CROSS-SECTOR SECURITY PRIORITIES

This chapter addresses the overarching, cross-sector initiatives that represent our national-level priorities for critical infrastructure and key asset protection. The focus is on cross-sector protection issues and activities that require immediate attention, encourage cooperation, and increase the cost-effectiveness of security investments. The protection initiatives outlined herein also support the three underlying objectives of this *Strategy*: (1) identifying and assuring the protection of our most nationally critical infrastructures and assets; (2) providing timely warning and assuring the protection of infrastructures and assets that face a specific, imminent threat; and (3) fostering an environment in which all stakeholders can better protect the infrastructures and assets under their control.

We have entered a fluid threat environment in which security must be viewed as an integral component of core practices and standard operations—not a box to be checked before addressing other issues. As the threat of terrorism persists and evolves, we must be able to adapt our security planning and protection efforts to remain effective and sustainable over the long term. The activities that follow in this *Strategy* represent the first steps in this national journey.

The cross-sector security initiatives addressed in this chapter fall into the following categories:

- Planning and Resource Allocation
- Information Sharing and Indications and Warnings
- Personnel Surety, Building Human Capital, and Awareness
- Technology and Research & Development
- Modeling, Simulation, and Analysis

Each section describes a cross-sector protection issue as well as the impediments to protection associated with that issue. It then identifies specific actions that will be taken to address those challenges and remove barriers hindering the implementation of needed protection activities.

PLANNING AND RESOURCE ALLOCATION

Effective and efficient risk assessment, protection planning, and resource allocation go hand in hand. They depend upon the ability of federal, state, and local governments, the private sector, and our international partners to work together to articulate and attain their individual and shared goals, requirements, and priorities.

State and local governments currently face unprecedented demands for their limited resources. Declines in revenues mean that states and local communities often lack the resources to undertake a full spectrum of prudent critical infrastructure protection measures. Because of these resource limitations, federal, state, and local authorities must collaborate more efficiently to assess, plan, and allocate their limited resources.

Industry is likewise coping with the consequences of dynamic threats and difficult economic environments. In some cases, certain critical-sector enterprises are concentrating their resources solely on remaining in business. To instill greater stability in the security investment process, it will be necessary for private-sector organizations to closely coordinate critical infrastructure protection plans and programs to ensure that federal and state governments, in particular, understand and recognize their future spending landscape.

Risk assessment and management must also be closely integrated and coordinated. Industries and institutions are in need of a common vocabulary and standards to guide their protection efforts. Close cooperation among all levels of government and the private sector both nationally and internationally is essential to developing a shared vernacular and vision for the future.

Planning and Resource Allocation Challenges

Heavy demands on state and local resources, uncertainties created by a lack of coordination, and dynamics of the terrorist threat underlie many of the challenges of the domestic protection environment. Since the September 11 attacks, state and local governments have been called upon to provide increased security for their critical infrastructures and key assets, border areas, airports, and seaports. Unanticipated revenue declines have affected most states and challenged their abilities to meet the requirements of operating under balanced budgets. Hence, they cannot increase expenditures to account for additional protective measures without making corresponding reductions in spending for other programs and services.

We often rely on state and local jurisdictions to protect key national assets (e.g., bridges, tunnels, nuclear power plants, dams, and airports). Conversely, state and local governments request federal resources at times to ensure the protection of their own critical infrastructures and key assets. Under uncertain and sustained elevated threat conditions, determining how best to allocate the scarce resources of the various jurisdictions responsibly and appropriately will require unprecedented levels of cooperation across all levels of government.

Another resource allocation challenge relates to the mechanisms through which states must apply for federal assistance. Current policies and procedures sometimes create inefficiencies in the federal grant decision-making process. Because they must seek funding from various sources according to different guidelines, state and local government officials often view complying with grant requirements and review processes as leading to duplications of effort. Rectifying the lack of streamlined mechanisms for providing federal funding to state and local governments will require a thorough cross-agency review.

Engaging U.S. states and territories in a collaborative framework for infrastructure protection is another important planning challenge. State and local law enforcement agencies and emergency responders are the first line of defense against deliberate acts of violence. In fact, state and local jurisdictions continue to bear a large share of post-September 11 security expenditures nationwide. Their concerns and constraints must be recognized and factored into our national protective scheme.

A key challenge in prioritizing efforts to enhance infrastructure protection is the difficulty in estimating the economic damage that could result from a terrorist attack. Such damage includes both the immediate effects of a strike (e.g., losses to plant and equipment) as well as any subsequent long-term economic losses. The cascading effects often overshadow short-term repercussions over time, yet they are extremely difficult to estimate. Relatively short-term disruptions to critical operations can produce significant downstream economic effects (e.g., price changes, lost contracts, lost financing, and losses in insurability). Predicting the extent of such effects accurately requires acute sensitivity to the myriad of interdependencies present in modern industrial and financial markets.

In the risk management process, certain aspects of criticality determination may also produce inadvertent consequences. Designating certain facilities as "critical" in conjunction with domestic protection efforts may result in their becoming more difficult and expensive to insure and operate. The federal government must work in concert with other key stakeholders to explore options for incentives to compensate for the costs engendered by the current threat environment.

Aligning disparate assessment methodologies presents another challenge. Presently, multiple methodologies from various departments and agencies are currently being used to assess vulnerabilities. In many cases, they are neither consistent, nor comparable, thereby complicating protection planning and resource allocation across the board.

Many critical infrastructures also cross international borders, raising unique protection challenges. We must, therefore, work closely with our friends and allies around the world to develop plans to secure the interconnected infrastructures that make up the international marketplace.

Planning and Resource Allocation Initiatives

It is incumbent in the planning and resource allocation process that federal, state, and local governments and private-sector stakeholders work together to:

- Define clearly their critical infrastructure and key asset protection objectives;
- Develop a business case for action to justify increased security investments;
- Establish security baselines, standards, and guidelines; and
- Identify potential incentives for security-related activities where they do not naturally exist in the marketplace.

To enable such actions, we will:

Create collaborative mechanisms for public- and private-sector critical infrastructure and key asset protection planning

DHS and other federal lead departments and agencies will enable and encourage the development of clearly defined collaborative mechanisms through which the public and private sectors can cooperate in national-level protection planning and performance measurement. The federal government will also work in conjunction with other stakeholders to assess critical infrastructure and asset vulnerabilities, share information, develop protection strategies and plans to eliminate or mitigate these vulnerabilities, and develop restoration and recovery plans for implementation in the aftermath of an attack. DHS will assess these sector plans for clarity, comprehensiveness, consistency, and resource prioritization.

DHS will also assimilate the individual sector plans into a comprehensive national plan for critical infrastructure and key asset protection to inform the federal government's annual process of planning, programming, and budgeting for national-level protection activities.

Identify key protection priorities and develop appropriate supporting mechanisms for these priorities

DHS, in collaboration with other key stakeholders, will develop a uniform methodology for identifying facilities, systems, and functions with national-level criticality to help establish federal, state, and local government and the private-sector protection priorities. Using this methodology, DHS will build a comprehensive database to catalog these critical facilities, systems, and functions. DHS will also maintain a comprehensive, up-to-date assessment of vulnerabilities and preparedness across critical sectors. This effort will help guide near-term protective actions and provide a basis for long-term leadership focus and informed resource investment.

DHS will furthermore establish a multi-year approach for critical infrastructure and key asset protection to instill predictability and structure in the planning process.

Foster increased sharing of risk-management expertise between the public and private sectors

Many different risk assessment methodologies are in use based on a wide variety of requirements and standards. Government and industry could each benefit greatly from the extensive experience of the other. DHS will coordinate the sharing of lessons learned and best practices to build a common

domestic protection assessment framework that is adaptable to different user environments.

Identify options for incentives for private organizations that proactively implement enhanced security measures

Consulting with the private sector, DHS will work with the Department of Commerce (DoC) and the Department of the Treasury to identify appropriate options for developing cost-effective incentives to compensate stakeholders for enhanced security investments.

This could include rewarding early adopters of new policies or providing various incentives for incorporating security enhancements into critical sector products and services.

Coordinate and consolidate federal and state protection plans

DHS will work with other federal departments and agencies to consolidate federal protection plans to clarify roles, responsibilities, and expectations. DHS will also work with the states to coordinate protection-planning efforts and provide them with a clear roadmap for action. Additionally, the Homeland Security Advisory System will be coordinated with state-level critical infrastructure and key asset protection plans.

Establish a taskforce to review legal impediments to reconstitution and recovery following an attack against a critical infrastructure or key asset

DHS, in concert with the Department of Justice (DoJ), will convene representatives from federal, state, and local governments, and the private sector to scrutinize regulatory and licensing procedures that could impede reconstitution of critical infrastructure service in emergencies and identify options for resolving them.

Reconstitution requirements for critical infrastructures may necessitate the waiving of established licensing and regulatory procedures during emergencies. Procedures for establishing these "post incident rule sets" need to be predetermined as part of part of a collaborative public-private partnership.

Develop an integrated critical infrastructure and key asset geospatial database

To enable effective critical infrastructure and key asset protection planning, analysis, and decision support, we must develop an integrated critical infrastructure and key asset geospatial database for access and specific use by federal, state, and local government officials, and the private sector.

A geospatial assurance partnership of appropriate government departments and agencies is needed to serve as the imagery/geospatial data broker, integrator, and coordinator for this database. DHS and other federal departments and agencies will continue current efforts to acquire data for priority population centers, domestic critical infrastructure sectors, and transborder infrastructures in cooperation with the private sector. This database will provide a common frame of reference for senior public- and private-sector decision makers and operational planners in support of vulnerability analysis, domestic preparedness, and incident management.

Conduct critical infrastructure protection planning with our international partners

In the aftermath of the September 11 attacks, we developed comprehensive bilateral critical infrastructure protection framework agreements and began a series of protection initiatives with our Canadian and Mexican neighbors. DHS, in concert with DoS and other federal departments and agencies will work to expand this security collaboration to include other key international partners. The overall objective of this effort will be to determine our transborder infrastructure vulnerabilities and implement measures to eliminate or mitigate these vulnerabilities.

INFORMATION SHARING AND INDICATIONS AND WARNINGS

To meet the challenges associated with the terrorist threat, public- and private-sector critical infrastructure and key asset protection stakeholders must have the ability to work together seamlessly. The federal government—particularly the intelligence and law enforcement communities—has a significant role in providing, coordinating, and ensuring that threat information is understood across all levels of government. Likewise, state and local law enforcement and private-sector security entities are also valuable sources of localized threat information. Additionally, they possess a much better understanding of the vulnerabilities impacting their facilities, systems, and functions than does the federal government. Development of accepted and efficient processes and systems for communication and exchange of crucial security-related information is critical to bridging existing gaps and building a foundation for cooperation.

The difficulties and roadblocks routinely faced by those attempting to share security information serve as major impediments to progress in the critical infrastructure and key asset protection mission area. An extraordinary level of cooperation and perseverance will be required to change the status quo. Federal, state, and local governments and the private sector must make every effort to promote effective information sharing and embrace efforts to establish timely, effective, and useful paths of communication between those who need it most. Information is a crucial tool in fighting terrorism, and getting the right information to the right party at the right time is a top priority.

Adequate protection of our critical infrastructures and key assets requires:

- Improved collection of threat information;
- Comprehensive and relevant threat assessment and analysis;
- Robust indications and warning processes and systems; and
- Improved coordination of information sharing activities.

Accurate, timely information is a fundamental element of our national critical infrastructure and key asset protection effort. It underpins all components of our protection strategy and enables preventive action, warning, preparation, and crisis response. Presently, major impediments exist to accomplishing effective information sharing among all levels of the public and private sectors. Overcoming these obstacles entails:

- Identifying what is to be accomplished by exchanging security-related information;
- Defining the type of information that must be shared to accomplish that purpose;
- Determining how and when to share and safeguard critical security information most properly;
- Deciding who the appropriate recipients of such information will be;
- Assigning responsibility for analyzing information and determining the threat implications; and
- Assigning responsibility for appropriate action once that information has been analyzed and the threat implications are clear.

Information Sharing and Indications and Warnings Challenges

The overall management of information sharing activities among government agencies and between the public and private sectors has lacked proper coordination and facilitation. As a result, the existing national mechanisms for collecting threat information, conducting risk analyses, and disseminating warnings have been inadequate for the domestic protection mission.

State and local governments and private sector officials have indicated that the threat information they receive from the federal government is often vague, duplicative,

and—in some cases—conflicting. They argue that they seldom receive indications and warnings that are specific, accurate, and timely enough to support difficult resource allocation decisions. Conversely, when relevant, timely information is shared, they point out that it often fails to reach the appropriate parties because of security clearance requirements.

Additionally, the current security clearance process is redundant and costly, with lengthy delays. In one example, current regulations require certain state and local law enforcement officials to be screened twice, once by state and local authorities and again by the federal government. We must streamline this process to make it more responsive to our protection needs.

In fact, protecting the Nation's critical infrastructures and key assets may not necessarily require such clearance for all stakeholders. If intelligence sources and methods are omitted, many intelligence reports may be declassified. Time-efficient procedures are needed to declassify relevant intelligence or extract information from classified sources and disseminate that information to the appropriate recipients. These concerns are complicated by the ineffective means by which sensitive information is transferred, as well as the mechanisms currently in place to ensure that required information is disseminated appropriately. Currently, there is no central, coordinating mechanism to assess the impact of sensitive information and ensure that it gets to all the parties with a need to know. Adding to this problem is the lack of technical communications systems to enable the secure transmittal of classified threat information to the owners and operators of concern.

The above issues pose a significant challenge and stand in the way of the partnership our Nation needs to assure the protection of its critical infrastructures and key assets. Underlying these issues is an inherent lack of trust among key stakeholders that we must overcome. Without all pieces of the information puzzle, we operate from a major disadvantage in the fight against terrorism.

Information Sharing and Indications and Warnings Initiatives

The enactment of the *Homeland Security Act of 2002*, the *Act*, represents substantial progress in removing the legal obstacles that stand in the way of information sharing between the public and private sectors. The *Act* provides that critical infrastructure information voluntarily submitted to DHS, when accompanied by an express statement of the expectation that it will be protected, will be exempt from disclosure under the *Freedom of Information Act* and state "Sunshine" laws. Further, if such information is submitted in good faith, it may not be directly used in civil litigation without the consent of the person submitting it.

The *Act* also provides for the establishment of governmental procedures for receiving, handling, and storing voluntarily submitted critical infrastructure information and for protecting the confidentiality of such information. It also provides for the development of mechanisms that, while preserving confidentiality, also permit the sharing of such information within the federal government and with state and local governments. The *Act* authorizes the federal government to provide advisories, alerts, and warnings to relevant businesses, targeted sectors, other governmental actors, and the general public regarding potential threats to critical infrastructure. The *Act* also stipulates that the federal government must protect the source of any voluntarily submitted information forming the basis of a warning as well as any proprietary or other information that is not properly in the public domain.

Finally, the *Act* enables private-sector actors to enter into voluntary agreements to promote critical infrastructure security, including appropriate forms of information sharing, without incurring the risk of antitrust liability. Under this new legal regime, DHS will be able to give proper assurances to private-sector owners and operators of critical infrastructure that the sensitive or proprietary information that they furnish will be protected. These assurances will encourage the private sector—which is uniquely positioned to provide information about the vulnerabilities of the infrastructure it owns and operates—to share that vital information with the government. At the same time, government will ensure that such action does not diminish competition in the market place.

Creating a more effective and efficient information-sharing regime to enable our core protective missions will require further government leadership and intense collaboration between public- and private-sector stakeholders. Specific initiatives include efforts to:

Define protection-related information sharing requirements and establish effective, efficient information sharing processes

One of the first steps we must take is to precisely define information sharing requirements as they pertain to the critical infrastructure and key asset protection mission. These requirements should focus on the sharing of real-time threat, vulnerability, and incident data; best practices; security guidelines; risk assessments; and operational procedures. DHS, in conjunction with DoJ, DoS, and other federal lead departments and agencies, will lead efforts to

establish this two-way requirements framework in collaboration with other key stakeholders, including international partners. Once requirements are determined, processes must be established to ensure that the appropriate users can access needed information in a timely manner.

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

To facilitate meaningful information exchange between the public and private sectors, we will implement the provisions of the *Act* rapidly to encourage the private sector to share sensitive security-related information and incident data. Accordingly, within the framework established by the *Act*, DHS will work with DoJ, Congress, other federal lead departments and agencies, and state lawmakers to:

- Implement appropriate protections for the private sector to share vulnerability assessments, incident reports, and other security data with government; and
- Explore appropriate mechanisms to share and exchange security-related information with our international partners.

Promote the development and operation of critical sector Information Sharing Analysis Centers

Sector-focused ISACs provide a model for public-private sector information sharing, particularly in the area of indications and warnings. Numerous critical infrastructure sectors use this structure to communicate potential risks, threats, vulnerabilities, and incident data among their constituent memberships.

ISACs generally have mechanisms in place that allow them to share many categories of relevant, sensitive information in a timely manner. Although the ISACs have proven to be a successful information sharing model thus far, their capabilities could be greatly improved, particularly with respect to developing advanced analytical capabilities. DHS and other federal lead departments and agencies will provide increased support to sector efforts to exchange security-related information via the ISACs. Additionally, DHS will work with industry to establish processes and mechanisms to help incorporate state and local government participation into the ISAC process.

Improve processes for domestic threat data collection, analysis, and dissemination to state and local government and private industry

Our intelligence community has longstanding processes for collection, analysis, and dissemination of information on threats to our national security interests. We must establish similar collection and assessment processes are needed to integrate information from all sources in the context of domestic critical infrastructure and key asset protection.

Additional processes must be put in place to ensure that state and local law enforcement and infrastructure and key asset owners and operators have full and timely access to needed information, including assessments of terrorist organization tactics, techniques, and procedures; assessments of terrorist capabilities and motivations; lessons learned from terrorist operations in other countries; and the comprehensive mapping of these products to sector vulnerabilities.

DHS, in collaboration with the intelligence community and the DoJ, will develop comprehensive threat collection, assessment, and dissemination processes that integrate intelligence and law enforcement capabilities relevant to the domestic protection mission. They will also develop processes to ensure that the results of this fusion of relevant intelligence and law enforcement data are disseminated to the appropriate stakeholders in a timely manner. This includes exploring ways to expedite the conduct of necessary background checks and issuance of security clearances to those with a need to know.

Support the development of interoperable secure communications systems for state and local governments and designated private sector entities

DHS will enlist the assistance of experts from NIST, the Department of Defense (DoD), and other appropriate organizations to develop technical systems for the sharing of sensitive information and then help state and local governments acquire access to them.

Complete implementation of the Homeland Security Advisory System

The Homeland Security Advisory System was implemented in early 2002. DHS will continue to work with other federal departments and agencies, state and local governments, and the private sector to interpret, harmonize, and identify appropriate actions that correspond to the various threat levels included in this system as they relate to their particular assets and operations.

PERSONNEL SURETY, BUILDING HUMAN CAPITAL, AND AWARENESS

Domestic security starts in our communities, in our own institutions, and in our businesses. Those who have access to and operate our critical infrastructures and key assets are crucial to our national protective scheme. The key issues impacting personnel surety, building human capital, and awareness encompass four main areas:

- Developing safeguards to prevent an insider or a disaffected or co-opted employee from conducting sabotage activities or facilitating terrorist access to a critical facility or system;
- Recruiting and training more skilled operations and security personnel to protect our critical infrastructures and key assets;
- Assuring that these workers are secure while doing their jobs; and
- Implementing communication and awareness programs to help businesses and communities take action to protect their respective assets and manage risk constructively.

Personnel Surety

The September 11 attacks demonstrated that terrorist organizations possess the capability to conduct long-term clandestine operations, with individual members blending into daily life in the United States. The "insider threat" is becoming an increasingly serious concern for critical infrastructure and key asset protection across all sectors. An "insider" is defined as an employee or anyone else who has routine access to critical facilities and systems. This group also includes contractors, temporary help, and outsourcers. Insiders, because of their access and positions of trust, can intentionally or unwittingly become terrorist surrogates by disclosing information relevant to critical nodes, vulnerabilities, operating characteristics, or security measures. They can also provide terrorists with direct access to and mobility within critical facilities and systems, such as operations centers and control rooms.

Building Human Capital

Related to personnel surety is the fundamental need to ensure that trustworthy, reliable, and trained personnel are available to protect critical infrastructures and key assets from terrorist attack. Private sector owners and operators depend on skilled employees to accomplish the protection mission. Security personnel and first responders, in particular, require adequate training, equipment, and other support to carry out their responsibilities effectively and with some degree of assurance that their personal security will not be in jeopardy while accomplishing their mission.

Awareness

A state of sustained preparedness requires widespread consciousness among members of the public—especially among those in government and the private sector most directly affected—of the scope and nature of the threat we face and the precautions we must take to meet the threat. The federal government, working with the private sector, has been engaged for several years in a systematic program to develop protection awareness among key business leaders in the critical sectors. This effort, which has increased significantly since September 11, has been especially productive. Additionally, the scope of the attacks themselves and the extensive publicity they engendered (e.g., congressional hearings and media coverage) have significantly raised public consciousness of the terrorist threat. This level of awareness must be sustained over the long term for our national protective effort to be truly successful.

Personnel Surety, Building Human Capital, and Awareness Challenges

Time-efficient, thorough, and periodic background screening of candidate employees, visitors, permanent and temporary staff, and contractors for sensitive positions is an important tool for protecting against the "insider threat." Unfortunately, in-depth personnel screening and background checks are often beyond the capabilities of private sector and non-federal government entities. Private employers also lack access to personnel reliability data—often in the possession of the federal government—that could help determine whether employees, contractors, and visitors should be employed at or allowed access to sensitive facilities. Part-time, temporary, and seasonal workers also challenge effective background screening processes because of the high level of employee turnover. Other challenges include concern for constitutional freedoms, costs associated with screening processes, and a lack of verifiable documentation and other sources of information.

Aside from personnel surety, shortages of skilled personnel in various professions—ranging from security technicians to emergency first responders—also impede critical infrastructure and key asset protection. Similarly, although private security officers are identified as an important source of protection for critical facilities, few formal standardized qualifications, training, or certification requirements exist for these positions across the critical sectors. Given the dynamic nature of the terrorist threat, there is an urgent need for ongoing training of security personnel to sustain skill levels and to remain up-to-date on evolving terrorist weapons and tactics.

Protection of employees from the terrorist threat or exposure to the potential aftereffects of an attack is an important concern for critical infrastructure and key asset owners and operators. They are also potential disincentives for their employees, security personnel, and first responders. Future attacks could result in biological, chemical, or radiological contaminants at an incident site that, without proper precautions, could endanger emergency workers, their families (by cross-contamination), and others in the exposed areas.

Despite the events of September 11, awareness of the implications of terrorist threats to critical infrastructures among members of industry in general remains relatively low. As time passes and focus on the events of that day recedes, the awareness and interest of the general public also recedes. As a result, security-related activities could lack the consistent focus required to assure protection, thus leaving us exposed once more.

Personnel Surety, Building Human Capital, and Awareness Initiatives

To overcome the challenges described above, we will:

Coordinate the development of national standards for personnel surety

DHS, in concert with DoJ, will convene an advisory task force to perform a comprehensive review of critical infrastructure sector personnel surety programs. The task force—to be comprised of federal agencies and departments, state and local governments, and private sector representatives—will develop advice on the creation of national standards and capabilities for background checks, screening, criminal investigations, and positive identification of key personnel employed in critical service sectors.

Harmonizing personnel surety policies and programs among critical infrastructure sectors will help create uniform standards and address concerns articulated by businesses regarding the adequacy of background checks for occupants of critical job categories. In developing national standards for personnel surety, however, we must find the balance that enables us to mitigate risk and defend our country while preserving individual freedoms and liberties.

Develop a certification program for background-screening companies

To complement private-sector employer efforts, DHS, in concert with DoJ, will develop a certification program for background-screening companies to ensure a base-line level of competence and reduce obstacles to timely and accurate verification of employee backgrounds and investigative histories.

In addition, DHS will initiate a study to identify options for creating or enabling access to databases to accredit candidates for critical positions and other potential hires, contract workers, and key service supplier personnel. Federal databases, such as those operated by the Immigration and Naturalization Service and various intelligence and law enforcement agencies, could be used to seed this process. As we undertake this effort, we must take the precautions necessary to protect individual constitutional freedoms.

Explore establishment of a certification regime or model security training program for private security officers

To maximize the effectiveness of the Nation's corps of private security personnel, DHS will work with law enforcement and federal security officials to initiate a dialogue with state and local counterparts,

private-sector infrastructure owners and operators, and private security firms concerning the creation of a training and certification regime for private security officers. One possible model is the program for security training provided by the federal law enforcement academies.

Identify requirements and develop appropriate programs to protect critical personnel

DHS will work with state and local government and industry representatives to identify requirements and develop appropriate programs to protect critical personnel who may become terrorist targets because of their roles in protection activities.

Security and first responder personnel must be assured of their own personal safety while engaging in their protection and response missions. These personnel may need to be equipped with the protective devices and clothing necessary to shield them from toxic or biological contamination and impede the transmission of potentially dangerous agents to others. In this regard, personal protective equipment must be developed with the needs of law enforcement and other first responders uppermost in mind across the critical infrastructure sectors. Programs must be implemented to ensure that security personnel and first responders receive protection training and education necessary for them to carry out their responsibilities.

Facilitate the sharing of public- and private-sector protection expertise

DHS, in concert with other federal lead departments and agencies, will develop a program to facilitate the sharing of protection expertise between the public and private sectors.

Training and exercises that test protection plans and personnel capabilities are critical to assessing required improvements in preparedness and sharing best practices. Accordingly, DHS will also develop and incorporate realistic hands-on and virtual exercises into its critical infrastructure and key asset protection education and training programs with the objective of exploring common protection issues and solutions. With proper design, these exercises can serve important outreach, training, coordination, and evaluation purposes across the public and private sectors.

Develop and implement a national awareness program for critical infrastructure and key asset protection

DHS, in concert with other key stakeholders, will identify and assess the requirements for a comprehensive, national awareness program that will support sustainability of preparedness programs, security investment, and protection activities, as well as the public's understanding of the terrorist threat environment.

Building awareness means creating a national appreciation for how security must be fundamentally incorporated into our daily lives and business operations. Our national awareness program should focus on the specific needs of the critical infrastructure industries to support informed private-sector decisions and enable the planning of relevant and effective protection strategies and resource allocation.

It must also be sufficiently comprehensive in scope to maintain the public's understanding and appreciation of the threat environment as it evolves and foster confidence in the strategies and approaches being taken to address it.

TECHNOLOGY AND RESEARCH & DEVELOPMENT

The terrorist threat challenges us to marshal our nation's advantages in the sciences and technology. Protecting our Nation's critical infrastructures and key assets against this threat will require a systematic, national effort to fully harness our research and development (R&D) capabilities. Doing so will enable us to meet many of our immediate needs for protective standards and solutions. It will also help lay the long-term foundation for developing the advanced tools and technologies that will enable more comprehensive and cost-effective protection solutions in the future, particularly regarding the most catastrophic threats we may have to confront.

Organizing this national effort will require persistence, careful planning, and coordination. Our national research enterprise is vast and complex. Private companies, universities, research institutions, and government laboratories of all sizes are conducting pure and applied research to develop the advanced materials, products, and services that will contribute to assuring the protection of critical infrastructures and key assets.

To best realize these advances, however, we must be able to identify needs—standards, tools, and processes—that span multiple sectors as a critical first step. Accomplishing this will enable us to establish research priorities and concentrate efforts and assign responsibilities in these areas while avoiding unnecessary duplication that can draw valuable capacity away from other needed research. It will also provide researchers, engineers, and infrastructure owners and operators with a minimum threshold of capabilities to guide product development efforts and provide end users a metric to gauge the sufficiency of the technological solutions they adopt.

Technology and Research & Development Challenges

The number and diversity of stakeholders present impediments to coordinating technological R&D activities for critical infrastructure and key asset protection. Organizations at each level of government and across the critical infrastructure sectors all have individual R&D priorities and interests intended to identify solutions to the particular problems they consider most important. One major challenge at the outset is to define the points of commonality among these disparate needs and efforts to determine where coordinated R&D activities will yield value across the broadest range of interests.

At the national level, the general lack of focus on long-term research, development, testing, and engineering for critical infrastructure and key asset protection is a significant shortfall in our current domestic protection posture. A need exists for a process to coordinate, with broad sector input, the creation and adoption of national research priorities, and support to cross-sector R&D activities.

In addition, our domestic protection requirements create a demand for new tools to contribute to security at the operational level. In this regard, we must work to improve our capability to conduct a wide range of tests on potential contaminants (e.g., biological, chemical, and radiological) that can be used to threaten our food and agriculture, water, mass transit, and other sectors. Similarly, we must expand our monitoring and surveillance capabilities to improve our ability to detect the presence of weapons of mass destruction and their components.

An especially great need exists for standards to support interoperable communications. The current lack of capability in this area consistently ranks as one of the most critical shortcomings in our protection and emergency response posture across the Nation. At present, federal, state, and local law enforcement personnel and fire, medical, and emergency management personnel use incompatible communications systems, introducing difficulties and barriers in information exchange and security operations. This lack of common standards in

communications equipment can seriously impede close collaboration among security personnel, first responders, state emergency management personnel, and federal officials prior to, during, and in the aftermath of a terrorist incident. Responses to terrorist incidents can be further complicated if differences in communications connectivity themselves become a target for terrorist exploitation.

The lack of reliable tools to authenticate the identities of personnel with direct access to our most critical facilities and systems also impedes security across sectors. A similar situation exists with respect to identification of law enforcement, fire, and emergency response personnel working in protection and incident response roles.

Finally, harmonizing the oftentimes conflicting need to enhance security while simultaneously maintaining reasonably open channels of commerce requires both new tools and processes that challenge technology. For example, critical dams, particularly those on navigable waterways, present difficult security challenges. The locks on such dams must remain available for the flow of commerce, yet waterborne threats must be abated. Other sectors such as air transportation, rail and maritime shipping, and site security at major commercial and government buildings, national landmarks, and the like present similar needs for effective, non-invasive monitoring and sensor capabilities.

Technology and Research & Development Initiatives

To respond to these challenges, government and industry must work together to develop standards in security technology for both physical and information infrastructures. Such standards would enable key stakeholders to collaborate more effectively to develop the products essential to enhancing the security of infrastructures and managing the interdependencies among them.

Accordingly, we will:

Coordinate public- and private-sector security research and development activities

DHS will coordinate with other appropriate federal agencies to support security technology research and development, including specialized pilot programs and projects. This effort will include exploration of mechanisms to migrate technologies developed by the DoD and other government agencies to the private sector for use in infrastructure protection. Activities in this area will include appropriate collaboration with our international partners to expand our research base and capitalize on technological solutions being developed by our friends and allies.

Coordinate interoperability standards to ensure compatibility of communications systems

We will act to establish and disseminate interoperability standards to ensure compatibility of communications systems used by federal, state, and local authorities. The Federal Communications Commission (FCC), will lead this effort, working in concert with DHS, other federal lead departments and agencies such as DOC's National Telecommunications and Information Administration, other standard-setting bodies such as NIST, affected user groups, and equipment manufacturers. Establishment of standards will enable secure and assured interoperable communications among all levels of homeland security entities. Standardized communication systems will enhance protection and incident response, as well as promote efficient planning and training at all levels.

Explore methods to authenticate and verify personnel identity

We must provide better means of identifying people in order to increase the security of our critical facilities, systems, and functions. We must create a uniform means of identifying law enforcement and security personnel and individuals with access to critical facilities and systems.

Technologies to be examined for this authentication scheme include biometric identifiers, magnetic strips, microprocessor-enabled "SMART" cards, and other systems. Such tools would enable quick authentication of identities in the protection and emergency response domains. The enhanced "scene control" entailed would facilitate investigations at the sites of terrorism incidents, and create an investigative baseline for comparing different analytical data.

Improve technical surveillance , monitoring and detection capabilities

We must improve our technical surveillance, detection (including non-invasive inspection methods), and monitoring systems for perimeter, entry area, and key node vigilance. We must also develop more robust detection systems for use by security personnel across our critical infrastructure sectors.

DHS, in collaboration with other public- and private-sector stakeholders, will develop a research agenda to explore technical solutions to surveillance and detection deficiencies in critical sectors, to include capabilities to detect chemical, biological, and radiological (CBR) residues.

MODELING, SIMULATION, AND ANALYSIS

Modeling, simulation, and analysis activities help to prioritize critical infrastructures and key assets protection activities and investments. This *Strategy* has discussed the challenges and uncertainties presented by critical nodes and single-points-of-failure within infrastructures, as well as increasing interdependencies that exist among the various infrastructure sectors both nationally and internationally. These interdependencies and key nodes are often difficult to identify and resolve, as are the cascading and cross-sector effects associated with their disruption. Properly employed, modeling, simulation, and analysis can provide valuable, predictive insights into potential consequences that could result from these dependencies and interdependencies in various threat scenarios.

Modeling, simulation, and analysis can also facilitate protection planning and decision support by enabling the mapping of complex interrelationships among the elements that make up the risk environment. For example, modeling traffic patterns through a particular junction, such as rail or air traffic through a key railhead or air terminal, allows analysis of the various possible outcomes of an attack on that node at various points in time. Such information would be helpful in drawing attention to likely cascading consequences that otherwise might have gone unconsidered.

Using models and simulations, responsible authorities can evaluate the risks associated with particular vulnerabilities more accurately and subsequently make more informed protection decisions. Modeling and simulation can also be used as a real-time decision support tool to help mitigate the effects of an attack or avert a secondary attack altogether.

Private-sector infrastructure and asset owners and operators possess considerable experience in preparing for and responding to a wide variety of naturally occurring events like floods, earthquakes, and hurricanes. Their expertise in planning and response stems from long histories of contending with the challenges associated with these naturally occurring phenomena. In contrast, the pervasive threat of terrorist strikes against our critical infrastructures and key assets is relatively new. Hence, no similar long-term data exist that track the patterns of such deliberate incidents; nor is there evidence as to which safeguards would be most effective, making the need to develop reliable, predictive surrogate data even more important.

Modeling, Simulation, and Analysis Challenges

Historically, we have relied on modeling, simulation, and analysis capabilities to enable decision support and planning activities related to national defense and intelligence missions. We must now find ways to employ them to develop creative approaches and enable complex decision support, risk management, and resource investment activities to combat terrorism at home.

Modeling, simulation, and analysis would provide significant value to many sectors across government and the economy. Demands for such studies will likely be great; and, as in the case of R&D planning, we will have to establish priorities among the projects to be undertaken, giving emphasis to those studies that are likely to yield common benefits and address the most stressing threats and vulnerabilities.

Improving our modeling and simulation resources must also include an effort to enhance data collection and standardization. Currently, much data relevant to national-level protection activities may not exist, be accessible, or reside in a standard format. Data collection processes, systems, and standards will have to be created and adopted to provide common representations of data across models and simulations.

Furthermore, enhancing our national modeling, simulation, and analysis capabilities will require a unified effort across the public and private sectors to yield the results needed in the most efficient and cost-effective manner possible. Through effective partnering across the federal interagency community, state and local government, national laboratories, academia, and commercial enterprises, we can enlist tremendous talents and resources to drive this capability forward. Cross-sector collaboration is also essential to establishing standard methodologies and consistent analytical frameworks for interpreting research results, especially when modeling infrastructure interdependencies.

Most industry officials have a fairly complete understanding of their own operations and associated vulnerabilities. However, many of these enterprises require assistance to identify their dependencies on other sectors and the degree of risk to which they are exposed as a function of those interdependencies. The potential impact of such interdependencies hit home for the banking and financial services sector on September 11, when the collapse of the World Trade Center towers interrupted telecommunications services in lower Manhattan. The disruption brought electronic financial transactions to a halt, with long-term economic impacts still being felt more than a year later.

In most cases, modeling and simulation capabilities are not well integrated into existing infrastructure protection planning activities. Achieving this integration will be critical to the task of translating modeling and simulation research data into effective guides for sector-focused protection planning, decision support, and resource allocation.

Modeling, Simulation, and Analysis Initiatives

Modeling, simulation, and analysis initiatives that we will pursue across the critical infrastructure sectors include efforts to:

Integrate modeling, simulation, and analysis into national infrastructure and asset protection planning and decision support activities

DHS will establish an advisory panel consisting of representatives from the public and private sectors, national laboratories, academia, and commercial research organizations to explore alternatives to integrate modeling and simulation activities into domestic protection planning.

The panel will be charged to review modeling, simulation, and analysis and advise DHS on ways to focus on-going and planned research activities on national priorities. Early in the process, emphasis will be given to developing and disseminating standards and methods for modeling sector interdependencies. Such standards will be based on a clear definition of assets or services deemed to be critical and will be tasked for development through nationally coordinated planning activities overseen by DHS.

Develop economic models of near- and long-term effects of terrorist attacks

The economic significance of terrorist attacks is not always clear, with short-term effects often only partially predictive of longer-term realities. Models of the temporal and cross-sector scope of economic damage caused by physical infrastructure attacks would assist policymakers and emergency management specialists in understanding and mitigating worst case effects.

Develop critical node/chokepoint and interdependency analysis capabilities

Fundamental to the core objective of modeling interdependencies and mapping the consequences of particular terrorist events, we will also undertake research to develop metrics for gauging the adequacy of infrastructure subsystems and key nodes compared to level of threat and effect. This includes comparing the robustness of different infrastructures at points where key centers or critical nodes are in close proximity to one another and can have cascading effects if attacked. Clearly identifying and addressing interdependencies among critical infrastructures in both a national and international context is high on our list of protection priorities.

Model interdependencies among sectors with respect to conflicts between sector alert and warning procedures and actions

Modeling alert responses and possible counterproductive effects of alert system designs will enhance flexibility and minimize duplication of effort. The intent of raising the Homeland Security Alert status is to trigger actions to protect infrastructures and make it more difficult for terrorists to act. These actions, however, may have disruptive consequences that may themselves interact in ways that could create additional vulnerabilities.

Conduct integrated risk modeling of cyber and physical threats, vulnerabilities, and consequences

Risk assessments help to identify and determine ways to manage risk to best allocate resources. These assessments include threat analysis to provide a baseline and frame of reference for risk management and investment decisions. This analysis, coupled with vulnerability assessments to determine the effectiveness of security systems and tools to provide consequence analysis, will provide information on critical assets and nodes. Such studies would comprise models of security incidents involving various types of both cyber and physical attacks. Analysis will focus on the complex interactions between physical and cyber systems to determine the full range of potential consequences and to ensure the applicability of findings across infrastructures in both a domestic and international context.

Develop models to improve information integration

The integration of threat and vulnerability information between sectors needs to be modeled, as does information sharing between the federal government and critical infrastructures, to identify points of inefficiency and information loss.