the federal government will coordinate the complementary efforts and capabilities of government and private institutions to raise our level of protection over the long term as appropriate for each of our critical infrastructures and key assets.

Every terrorist event has a potential national impact. The federal government will, therefore, take the lead to ensure that the three principal objectives detailed in the *Introduction* of this *Strategy* are met. This leadership role involves:

- Taking stock of our most critical facilities, systems, and functions and monitoring their preparedness across economic sectors and governmental jurisdictions;
- Assuring that federal, state, local, and private entities work together to protect critical facilities, systems, and functions that face an imminent threat and/or whose loss could have significant national consequences;
- Providing and coordinating national-level threat information, assessments, and warnings that are timely, actionable, and relevant to state, local, and private sector partners;
- Creating and implementing comprehensive, multi-tiered protection policies and programs;
- Exploring potential options for enablers and incentives to encourage stakeholders to devise solutions to their unique protection impediments;
- Developing cross-sector and cross-jurisdictional protection standards, guidelines, criteria, and protocols;
- Facilitating the sharing of critical infrastructure and key asset protection best practices and processes and vulnerability assessment methodologies;
- Conducting demonstration projects and pilot programs;
- Seeding the development and transfer of advanced technologies while taking advantage of private-sector expertise and competencies;
- Promoting national-level critical infrastructure and key asset protection education and awareness; and
- Improving the federal government's ability to work with state and local responders and service providers.

Federal Lead Departments and Agencies

The *National Strategy for Homeland Security* provides a sector-based organizational scheme for protecting critical infrastructure and key assets. It identifies the federal lead departments and agencies responsible for coordinating protection activities and developing and maintaining collaborative relationships with their state and local government and industry counterparts in the critical sectors.

In addition to securing federally owned and operated infrastructures and assets, the role of the federal lead departments and agencies is to assist state and local governments and private-sector partners in their efforts to:

- Organize and conduct protection and continuity of government and operations planning, and elevate awareness and understanding of threats and vulnerabilities to their critical facilities, systems, and functions;
- Identify and promote effective sector-specific protection practices and methodologies; and
- Expand voluntary security-related information sharing among private entities within the sector, as well as between government and private entities.

Department of Homeland Security

The Department of Homeland Security (DHS) will provide overall cross-sector coordination in this new organizational scheme, serving as the primary liaison and facilitator for cooperation among federal agencies, state and local governments, and the private sector. As the cross-sector coordinator, DHS will also be responsible for the detailed refinement and implementation of the core elements of this *Strategy*.

Other Federal Departments and Agencies

Besides the designated federal lead departments and agencies, the federal government will rely on the unique expertise of other departments and agencies to enhance the physical protection dimension of homeland security. Additionally, overall sector initiatives will often include an international component or requirement, require the development of a coordinated relationship with other governments or agencies, and entail information sharing with foreign governments. Accordingly, the Department of State (DoS) will support the development and implementation of sector protection initiatives by laying the groundwork for bilateral and multilateral infrastructure protective agreements with our international allies.

State and Local Government Responsibilities

The 50 states, 4 territories, and 87,000 local jurisdictions that comprise this Nation have an important and unique role to play in the protection of our critical infrastructures and key assets. State and local governments, like the federal government, should identify and secure the critical infrastructures and key assets they own and operate within their jurisdictions.

States should also engender coordination of protective and emergency response activities and resource support among local jurisdictions and regions in close collaboration with designated federal lead departments and agencies. States should further facilitate coordinated planning and preparedness for critical infrastructure and key asset protection, applying unified criteria for determining criticality, prioritizing protection investments, and exercising preparedness within their jurisdictions. States should also act as conduits for requests for federal assistance when the threat at hand exceeds the capabilities of local jurisdictions and private entities within those jurisdictions. Finally, states should facilitate the exchange of relevant security information and threat alerts down to the local level.

State and local governments look to the federal government for coordination, support, and resources when national requirements exceed local capabilities. Protecting critical infrastructures and key assets will require a close and extensive cooperation among all three levels of government. DHS, in particular, is designed to provide a single point of coordination with state and local governments for homeland security issues, including the critical infrastructure and key asset protection mission area. Other federal lead departments and agencies and law enforcement organizations will provide support as needed and appropriate for specific critical infrastructure and key asset protection requirements.

Private Sector Responsibilities

The lion's share of our critical infrastructures and key assets are owned and operated by the private sector. Customarily, private sector firms prudently engage in risk management planning and invest in security as a necessary function of business operations and customer confidence. Moreover, in the present threat environment, the private sector generally remains the first line of defense for its own facilities. Consequently, private-sector owners and operators should reassess and adjust their planning, assurance, and investment programs to better accommodate the increased risk presented by deliberate acts of violence. Since the events of

September 11, many businesses have increased their threshold investments and undertaken enhancements in security in an effort to meet the demands of the new threat environment.

For most enterprises, the level of investment in security reflects implicit risk-versus-consequence tradeoffs, which are based on: (1) what is known about the risk environment; and (2) what is economically justifiable and sustainable in a competitive marketplace or in an environment of limited government resources. Given the dynamic nature of the terrorist threat and the severity of the consequences associated with many potential attack scenarios, the private sector naturally looks to the government for better information to help make its crucial security investment decisions.

Similarly, the private sector looks to the government for assistance when the threat at hand exceeds an enterprise's capability to protect itself beyond a reasonable level of additional investment. In this light, the federal government will collaborate with the private sector (and state and local governments) to assure the protection of nationally critical infrastructures and assets; provide timely warning and assure the protection of infrastructures and assets that face a specific, imminent threat; and promote an environment in which the private sector can better carry out its specific protection responsibilities.

Near-term Roadmap: Cross-Sector Security Priorities

The issues and security initiatives outlined in the *Cross-Sector Security Priorities* chapter of this document represent important, near-term national priorities. They are focused on impediments to physical protection that significantly impact multiple sectors of our government, society, and economy. Potential solutions to the problems identified—such as information sharing and threat indications and warning—are high-leverage areas that, when realized, will enhance the Nation's collective ability to protect critical infrastructures and key assets across the board. Accordingly, DHS and designated federal lead departments and agencies will prepare detailed implementation plans to support the activities outlined in this chapter.

This *Strategy* identifies major cross-sector initiatives in five areas:

Planning and Resource Allocation: This *Strategy* identifies eight major initiatives in this area.

- Create collaborative mechanisms for government-industry critical infrastructure and key asset protection planning;
- Identify key protection priorities and develop appropriate supporting mechanisms for these priorities;
- Foster increased sharing of risk-management expertise between the public and private sectors;
- Identify options for incentives for private organizations that proactively implement enhanced security measures;
- Coordinate and consolidate federal and state protection plans;
- Establish a task force to review legal impediments to reconstitution and recovery in the aftermath of an attack against a critical infrastructure or key asset;
- Develop an integrated critical infrastructure and key asset geospatial database; and
- Conduct critical infrastructure protection planning with our international partners.

Information Sharing and Indications and Warnings: This *Strategy* identifies six major initiatives in this area.

- Define protection-related information sharing requirements and establish effective, efficient information sharing processes;
- Implement the statutory authorities and powers of the *Homeland Security Act of 2002* to protect security and proprietary information regarded as sensitive by the private sector;
- Promote the development and operation of critical sector Information Sharing Analysis Centers;
- Improve processes for domestic threat data collection, analysis, and dissemination to state and local government and private industry;
- Support the development of interoperable secure communications systems for state and local governments and designated private sector entities; and
- Complete implementation of the Homeland Security Advisory System.

Personnel Surety, Building Human Capital, and Awareness: This *Strategy* identifies six major initiatives in this area.

- Coordinate the development of national standards for personnel surety;
- Develop a certification program for background-screening companies;

- Explore establishment of a certification regime or model security training program for private security officers;
- Identify requirements and develop programs to protect critical personnel;
- Facilitate the sharing of public- and private-sector protection expertise; and
- Develop and implement a national awareness program for critical infrastructure and key asset protection.

Technology and Research & Development: This *Strategy* identifies four major initiatives in this area.

- Coordinate public- and private-sector security research and development activities;
- Coordinate interoperability standards to ensure compatibility of communications systems;
- Explore methods to authenticate and verify personnel identity; and
- Improve technical surveillance, monitoring and detection capabilities.

Modeling, Simulation, and Analysis: This *Strategy* identifies seven major initiatives in this area.

- Enable the integration of modeling, simulation, and analysis into national infrastructure and asset protection planning and decision support activities;
- Develop economic models of near- and long-term effects of terrorist attacks;
- Develop critical node/chokepoint and interdependency analysis capabilities;
- Model interdependencies across sectors with respect to conflicts between sector alert and warning procedures and actions;
- Conduct integrated risk modeling of cyber and physical threats, vulnerabilities, and consequences; and
- Develop models to improve information integration.

Unique Protection Areas

In addition to the cross-sector themes addressed in this *Strategy*, the individual critical infrastructure sectors and special categories of key assets have unique issues that require action. These considerations and associated enabling initiatives are discussed in the last two chapters of this *Strategy*:

Securing Critical Infrastructures: This *Strategy* identifies major protection initiatives for the following critical infrastructure sectors:

- Agriculture and Food
- Water
- Public Health
- Emergency Services
- Defense Industrial Base
- Telecommunications
- Energy
- Transportation
- Banking and Finance
- Chemicals and Hazardous Materials
- Postal and Shipping

Protecting Key Assets: This *Strategy* identifies major protection initiatives for the following key asset categories:

- National Monuments and Icons
- Nuclear Power Plants
- Dams
- Government Facilities
- Commercial Key Assets

---

1 The *National Strategy for Homeland Security* defines "State" to mean "any state of the United States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, or the trust territory of the Pacific Islands." The *Strategy* defines "local government" as "any county, city, village, town, district, or other political subdivision of any state, any Native American tribe or authorized tribal organization, or Alaska native village or organization, and includes any rural community or unincorporated town or village or any other public entity for which and application for assistance is made by a state or political subdivision thereof."