THE CASE FOR ACTION

Developing an effective strategy for critical infrastructure and key asset protection requires a clear understanding of the threats we face and the potential consequences they entail. The September 11 attacks were a wake-up call. Before these devastating events, we, as Americans, considered ourselves relatively immune to a massive physical attack on our homeland. Our victory in the Cold War left us with few significant conventional military threats, and the world of terrorism seemed more the concern of troubled regions like the Middle East than Middle America. As a Nation, we were generally unfamiliar with the motivations of terrorists and the deep hatred behind their agendas. Furthermore, we underestimated the depth and scope of their capabilities and did not fully appreciate the extent to which they would go to carry out their destructive acts. The September 11 attacks changed these misconceptions.

Al-Qaeda terrorists exploited key elements of our own transportation infrastructure as weapons. Their targets were key assets symbolic of our national prestige and military and economic power. The effects of the attacks cascaded throughout our society, economy, and government. As a Nation, we became suddenly and painfully aware of the extent of our domestic vulnerability—more so than at any time since the Second World War.

To protect our critical infrastructures and key assets from further terrorist exploitation, we must understand the intent and objectives of terrorism as well as the tactics and techniques its agents could employ against various types of targets. We must complement this understanding with a comprehensive assessment of the 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 SIGNIFICANCE OF CRITICAL INFRASTRUCTURES AND KEY ASSETS

The Importance of Critical Infrastructures

America's critical infrastructure sectors provide the goods and services that contribute to a strong national defense and thriving economy. Moreover, their continued reliability, robustness, and resiliency create a sense of confidence and form an important part of our national identity and strategic purpose. They also frame our way of life and enable Americans to enjoy one of the highest overall standards of living of any country in the world.

When we flip a switch, we expect light. When we pick up a phone, we expect a dial tone. When we turn a tap, we expect drinkable water. Electricity, clean water, and telecommunications are only a few of the critical infrastructure services that we tend to take for granted. They have become so basic in our daily lives that we notice them only when, for some reason, service is disrupted. When disruption does occur, we expect reasonable explanations and speedy restoration of service.

The *National Strategy for Homeland Security* categorizes our critical infrastructures into the following sectors:

CRITICAL INFRASTRUCTURE SECTORS

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

Critical infrastructures are "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

- USA Patriot Act

Together these industries provide:

Production and Delivery of Essential Goods and Services

Critical infrastructure sectors such as agriculture, food, and water, along with public health and emergency services, provide the essential goods and services that Americans depend on to survive.

Energy, transportation, banking and financial services, chemical manufacturing, postal services, and shipping sustain the Nation's economy and make possible and available a continuous array of goods and services.

Interconnectedness and Operability

Information and telecommunications infrastructures connect and increasingly control the operations of other critical infrastructures.

Public Safety and Security

Our government institutions guarantee our national security, freedom, and governance, as well as services that make up the Nation's public safety net.

The facilities, systems, and functions that comprise our critical infrastructures are highly sophisticated and complex. They consist of human capital and physical and cyber systems that work together in processes that are highly interdependent. They each encompass a series of key nodes that are, in turn, essential to the operation of the critical infrastructures in which they function. To complicate matters further, our most critical infrastructures typically interconnect and, therefore, depend on the continued availability and operation of other dynamic systems and functions.

For example, e-commerce depends on electricity as well as information and communications. Assuring electric service requires operational transportation and distribution systems to guarantee the delivery of fuel necessary to generate power. Such interdependencies

have developed over time and are the product of innovative operational processes that have fueled unprecedented efficiency and productivity. Given the dynamic nature of these interdependent infrastructures and the extent to which our daily lives rely on them, a successful terrorist attack to disrupt or destroy them could have tremendous impact beyond the immediate target and continue to reverberate long after the immediate damage is done.

The Importance of Key Assets

Key assets represent individual targets whose destruction could cause large-scale injury, death, or destruction of property, and/or profoundly damage our national prestige, and confidence. Such assets and activities alone may not be vital to the continuity of critical services on a national scale, but an attack on any one of them could produce, in the worst case, significant loss of life and/or public health and safety consequences. This category includes such facilities as nuclear power plants, dams, and hazardous materials storage facilities.

Other key assets are symbolically equated with traditional American values and institutions or U.S. political and economic power. Our national symbols, icons, monuments, and historical attractions preserve history, honor achievements, and represent the natural grandeur of our country. They also celebrate our American ideals and way of life—a key target of terrorist attacks. Successful terrorist strikes against such assets could profoundly impact national public confidence. Monuments and icons, furthermore, tend to be gathering places for large numbers of people, particularly during high-profile celebratory events—a factor that adds to their attractiveness as targets.

Ownership of key assets varies. The private sector owns and operates dams and nuclear power plants as well as most of this Nation's large buildings holding important commercial and/or symbolic value and/or housing large numbers of people. The protection of national monuments and icons often entails overlapping state, local, and federal jurisdictions. Some are managed and operated by private foundations. These realities complicate our protective efforts.

UNDERSTANDING THE THREAT

Characteristics of Terrorism

The September 11 attacks offered undeniable proof that our critical infrastructures and key assets represent high-value targets for terrorism. The attacks underscored the determination and patience of our terrorist enemies. The highly coordinated nature of the strikes demonstrated a previously unanticipated level of sophistication in terms of planning and execution. Through these attacks, Al-Qaeda terrorists also showed a dogged resolve in pursuit of their objectives. When their first attempt to topple the World Trade Center towers failed in 1993, they persisted by planning and executing a second attack eight years later that proved to be more successful than even they expected.

Our terrorist enemies have proven themselves to be opportunistic and flexible. As illustrated by the two separate World Trade Center attacks, they learn from experience and modify their tactics accordingly. They also adapt their methods in order to exploit newly observed or perceived vulnerabilities. As security increases around more predictable targets, they will likely seek more accessible and less protected facilities and events. Enhancing countermeasures against any one terrorist tactic, therefore, makes it more likely that terrorists will favor another.

Terrorists are inventive and resourceful in terms of target selection, as well as in the selection and use of specific instruments of violence and intimidation. They exploit vulnerabilities wherever they exist, with any means at their disposal, at times and locations of their choosing. Terrorists are attempting to acquire a broad range of weapons, from high-yield conventional explosives and firearms to weapons of mass destruction. Oftentimes the nature of the target will dictate the weapon of choice. Other times the availability of a particular type of weapon, such as a nuclear or biological device, will determine target selection. The matching of means to ends is limited only by the creativity and resources of the terrorists; the only constant is their desire to inflict maximum destruction, injury, and shock in pursuit of their strategic objectives.

Terrorism is with us for the foreseeable future. Following the September 11 attacks, President Bush stated that the war on terrorism would be a long-term effort. While the tools and tactics of terrorists may change, their fundamental determination remains the same. Those with enmity toward the U.S. and its interests consider terrorism an effective weapon to use against us, and they will continue to employ such tactics until we can prove that it is not.

The Nature of Possible Attacks

The terrorist endgame includes a complex mix of political, economic, and psychological objectives. To achieve their objectives, terrorists may choose to target critical infrastructures and key assets as low-risk means to generate mass casualties, shock, and panic.

Terrorists target critical infrastructure and key assets to achieve effects that fall into three general categories:

- *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.

  The immediate damage to facilities and disruption of services that resulted from the attack on the World Trade Center towers, which housed critical assets of the financial services sector, are examples of direct infrastructure effects.

- *Indirect infrastructure effects:* Cascading disruption and financial consequences for government, society, and economy through public- and private-sector reactions to an attack.

  Public disengagement from air travel and other facets of the economy as a result of the September 11 attacks exemplifies this effect. Mitigating the potential consequences from these types of attacks will require careful assessment of policy and regulatory responses, understanding the psychology of their impacts, and appropriately weighing the costs and benefits of specific actions in response to small-scale attacks.

- *Exploitation of infrastructure:* Exploitation of elements of a particular infrastructure to disrupt or destroy another target.

  On September 11, terrorists exploited elements of the aviation infrastructure to attack the World Trade Center and the Pentagon, which represented seats of U.S. economic and military power. Determining the potential cascading and cross-sector consequences of this type of attack is extremely difficult.

CHALLENGES TO PROTECTING CRITICAL INFRASTRUCTURES AND KEY ASSETS

The New Front Lines

Our technologically sophisticated society and institutions present a wide array of potential targets for terrorist exploitation. Our critical infrastructure industries change rapidly to reflect the demands of the markets they serve. Much of the expertise required for planning and taking action to protect critical infrastructures and key assets lies outside the federal government, including precise knowledge of what needs to be protected. In effect, the front lines of defense in this new type of battle have moved into our communities and the individual institutions that make up our critical infrastructure sectors.

Private industry owns and operates approximately 85 percent of our critical infrastructures and key assets. Facility operators have always been responsible for protecting their physical assets against unauthorized intruders. These measures, however conventionally effective, generally have not been designed to cope with significant military or terrorist threats, or the cascading economic and psychological impact they may entail.

The unique characteristics of critical infrastructures and key assets, their continuing—often rapid—evolution, and the significant impediments complicating their protection will require an unprecedented level of key public- and private-sector cooperation and coordination. Our country has more than 87,000 jurisdictions of local governance alone. The challenge ahead is to develop a coordinated and complementary system that reinforces protection efforts rather than duplicates them, and that meets mutually identified essential requirements. In addition, many of our critical infrastructures also span national borders and, therefore, must be protected within the context of international cooperation.

A NEW PARADIGM: COOPERATION AND PARTNERSHIP

Our open society, highly creative and responsive economic markets, and system of values that engenders individual recognition and freedom have created wealth for our nation, built a strong national security system, and instilled a sense of national confidence in the future. Destruction of our traditions, values, and way of life represents a key objective of our terrorist enemies. Ironically, the tenets of American society that make us free also create an environment that facilitates terrorist operations.

As we strive to understand the nature of terrorism and identify appropriate means to defend against it, we will require new collaborative structures and mechanisms for working together. During the Cold War era, many government and private organizations isolated parts of their physical and information infrastructures into "stovepipes" to assure their protection. This approach is no longer adequate to protect our homeland from determined terrorists. Stimulating voluntary, rapidly adaptive protection activities requires a culture of trust and ongoing collaboration among relevant public- and private-sector stakeholders, rather than more traditional systems of command and control.

Security investments made by all levels of government and private industry have increased since the September 11 attacks. As terrorism continues to evolve, so must the way in which we protect our

country and ourselves. The costs of protection—including expenditures to develop new technologies, tools, and procedures—will weigh heavily on all levels of government and private industry. Consequently, an effective protection strategy must incorporate well-planned and highly coordinated approaches that have been developed by the best minds in our country through innovation and sharing of information, best practices, and shared resources.

National Resilience: Sustaining Protection for the Long Term

Combating terrorism will be a long-term effort. Its dynamic nature means that we must enhance the protection of our critical infrastructures and key assets in an environment of persistent and evolving threats.

Our Nation's critical infrastructures are generally robust and resilient. These attributes result from decades of experience gained from responding to natural disasters, such as hurricanes and floods, and the deliberate acts of malicious individuals. The critical infrastructure sectors have learned from each disruption and applied those lessons to improve their protection, response, and recovery operations. For example, during the immediate aftermath of the September 11 attacks, the electric system in New York City remained operational for the island of Manhattan outside of the World Trade Center complex—Ground Zero. Furthermore, needed electric service at Ground Zero was quickly and efficiently restored to support rescue and recovery operations. This success is a good example of American ingenuity, as well as a tenacious application of lessons learned from the 1993 World Trade Center bombing and other terrorist events.

Resilience is characteristic of most U.S. communities, and it is reflected in the ways they cope with natural disasters. Over time, residents of communities in areas that are persistently subjected to natural disasters become accustomed to what to expect when one occurs. Institutions and residents in such areas grow to understand the nature of catastrophic events, as well as their roles and responsibilities in managing their after-effects. They are also familiar with and rely on trusted community systems and resources that are in place to support protection, response, and recovery efforts. As a result, they have confidence in their communities' abilities to contend with the aftermath of disasters and learn from each event.

Institutions and residents nationwide must likewise come to understand the nature of terrorism, its consequences, and the role they play in combating it. Ideally, they will become familiar with and have confidence in

THE PROTECTION CHALLENGE

Agriculture and Food	1,912,000 farms; 87,000 food-processing plants
Water	1,800 federal reservoirs; 1,600 municipal waste water facilities
Public Health	5,800 registered hospitals
Emergency Services	87,000 U.S. localities
Defense Industrial Base	250,000 firms in 215 distinct industries
Telecommunications	2 billion miles of cable
Energy	
Electricity	2,800 power plants
Oil and Natural Gas	300,000 producing sites
Transportation	
Aviation	5,000 public airports
Passenger Rail and Railroads	120,000 miles of major railroads
Highways, Trucking, and Busing	590,000 highway bridges
Pipelines	2 million miles of pipelines
Maritime	300 inland/costal ports
Mass Transit	500 major urban public transit operators
Banking and Finance	26,600 FDIC insured institutions
Chemical Industry and Hazardous Materials	66,000 chemical plants
Postal and Shipping	137 million delivery sites
Key Assets	
National Monuments and Icons	5,800 historic buildings
Nuclear Power Plants	104 commercial nuclear power plants
Dams	80,000 dams
Government Facilities	3,000 government owned/operated facilities
Commercial Assets	460 skyscrapers

*These are approximate figures.

the protection, response, and recovery mechanisms that exist within their communities. Together with local officials, private organizations and residents must work to improve these systems and resources to meet the challenge of safeguarding our country from terrorists.

Our challenge is to identify, build upon, and apply the lessons learned from the September 11 attacks to anticipate and protect against future terrorist attacks on our critical infrastructures and key assets. Our ability to do so will determine how successfully we adapt to the current dynamic threat environment and whether we can emerge as a stronger, more vibrant nation with our values and way of life intact.