
ORGANIZING AND PARTNERING FOR CRITICAL INFRASTRUCTURE AND KEY ASSET PROTECTION

Implementing a comprehensive national critical infrastructure and key asset protection strategy requires clear and unifying organization, clarity of purpose, 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. Without it, accomplishing the task of coordinating and integrating domestic protection policy, planning, resource management, performance measurement, and enabling initiatives across federal, state, and local governments, and the private sector would be impossible.

The work of providing a clearly defined and unifying organizational framework began with the publication of the President's *National Strategy for Homeland Security* and continues in this document. This chapter clarifies public- and private-sector roles and responsibilities for critical infrastructure and key asset protection. Ultimately, success lies in our ability to draw effectively and efficiently upon the unique core competencies and resources of each stakeholder. Given the range and complexity of required protection activities and the number of entities involved, clearly-defined authority, accountability, and coordinating processes will provide the foundation for a successful and sustainable national protection effort.

ORGANIZATION AND PARTNERING CHALLENGES

Overlapping federal, state, and local governance and the ownership structure of our critical infrastructures and key assets present significant protection challenges. The entities involved are diverse, and the level of understanding of protection roles and responsibilities differs accordingly. Furthermore, these organizations and individuals represent systems, operations, and institutional cultures that are complex and diverse. The range of protective activities that each must undertake is vast and varies from one enterprise to the next. Finally, overlapping protection authorities across federal, state, and local jurisdictions vary greatly. Success in implementing this *Strategy's* wide range of protection activities lies in establishing a unifying organizational framework that allows the development of

complementary, collaborative relationships and efficiently aligns our Nation's protection resources.

CLARIFYING ROLES AND RESPONSIBILITIES

In our federalist system of government, federal, state, and local governments and private industry have specific roles and perform certain functions that must be integrated to assure protection. Additionally, each critical infrastructure owner/operator possesses unique capabilities, expertise, and resources that, when integrated appropriately, can contribute to a comprehensive national protection effort.



Federal Government Responsibilities

The federal government has fundamental, clearly defined responsibilities under the Constitution. Providing for the common defense and promoting the general welfare of our country are among them. The federal government alone has the capability to use military, intelligence, and diplomatic assets to defend America's interests outside its borders. Closer to home, with support from state and local governments, the federal government has also traditionally led the effort to maintain the security of our borders. To prevent terrorists from entering the U.S., the federal government employs several tools unique to its arsenal, including: military, diplomatic, and intelligence-gathering activities; immigration and naturalization functions; and border agents, customs inspectors, and port and air terminal security.

The federal law enforcement apparatus consists of mechanisms that allow it to coordinate multi-jurisdictional approaches to security threats and incidents and the pursuit of perpetrators across state lines and overseas. Additionally, federal agencies conduct vital research activities, coordinate protection planning and incident management, and provide material and other types of support to state and local authorities. These capabilities serve as elements of deterrence, prevention, protection, and incident response.

Beyond such critical services and functions, the federal government has the capacity to organize, convene, and coordinate across governmental jurisdictions and the private sector. It therefore has the responsibility to develop coherent national policies, strategies, and programs. 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 for each of our critical infrastructures and key assets.

Every terrorist event has national impact. The federal government will therefore take the lead to insure that the three principal objectives defined 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 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 would have significant, national-level consequences;

- Providing and coordinating national threat 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 public- and-private sector entities to devise solutions to their unique protection impediments;
- Developing protection standards, guidelines, and protocols across sectors and jurisdictions;
- Facilitating the exchange of critical infrastructure and key asset protection best practices 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 its ability to work with state and local responders and service providers through partnership.

As custodian of many of our Nation's key assets, such as some of our most treasured icons and monuments, and as the owner and operator of mission-critical facilities, the federal government also has significant, direct protection responsibilities. Accordingly, the federal government will take appropriate steps to:

- Identify its own critical facilities, systems, and functions;
- Identify the critical nodes upon which these assets depend;
- Assess associated vulnerabilities; and
- Implement appropriate steps to mitigate those vulnerabilities and protect the infrastructures and assets under its control.

Federal Lead Departments and Agencies

Each critical infrastructure sector has unique security challenges. The *National Strategy for Homeland Security* provides a sector-based organizational scheme for protecting America's critical infrastructures and key assets. (See *Federal Organization for Critical Infrastructure and Key Asset Protection*, p. 18.) This organizational scheme identifies the federal lead departments and agencies charged with coordinating

protection activities and cultivating long-term collaborative relationships with their sector counterparts.

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

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

Each federal lead department or agency selects a “sector liaison,” who represents industry’s primary interface with the government. Industry’s counterpart, the “sector coordinator,” is designated by the federal lead department or agency to serve as a neutral party and facilitate sector coordination for a wide range of planning and activities to secure critical facilities and systems.

The federal government will expand on this model of public-private sector cooperation as a key component of our strategy for action. Accordingly, the federal lead departments and agencies of critical infrastructure sectors newly identified in the *National Strategy for Homeland Security* will take immediate steps to designate sector liaisons and coordinators and initiate protection activities. This will include identifying critical facilities, systems, and functions within their sectors and facilitating the development of sector protection plans.

Department of Homeland Security

The organizational model of federal lead departments and agencies provides a focused leadership structure for national-level protection coordination and planning. The newly created Department of Homeland Security (DHS) will significantly enhance the effectiveness of this model by providing overall cross-sector coordination. In this role, DHS will serve as the primary liaison and facilitator for cooperation among federal departments and 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*. This charter includes building and maintaining a complete, current,

and accurate assessment of national-level critical assets, systems, and functions, as well as assessing vulnerabilities and protective postures across the critical infrastructure sectors. DHS will use this information to assess threats, provide timely warnings to threatened infrastructures, and build “red team” capabilities to evaluate preparedness across sectors and government jurisdictions. Furthermore, DHS will collaborate with other federal departments and agencies, state and local governments, and the private sector to define and implement complementary structures and coordination processes for critical infrastructure and key asset protection. An effective starting point for this effort is the approach presently employed by federal lead departments and agencies and state and local governments to cooperate when responding to natural disasters.

In addition to cross-sector coordination, DHS will act as the federal lead department for several sectors, including government, emergency response, transportation, postal and shipping, and information and telecommunications.

To fulfill these responsibilities, DHS will:

Build partnerships with state and local governments and the private sector by designing and implementing its own processes to be open, inclusive, and results-oriented.

- Actively develop opportunities to build upon proven models;
- Identify and share the federal government’s core competencies, capabilities, and selected resources to enhance the efforts of its partners; and
- Facilitate honest brokering and communication between organizations and sectors.

Office of Homeland Security

The Office of Homeland Security (OHS) will continue to act as the President’s principal policy advisory staff and coordinating body for major interagency policy issues related to Homeland Security, including the critical infrastructure and key asset protection mission area. The functions of OHS will be to advise and assist the President in the coordination of the Executive Branch’s efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States. OHS will work with the Office of Management and Budget (OMB) to integrate and endorse the President’s critical infrastructure and key asset protection budget proposals. Under its existing authority, OHS will also work with OMB to certify that the budgets of other federal departments and agencies are sufficient to carry out their respective protection missions effectively.

**FEDERAL GOVERNMENT ORGANIZATION TO
PROTECT CRITICAL INFRASTRUCTURE AND KEY ASSETS**

President

Secretary of Homeland Security

Federal, state, local, and private sector coordination and integration
Comprehensive national infrastructure protection plan
Mapping threats to vulnerabilities and issuing warnings

Sector	Lead Agency
Agriculture	Department of Agriculture
Food:	
<i>Meat and poultry</i>	Department of Agriculture
<i>All other food products</i>	Department of Health & Human Services
Water	Environmental Protection Agency
Public Health	Department of Health & Human Services
Emergency Services	Department of Homeland Security
Government:	
<i>Continuity of government</i>	Department of Homeland Security
<i>Continuity of operations</i>	All departments and agencies
Defense Industrial Base	Department of Defense
Information and Telecommunications	Department of Homeland Security
Energy	Department of Energy
Transportation	Department of Homeland Security*
Banking and Finance	Department of the Treasury
Chemical Industry and Hazardous Materials	Environmental Protection Agency
Postal and Shipping	Department of Homeland Security
National Monuments and Icons	Department of the Interior

* Under the *Homeland Security Act of 2002*, the Transportation Security Administration, responsible for securing our Nation's transportation systems, will become part of the Department of Homeland Security. The new Department will coordinate closely with the Department of Transportation, which will remain responsible for transportation safety.

Other Federal Departments and Agencies

Besides the designated federal lead departments and agencies, the federal government will integrate the unique expertise and skill sets of numerous other departments and agencies to enhance the physical protection dimension of homeland security. For example, the National Institute of Science and Technology's (NIST's) National Standards and Measurements Laboratory will play a significant role in standards-setting for the critical infrastructure and key asset protection mission. Recent examples of this role are reflected in the language of the *USA Patriot Act of 2001*, *Enhanced Border Security and Visa Reform Act of 2002*, and *National Construction Safety Team Act*.

Overall sector initiatives will often comprise international components, require the development of coordinated relationships with foreign governments or agencies, and entail information sharing with foreign governments. Accordingly, the Department of State (DoS) will support the development and implementation of protection initiatives by laying the groundwork for bilateral and multilateral infrastructure protective agreements with our international friends and allies. Through its unique responsibility to lead U.S. foreign policy and support the programs and efforts of other federal departments and agencies, DoS will play a key role in advancing our critical infrastructure and key asset priorities.

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. All U.S. states and territories have established homeland security liaison offices to manage their counter-terrorism and infrastructure protection efforts. In addition, the states have law enforcement agencies, National Guard units, and other critical services that can be employed to protect their communities.

Like the federal government, states should identify and secure the critical infrastructures and key assets under their control. With the support of federal lead departments and agencies, states should also promote the coordination of protective and emergency response activities and resource support among local jurisdictions and between regional partners. States should further facilitate coordinated planning and preparedness by applying unified criteria for determining criticality, prioritizing protection investments, and exercising preparedness within their jurisdictions. They should also act as conduits for requests for federal assistance when the threat at hand exceeds the

capabilities of state and local jurisdictions and the private entities within them. States should also facilitate the exchange of relevant security information and threat alerts down to the local level.

Many states have well-organized relationships with one another through various organizations, such as the National Emergency Managers Association and the National Governors Association, as well as through mutual support agreements. Coordinating with one another, they can capitalize on their mutual capabilities through regional approaches to protection. As proven during September 11 response efforts, mutual aid agreements and other such successful cooperative processes for crisis management demonstrate the competence of various jurisdictions and organizations to plan and work together.

At the onset, every disruption or attack is a local problem. Regardless of who owns and operates the affected infrastructure, each requires an immediate response by local authorities and communities who must support the initial burden of action before the incident escalates to a national event.

Local governments represent the front lines of protection and the face of public services to the American people. Their core competencies must include knowledge of their communities, residents, landscapes, and existing critical services for maintaining public health, safety, and order. Communities look to local leadership to assure safety, economic opportunities, and quality of life. Public confidence, therefore, starts locally and is dependent upon how well communities plan and are able to protect their citizens, respond to emergencies, and establish order from chaos. When local authorities succeed in preventing or mitigating loss of life or property, or, as in New York City on September 11, respond to disaster with clarity of purpose and effectiveness, they affirm their capabilities and bolster public confidence. For this reason, local communities play critical roles in preparing their citizens for emergencies and engaging their public and private leadership in the development of coordinated local and regional plans to assure the protection of residents and businesses.

State and local governments look to the federal government for support and resources when national requirements exceed their capabilities to fulfill them. Protecting critical infrastructures and key assets will require a particularly close and well-organized partnership among all levels of government. DHS, in particular, will provide a single point of coordination for state and local governments for homeland security issues. Other federal lead departments and agencies and federal law enforcement organizations will provide

support as needed and appropriate for specific critical infrastructure and key asset protection issues.

Private-Sector Responsibilities

The lion's share of our critical infrastructures and key assets are owned and operated by the private sector. Customarily, private companies prudently engage in risk management planning. They also invest in security as a necessary component of their business operations and to assure customer confidence. In the present threat environment, the private sector 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 accommodate the increased risk presented by deliberate acts of terrorism. Since the events of September 11, enterprises nationwide have increased their investments in security to meet the demands of the new threat environment.

For most enterprises, the level of security investment they undertake reflects implicit risk-versus-consequence tradeoffs, which are determined 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 resources. Given the dynamic nature of the terrorist threat and the severity of the potential consequences associated with many potential attack scenarios, the private sector will look to the government to help better inform its crucial security investment decisions. Similarly, the private sector will require assistance when the threat exceeds an enterprise's capability to protect itself beyond a reasonable level of security investment. The federal government will collaborate with public- and private-sector entities to assure the protection of nationally critical infrastructures and assets, provide timely warnings and help assure the protection of infrastructures that are specifically threatened, and promote an environment in which the private sector can better carry out its specific protection responsibilities.

The availability of both timely, credible information and relevant expertise, complemented by inclusive access to affordable tools and best practices, encourages the private sector to make prudent investments earlier and at all levels of the risk management spectrum. By developing mutually beneficial relationships and coordinating protection efforts, public-private partnership can significantly enhance our Nation's ability to protect its critical infrastructures and key assets.

Working with DHS and other federal lead departments and agencies, sector coordinators will play a crucial role

in enabling this collaboration. Sector coordinators will also work with the government to identify, promote, and share industry-specific best practices. To fulfill their protection agendas, sector coordinators will rely on DHS and other federal lead departments and agencies to provide consistent guidance and criteria for sector-specific protection planning and investment as well as for relevant, actionable, and timely indications and warnings. The private sector may also require incentives to stimulate investment. Accordingly, sector liaisons and sector coordinators will work with their counterparts to explore potential catalysts and reduce the barriers to public-private sector cooperation.

In addition to formal government support, private industry can take many steps to improve its own security posture across the board. Many industries have developed alliances to sustain reliability and assure public confidence in their national-level infrastructures. Because the public's perception of a sector's overall performance can affect the shareholder values of its individual members, many institutions cooperate within a framework for sharing operational and security-related best practices. Sectors whose constituent enterprises are highly interconnected have also developed mutual aid agreements to prevent the disruption of one member's systems from cascading to others across the sector. Reliability activities of the energy sector, specifically the electricity industry, are an example of an effective critical infrastructure partnership.

Even before the September 11 attacks, several critical infrastructure industries had already established Information Sharing and Analysis Centers (ISACs) to formalize information exchange among their members and improve the management of operational risks from physical and cyber disruption. Moreover, many sector organizations, working with their federal counterparts, have also developed plans to contribute to the national protection effort. Federal support of sector ISACs and protection planning must now expand to include the newly designated critical infrastructure sectors.

Partnership will provide the foundation for developing and implementing coordinated protection strategies. True partnerships require continuous interaction and, above all, trust. Currently, however, there are barriers impeding the public and private sectors from achieving a relationship of this level. Many current attitudes and institutional relationships, processes, and structures are products of a bygone era. Safeguarding our critical infrastructures and key assets from terrorism in today's fluid marketplace and threat environment requires a new, more cooperative set of institutional relationships and attitudes. The need for partnering is clear.