INTRODUCTION

On July 16, 2002, President Bush issued the *National Strategy for Homeland Security*, an overarching strategy for mobilizing and organizing our Nation to secure the U.S. homeland from terrorist attacks. It communicates a comprehensive approach "based on the principles of shared responsibility and partnership with Congress, state and local governments, the private sector, and the American people"—a truly national effort, not merely a federal one.

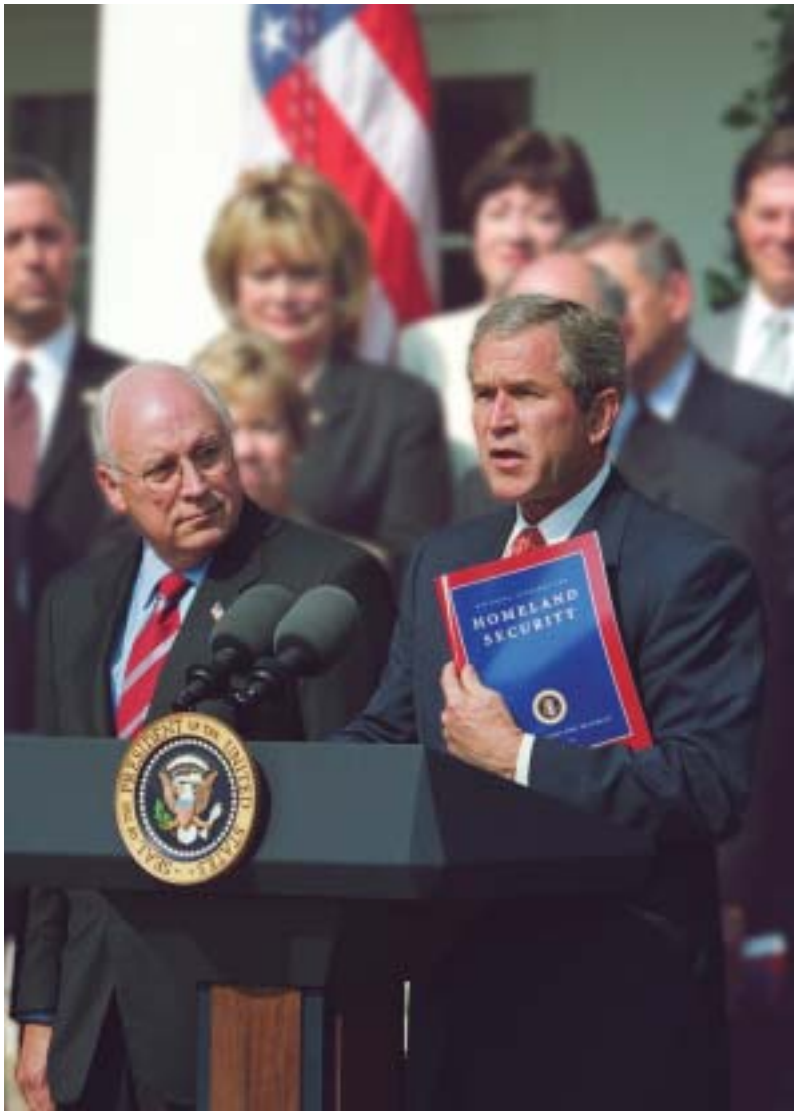
The *National Strategy for Homeland Security* defines "homeland security" and identifies a strategic framework based on three national objectives. In order of priority, these are: (1) preventing terrorist attacks within the United States, (2) reducing America's vulnerability to terrorism, and (3) minimizing the damage and recovering from attacks that do occur.

HOMELAND SECURITY CRITICAL MISSION AREAS

- Intelligence and Warning
- Border and Transportation Security
- Domestic Counter-terrorism
- Protecting Critical Infrastructures and Key Assets
- Defending against Catastrophic Terrorism
- Emergency Preparedness and Response

To attain these objectives, the *National Strategy for Homeland Security* aligns our homeland security efforts into six critical mission areas: intelligence and warning, border and transportation security, domestic counter-terrorism, protecting critical infrastructures and key assets, defending against catastrophic terrorism, and emergency preparedness and response.

This document, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, the *Strategy*,[1] takes the next step to facilitate the strategic planning process for a core mission area identified in



"The United States will forge an unprecedented level of cooperation throughout all levels of government, with private industry and institutions, and with the American people to protect our critical infrastructure and key assets from terrorist attack."

-The National Strategy for Homeland Security

the *National Strategy for Homeland Security*—reducing the Nation's vulnerability by protecting our critical infrastructures and key assets from physical attack. It 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. It also provides a unifying organizational structure and identifies specific initiatives to drive our near-term national protection priorities and inform the resource allocation process. Most importantly, it provides 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 World Trade Center and Pentagon attacks on September 11, 2001, to improve the security of their critical facilities, systems, and functions. Building on these efforts, this *Strategy* 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. Accordingly, this *Strategy* belongs and applies to the Nation as a whole, not just to the federal government or its constituent departments and agencies.

This *Strategy* complements the *National Strategy to Secure Cyberspace*, which focuses on the identification, assessment, and protection of interconnected information systems and networks. The *Physical and Cyber Strategies* share common underlying policy objectives and principles. Together, they form the road ahead for one of our core homeland security mission areas.

A NEW MISSION

The September 11 attacks on the World Trade Center and the Pentagon 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. Ironically, the basic nature of our free society greatly enables terrorist operations and tactics, while, at the same time, it 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.

Protecting America's critical infrastructures and key assets represents an enormous challenge. Our Nation's critical infrastructures and key assets are a highly complex, heterogeneous, and interdependent mix of facilities, systems, and functions that are vulnerable to a wide variety of threats. Their sheer numbers, pervasiveness, and interconnected nature create an almost infinite array of high-payoff targets for terrorist exploitation. Given the immense size and scope of the potential target set, we cannot assume that we will be able to protect completely all things at all times against all conceivable threats. As we develop protective measures for one particular type of target, our terrorist enemies will likely focus on another. To be effective, our national protection strategy must be based on a thorough understanding of these complexities as we build and implement a focused plan for action.

DEFINING THE END STATE: STRATEGIC OBJECTIVES

To frame the initial focus of our national protection effort, we must acknowledge that the assets, systems, and functions that comprise our infrastructure sectors are not uniformly "critical" in nature, particularly in a national or major regional context.

The first objective of this *Strategy* is to identify and assure the protection of those assets, systems, and functions that we deem most "critical" in terms of national-level public health and safety, governance, economic and national security, and public confidence. We must develop a comprehensive, prioritized assessment of facilities, systems, and functions of national-level criticality and monitor their preparedness across infrastructure sectors. The federal government will work closely with state and local governments and the private sector to establish a uniform methodology for determining national-level criticality. This methodology will enable a focus on high-priority activities and the development of consistent approaches to counter the terrorist threat.

The second major objective is to assure the protection of infrastructures and assets that face a specific, imminent threat. Federal, state, and local governments and private-sector partners must collaborate closely to develop thorough assessment and alert processes and systems to ensure that threatened assets receive timely advance warnings. These entities must further cooperate to provide focused protection against the anticipated threat.

Finally, as we act to secure our most critical infrastructures and assets, we must remain cognizant that criticality varies as a function of time, risk, and market changes. Acting to better secure our highest priority facilities, systems, and functions, we should expect our terrorist enemies to shift their destructive focus to targets they consider less protected and more likely to yield desired shock effects. Hence, the third objective of this *Strategy* is to pursue collaborative measures and initiatives to assure the protection of other potential targets that may become attractive over time. The focus will be to foster an environment in which key public- and private-sector stakeholders can better protect the infrastructures and assets they control according to their specific responsibilities, competencies, and capabilities.

The last three chapters of this *Strategy* detail the cross-sector and sector-specific priority solution paths we will pursue to achieve the fullest measure of national protection possible across all categories of critical infrastructures and key assets.

HOMELAND SECURITY AND INFRASTRUCTURE PROTECTION: A SHARED RESPONSIBILITY

Protecting America's critical infrastructures and key assets calls for a transition to an important new national cooperative paradigm. The basic tenets of *homeland* security are fundamentally different from the historically defined tenets of *national* security. Historically, securing the United States entailed the projection of force outside of our borders. We protected ourselves by "keeping our neighborhood safe" in the global, geopolitical sense. The capability and responsibility to carry out this mission rested largely with the federal government.

The emergence of international terrorism within our borders has moved the front line of domestic security to Main Street, U.S.A. Faced with the realities of the September 11 attacks, the mission of protecting our homeland now entails "keeping our neighborhood safe" in the most literal sense. Safeguarding our Nation against the terrorist threat depends on our ability to marshal and project appropriate resources inward. Respect for the open, pluralistic nature of our society; the individual rights and liberties of our citizenry; and our federalist system of government define the framework within which security can be implemented.

Acting alone, the federal government lacks the comprehensive set of tools and competencies required

"Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur."

-The National Strategy for Homeland Security

to deliver the most effective protection and response for most homeland security threats. Therefore, to combat the threat terrorism poses for our critical infrastructures and key assets, we must draw upon the resources and capabilities of those who stand on the new front lines—our local communities and private sector entities that comprise our national critical infrastructure sectors.

Forging this unprecedented level of cooperation will require dramatic changes in the institutional mindsets honed and shaped by Cold War-era regimes. Success in this effort must be built and sustained over time. This *Strategy* provides a starting point for defining how this national-level cooperation can best be achieved.

In the context of a new national cooperative paradigm, this *Strategy* further serves as an important vehicle for educating the public and achieving realistic expectations on the emergent terrorist threat and the roles government and industry must play in defending against it. Public understanding and acceptance of this *Strategy* is essential. The American public's resilience and support will be sustainable in the aftermath of future terrorist attacks only if expectations are clearly defined, attainable, and fulfilled.

STRATEGY OVERVIEW

This *Strategy* is comprehensive in scope and focused in detail. The following chapters lay out a roadmap to identify specific priority actions to be taken to assure more comprehensive protection of our critical infrastructures and key assets.

The Case for Action

This chapter discusses the role critical infrastructures and key assets play as a foundation of our Nation's economic security, governance, national defense, public health and safety, and public confidence. It describes in greater detail the characteristics of terrorism and the challenges we must

address to protect the Nation's critical infrastructures and key assets against this threat.

National Policy and Guiding Principles

This chapter describes the overarching national policy and guiding principles that underpin this *Strategy* and our collective approach to action.

Organizing and Partnering for Critical Infrastructure and Key Asset Protection

This chapter provides an organizational structure for our national-level critical infrastructure and key asset protection effort. It also clarifies key public- and private-sector roles and responsibilities and provides a collaborative framework for cross-sector and cross-jurisdictional infrastructure and asset protection.

Cross-Sector Security Priorities

This chapter addresses important cross-sector issues, impediments to action, and the steps necessary to address them. It describes actions to foster cooperation, lower costs, and provide leverage across key issue areas for maximum effect. In concert, these initiatives form the framework through which we will align the resources of the federal budget to the critical infrastructure and key asset protection mission.

Securing Critical Infrastructures

This chapter outlines protection priorities for the critical infrastructure sectors identified in the *National Strategy for Homeland Security*. The overviews provided are designed to highlight pressing issues in need of concerted attention at the individual sector level. Each federal lead department and agency will develop plans and programs to implement or facilitate these priority sector initiatives.

Protecting Key Assets

This chapter describes protection considerations for unique facilities, such as dams, nuclear power plants, and national monuments and icons whose attack, in a worst-case scenario, could present significant health and safety and/or public confidence consequences.

Conclusion

This chapter summarizes the next steps required to assure comprehensive protection of our critical infrastructures and key assets.

---

1 The primary focus of this *Strategy* is the physical protection of critical infrastructures and key assets. The protective strategy for information technology and network assets for specific sectors is discussed in detail in the *National Strategy to Secure Cyberspace*. Accordingly, the protection of the Information Technology component of the Information and Telecommunications sector is not discussed in this document.