SECURING CRITICAL INFRASTRUCTURES

Our society and modern way of life depend on a complex system of critical infrastructures. The *National Strategy for Homeland Security* has identified 13 critical sectors. As we learn more about threats, means of attack, and the various criteria that make targets lucrative for terrorists, this list will evolve. The critical infrastructure sectors consist of agriculture and food, water, public health, emergency services, government,[1] the defense industrial base, information and telecommunications,[2] energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping.[3] Common issues of concern to these sectors are described in the *Cross-Sector Security Priorities* chapter of this strategy.

For each critical sector, this chapter discusses:

- Unique characteristics of the infrastructure sector itself and the industry that supports it;
- Current efforts that are underway to protect sector-specific goods and service delivery and associated critical assets, systems, and functions;
- Unique protection challenges; and
- Priority protection action areas for the sector to address in a collaborative fashion.

Consistent with the principles of this *Strategy*, any initiatives involving significant federal resources will be prioritized across the critical sectors, taking into account the risks and consequences of potential threats and the proper sharing of protection responsibilities among the various stakeholders.

---

1 The primary focus of this *Strategy* is the physical protection of critical infrastructures and key assets. Each lead federal department and agency has developed a continuity of operations plan (COOP) to ensure the continuity of government (COG) for its sector. As these plans are classified, COG will not be discussed in this document.

2 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.

3 The protection of National Monuments and Icons is addressed in Chapter VII, "Protecting Key Assets."

AGRICULTURE AND FOOD

From farm to table, our Nation's agriculture and food systems are among the most efficient and productive in the world. These industries are a source of essential commodities in the U.S., and they account for close to one-fifth of the Gross Domestic Product. A significant percentage of that figure also contributes to our export economy, as the U.S. exports approximately one quarter of its farm and ranch products.

The Agriculture and Food Sectors include:

- The supply chains for feed, animals, and animal products;
- Crop production and the supply chains of seed, fertilizer, and other necessary related materials; and
- The post-harvesting components of the food supply chain, from processing, production, and packaging through storage and distribution to retail sales, institutional food services, and restaurant or home consumption.

Changes in the ways that food is produced, distributed, and consumed present new challenges for ensuring its safety and security. More of our food is grown abroad, many foods are transported long distances, and we eat away from home more frequently. Public confidence in the safety of agricultural and food-processing and packaging systems represents a key part of sustaining the economic viability of these sectors. America's reputation as a reliable supplier of safe, high quality foodstuffs is likewise essential to maintaining the confidence of foreign customers who are important to the national economy as a whole.

The United States has a strong, well functioning food-safety system to protect the public against unintentional contamination of food products. Besides the agriculture and food industries' measures to ensure food safety, the overall mechanism includes extensive analyses of critical control points in the food supply chain and federal, state, and local inspections of food processing and storage facilities, as well as food service establishments. Sector enterprises are currently in the process of assessing physical security practices and procedures in place at their facilities, particularly processing plants.

Agriculture and Food Sector Challenges

The fundamental need for food, as well as great public sensitivity to food safety makes assuring the security of food production and processing a high priority.

Our food and agriculture industries have been developed over several decades and are unique with respect to their structures and processes. The greatest threats to the food and agricultural systems are disease and contamination, in which case, sector decentralization represents a challenge to assuring their protection. Government and industry have worked together in the past to deal with isolated instances of deliberate food tampering. The effectiveness of the food safety system with regard to preventing, detecting, and mitigating

the effects of unintentional or isolated contaminations offers a foundation to build upon for countering deliberate acts to corrupt the food supply.

Because of the food system's many points of entry, detection is a critical tool for securing the agriculture and food sectors. There is an urgent need to improve and validate analytical methods for detecting bioterrorist agents in food products, as well as a need for enhanced laboratory capabilities and capacities. The existing system of federal, state, and local public health and agriculture laboratories was established to detect the presence of traditional human pathogens that occasionally and unintentionally contaminate foods. Although this system continues to serve an important role in safeguarding public health from these traditional agents, its capabilities must be enhanced to enable protection from a wide spectrum of nontraditional agents. This enhanced system must also be capable of eliminating the occurrence of false positives for threat agents in food and agricultural products in addition to inconsistencies in detecting them when they are present.

Additionally, we must expand our system of laboratories to accommodate the requirements that could result from a bioterrorist attack on the food supply. We must also increase the number of qualified personnel (veterinarians and lab technicians) and laboratories with the ability to diagnose and treat animal disease outbreaks and crop contamination. Moreover, many state budgets for such inspection, detection, and training protocols will need to be revisited to provide for such initiatives.

Moving and processing crops and animals require transporting them over long distances. During transport, these resources spend time in storage areas and facilities where they may come in contact with other products. Accordingly, the agriculture and food sectors depend on transportation system owners and operators, particularly regarding trucks and containers, to meet the safety and security standards necessary to protect food products in transit. We must improve mechanisms designed to track the movement of animals and commodities in transit and enable officials to pinpoint where an outbreak or contamination originates.

Rapid acquisition and use of threat information could help to prevent an attack from spreading beyond individual facilities or local communities to become a regional or national problem. Unfortunately, serious institutional barriers and disincentives for sharing such information exist within the sectors and their structures. For instance, there are significant, direct economic disincentives associated with reporting problems or suspected contamination in food processing.

Meanwhile, the agriculture and food markets are highly competitive, and many parts of the food system operate within slim profit margins. As a result, some companies may be more likely to hold onto information related to incidents involving suspected contamination in order to prevent the potential financial consequences of what might be a false alarm.

Protecting the public from an outbreak or contamination incident requires timely reporting of information for prompt decision-making and action. In the current environment, when crops or animals must be culled or preventively killed to deal with disease or contamination, the fear of a negative public response and attendant economic implications to the sector may impede the needed levels of response in the agriculture and food sectors.

Deliberate contaminations by terrorists aim to harm people or animals to the greatest extent possible. Another principal objective is to create panic and inflict economic damage. Because of the influence the media has on how the public responds to incidents, clear and accurate communication of information to news outlets is essential. Official spokespersons at state, regional, and national levels should be pre-assigned. Although food regulators routinely communicate with industry on food-safety issues, planning for public communications in the event of a deliberate contamination should also be a priority, as should defining stakeholder responsibilities within those plans.

Agriculture and Food Sector Initiatives

Information derived from assessment of sector food-safety processes and procedures can provide a foundation for developing an agriculture and food sector critical infrastructure protection system. For example, two major efforts to establish procedures for accidental outbreaks of animal disease have already been completed.[1] While plans for these studies were drafted with accidental introductions of disease or contamination in mind, their findings and recommendations may also apply to intentional acts. Another example of ongoing activities in this area is the implementation of recommendations from the 1999 Animal and Plan Health Inspection report, *Safeguarding American Plant Resources*. Further study and collaborative policy development are required to determine whether and how the food safety system could be extended to deal with food security issues.

Additional agriculture and food sector protection initiatives include efforts to:

Evaluate overall sector security and identify and address vulnerabilities

DHS and the Departments of Agriculture (USDA) and Health and Human Services (HHS), working in collaboration with state and local governments and industry, will undertake a broad risk assessment of the agriculture and food sectors to evaluate overall security and identify and address existing vulnerabilities.

Enhance detection and testing capabilities across the agricultural and food networks

DHS, USDA, and HHS, in collaboration with state and local governments and industry, will work to increase detection and testing capacity. Exploring mechanisms to improve detection capabilities, ranging from technology development to increasing the number of veterinary, epidemiology, and technical specialists at the state level, will facilitate earlier detection and response. Enhancing trace-back systems and increasing detection capabilities at borders and ports of origin will also significantly increase protection. Identifying, creating, and certifying additional laboratory capacity across the country would likewise increase the speed of analysis and response.

Assess transportation-related security risks

DHS, USDA, HHS, and the Department of Transportation (DoT) will work with representatives from the agriculture and food industries to assess security risks in food and commodity transport and develop appropriate solutions. The scope of the issues requires a thorough risk assessment integrating transportation security measures into ongoing and newly initiated countermeasures undertaken by the food industry. Additional considerations include standardizing the methods by which the agriculture and food industries report truck hijackings and cargo thefts, and then disseminating these reports within the food industry.

Identify potential infrastructure protection incentives; identify and address existing disincentives

DHS working with USDA and HHS will explore options for developing incentives or reducing disincentives to encourage the prompt reporting of problems.

Develop emergency response strategies

DHS, USDA, and HHS, working with sector counterparts, will develop a strategy to coordinate risk communications and other emergency response activities.

---

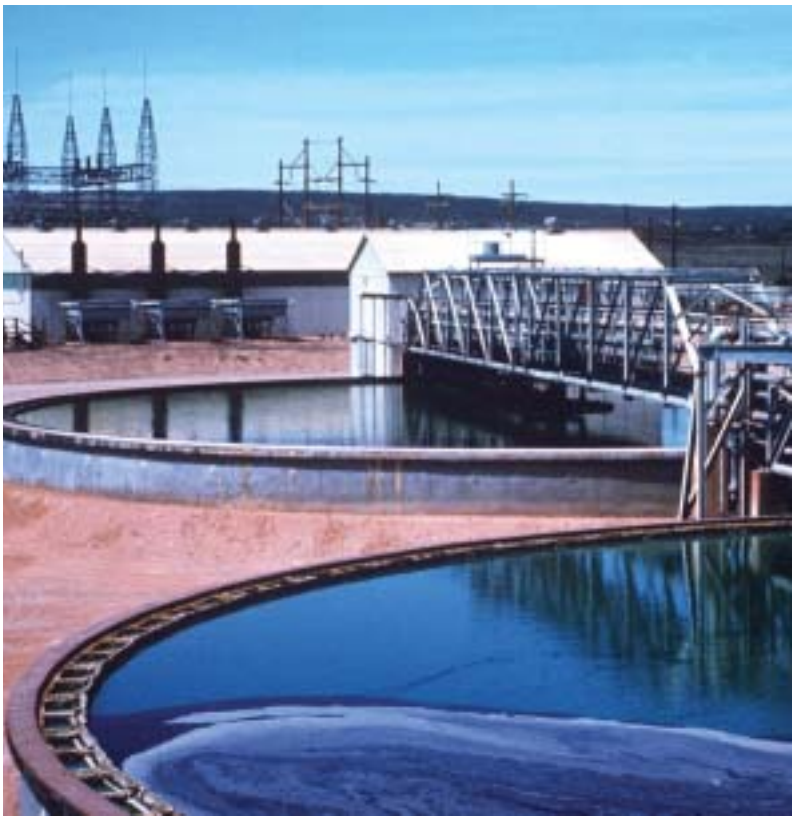
1 These efforts are reported in *The Animal Health Safeguarding Review: Results and Recommendations*, October 2001, by the National Association of State Departments of Agriculture Research Foundation, and *The U.S. National Animal Health Emergency Management System, 2001 Annual Report*.

WATER

The Nation's water sector is critical from both a public health and an economic standpoint. The water sector consists of two basic, yet vital, components: fresh water supply and wastewater collection and treatment. Sector infrastructures are diverse, complex, and distributed, ranging from systems that serve a few customers to those that serve millions. On the supply side, the primary focus of critical infrastructure protection efforts is the Nation's 170,000 public water systems. These utilities depend on reservoirs, dams, wells, and aquifers, as well as treatment facilities, pumping stations, aqueducts, and transmission pipelines. The wastewater industry's emphasis is on the 19,500 municipal sanitary sewer systems, including an estimated 800,000 miles of sewer lines. Wastewater utilities collect and treat sewage and process water from domestic, commercial, and industrial sources. The wastewater sector also includes storm water systems that collect and sometimes treat storm water runoff.

The water sector has taken great strides to protect its critical facilities and systems. For instance, government and industry have developed vulnerability assessment methodologies for both drinking water and wastewater facilities and trained thousands of utility operators to conduct them. In response to the *Public Health Security and Bioterrorism Preparedness and Response Act of 2002*, the Environmental Protection Agency (EPA) has developed baseline threat information to use in conjunction with vulnerability assessments. Furthermore, to defray some of the cost of those studies, the EPA has provided assistance to drinking water systems to enable them to undertake vulnerability assessments and develop emergency response plans.

To improve the flow of information among water-sector organizations, the industry has begun development of its sector-ISAC. The Water ISAC will provide a secure forum for gathering, analyzing, and sharing security-related information. Additionally, several federal agencies are working together to improve the warehousing of information regarding contamination threats, such as the release of biological, chemical, and radiological substances into the water supply, and how to respond to their presence in drinking water. With respect to identifying new technologies, the EPA has an existing program that develops testing protocols and verifies the performance of innovative technologies. It has also initiated a new program to verify monitoring technologies that may be useful in detecting or avoiding biological or chemical threats.



Water Sector Challenges

The basic human need for water and the concern for maintaining a safe water supply are driving factors for water infrastructure protection. Public perception regarding the safety of the Nation's water supply is also significant, as is the safety of people who reside or work near water facilities. In order to set priorities among the wide range of protective measures that should be taken, the water sector is focusing on the types of infrastructure attacks that could result in significant human casualties and property damage or widespread economic consequences. In general, there are four areas of primary concentration:

- Physical damage or destruction of critical assets, including intentional release of toxic chemicals;
- Actual or threatened contamination of the water supply;
- Cyber attack on information management systems or other electronic systems; and
- Interruption of services from another infrastructure.

To address these potential threats, the sector requires additional focused threat information in order to direct

investments toward enhancement of corresponding protective measures. The water sector also requires increased monitoring and analytic capabilities to enhance detection of biological, chemical, or radiological contaminants that could be intentionally introduced into the water supply. Some enterprises are already in the process of developing advanced monitoring and sampling technologies, but additional resources from the water sector will likely be needed. Environmental monitoring techniques and technologies and appropriate laboratory capabilities require enhancement to provide adequate and timely analysis of water samples to ensure early warning capabilities and assess the effectiveness of clean-up activities should an incident occur. Specific innovations needed include new broad-spectrum analytical methods, monitoring strategies, sampling protocols, and training.

Approaches to emergency response and the handling of security incidents at water facilities vary according to state and local policies and procedures. With regard to the public reaction associated with contamination or perceived contamination, it is essential that local, state, and federal departments and agencies coordinate their protection and response efforts. Maintaining the public's confidence regarding information provided and the timeliness of the message is critical. Suspected events concerning water systems to date have elicited strong responses that involved taking systems out of service until their integrity could be verified, announcing the incident to the public, and issuing "boil water" orders.

The operations of the water sector depend extensively on other sectors. The heaviest dependence is on the energy sector. For example, running pumps to move water and wastewater and operating drinking water and wastewater treatment plants require large amounts of electricity. To a lesser extent, the water sector also depends on the transportation system for supplies of water treatment chemicals, on natural gas pipelines for the energy used in some operational activities, and on the telecommunications sector. Water and wastewater systems are increasingly automated and controlled from remote locations for efficiency.

Water Sector Initiatives

Water infrastructure protection initiatives are guided both by the challenges that the water sector faces and by recent legislation.[1] Additional protection initiatives include efforts to:

Identify high-priority vulnerabilities and improve site security

EPA, in concert with DHS, state and local governments, and other water sector leaders, will work to identify processes and technologies to better secure key points of storage and distribution, such as dams, pumping stations, chemical storage facilities, and treatment plants. EPA and DHS will also continue to provide tools, training, technical assistance, and limited financial assistance for research on vulnerability-assessment methodologies and risk-management strategies.

Improve sector monitoring and analytic capabilities

EPA will continue to work with sector representatives and other federal agencies to improve information on contaminants of concern and to develop appropriate monitoring and analytical technologies and capabilities.

Improve sector-wide information exchange and coordinate contingency planning

DHS and EPA will continue to work with the sector coordinator and the water ISAC to coordinate timely information on threats, incidents, and other topics of special interest to the water sector. DHS and EPA will also work with the sector and the states to standardize and coordinate emergency response efforts and communications protocols.

Work with other sectors to manage unique risks resulting from interdependencies

DHS and EPA will convene cross-sector working groups to develop models for integrating priorities and emergency response plans in the context of interdependencies between the water sector and other critical infrastructures.

---

1 On June 12, 2002, President Bush signed the *Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act)* into law. The *Bioterrorism Act* requires many drinking water systems to conduct vulnerability assessments, certify and submit copies of their assessments to EPA, and prepare or revise their emergency response plans.

PUBLIC HEALTH

The public health sector is vast and diverse. It consists of state and local health departments, hospitals, health clinics, mental health facilities, nursing homes, blood-supply facilities, laboratories, mortuaries, and pharmaceutical stockpiles.

Hospitals, clinics, and public health systems play a critical role in mitigating and recovering from the effects of natural disasters or deliberate attacks on the homeland. Physical damage to these facilities or disruption of their operations could prevent a full, effective response and exacerbate the outcome of an emergency situation. Even if a hospital or public health facility were not the direct target of a terrorist strike, it could be significantly impacted by secondary contamination involving chemical, radiological, or biological agents.

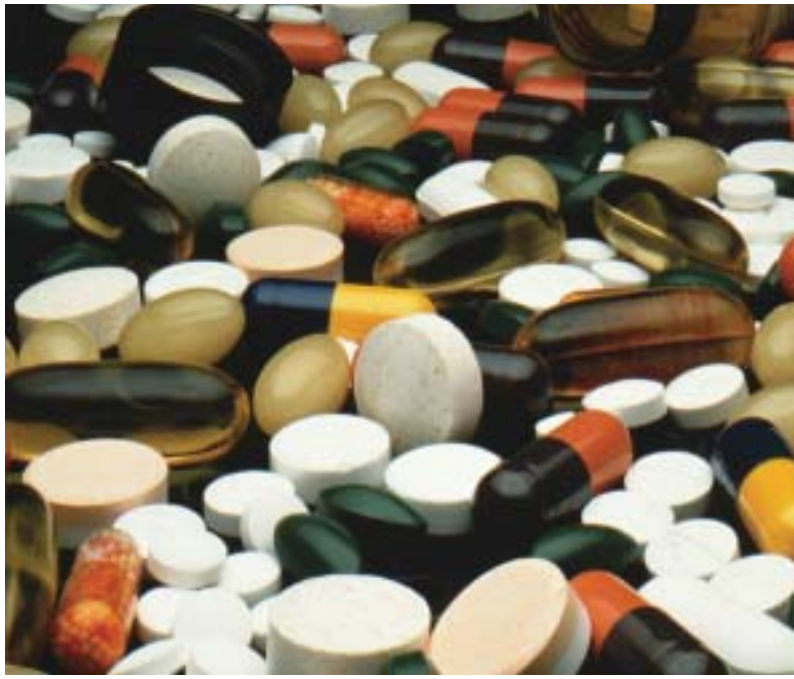
In addition to established medical networks, the U.S. depends on several highly specialized laboratory facilities and assets, especially those related to disease control and vaccine development and storage, such as the HHS Centers for Disease Control and Prevention, the National Institutes of Health, and the National Strategic Stockpile.

Public Health Sector Challenges

Public health workers are accustomed to placing themselves in harm's way during an emergency. They may be unlikely, however, to view themselves as potential targets of terrorist acts.

Most hospitals and clinics are freely accessible facilities that provide the public with an array of vital services. This free access, however, also makes it difficult to identify potential threats or prevent malicious entry into these facilities. This fact, combined with a lack of means and standards to recognize and detect potentially contaminated individuals, can have an important impact on facility security and emergency operations.

Another significant challenge is the variation in structural and systems design within our hospitals and clinics. On one hand, so-called "immune buildings" have built-in structural design elements that help prevent contamination and the spread of infectious agents to the greatest extent possible. Such features include controlled airflow systems, isolation rooms, and special surfaces that eliminate infectious agents on contact. At the other extreme are buildings with relatively little built-in environmental protection. Protection of this category of facility presents the greatest challenge.



During an epidemic, infectious individuals who continue to operate in the community at large may pose a significant public health risk. The sector needs to develop comprehensive protocols governing the isolation of infectious individuals during a crisis.

Additional public health sector challenges relate to the maintenance, protection, and distribution of stockpiles of critical emergency resources. Currently, other than the National Strategic Stockpile, there are limited resources for rotating and replenishing supplies of critical materials and medicines. Supply chain management for medical materials also requires greater attention to ensure secure and efficient functioning during an emergency. Potential solutions to these problems are impacted by complex legal and tax issues. Currently, the federal government has only limited regulatory authority to request information from companies concerning their available inventory of medical supplies and their capacity to produce them. Since pharmaceutical companies are taxed on their product inventories, they try to avoid stockpiling finished goods and meet demand through "just-in-time" manufacturing.

Sector-specific legal and regulatory issues also tend to impede the effective protection of assets and services. The *Emergency Medical Treatment and Active Labor Act* requires hospitals to treat patients requiring emergency care regardless of their insurance status. Disaster

situations involving mass casualties tax the resources of critical facilities in terms of manpower, medical supplies, and space. As patients are stabilized, it is often necessary to transfer them to other hospitals to free up critical resources for newly arriving casualties. With respect to disaster victims without insurance, however, once treatment is no longer an emergency, hospitals are not bound to treat them. As a result, many second-tier, noncritical hospitals will not or cannot accept uninsured patients, thereby requiring the critical hospital by default to continue nonemergency treatment. Additionally, privacy rules mandated in the *Health Insurance Portability and Accountability Act* should be reviewed to determine whether they could prevent the sharing of critical data in the event of an epidemic.

Existing security challenges have focused the public health sector on assessing its ability to deliver critical services during a crisis. Many hospitals, however, are faced with operating at limited profit margins and, therefore, have difficulty making appropriate security investments.

Finally, specialized medical and pharmaceutical laboratories merit special attention—particularly those handling highly toxic or infectious agents. These facilities are mission-critical with respect to identifying hazardous agents should an attack or outbreak occur. These facilities also enable the containment, neutralization, and disposal of such hazardous materials. Overcoming the protection challenges associated with securing these specialized assets is a top priority.

Public Health Sector Initiatives

Public health sector protection initiatives include efforts to:

Designate trusted communicators

HHS will work with state and local public health officials to identify, appoint, train, and prepare recognized subject matter experts to speak on behalf of the public health sector in times of crisis. These appointees would act as important envoys of homeland security information to communicate consistent, accurate information, as well as to inform, instruct, and reassure the American public. Additionally, HHS leaders will be prepared to play substantial roles at the national level in communicating with the public regarding risks associated with bioterrorism or other public health emergencies.

Review mission critical operations, establish protection priorities, and ensure adequate security and redundancy for critical laboratory facilities and services

HHS will work with hospitals and clinics in the public health sector to review their mission-critical systems and operations and help them create detailed plans to focus security investments and increase their protection. In partnership with state health departments, HHS and DHS will identify and prioritize national-level critical hospitals and medical centers, as well as their most important component facilities, systems, and services.

HHS and DHS will work with the health care sector to ensure that key laboratory facilities are protected and have adequate redundancy with respect to critical capabilities and data systems.

Enhance surveillance and communication capabilities

HHS will assist public health sector officials to identify requirements for robust surveillance systems and coordinate links between public health monitoring facilities and healthcare delivery systems.

Develop criteria to isolate infectious individuals and establish triage protocols

HHS will work with state and local health officials to develop isolation and quarantine standards to improve the protection of the unaffected population during a public health crisis. HHS will also work with state and local health officials during consequence management planning to set priorities for the deployment of vaccination and prophylaxis resources in of the event of a terrorist incident involving biological or chemical weapons.

Enhance protection of emergency stockpiles of medical supplies and domestic and international pharmaceutical manufacturing facilities

HHS and DHS will work with the health care sector to enable the protection of stockpiles of medical supplies and other critical materials, distribution systems, and the critical systems of medical institutions, including basic surveillance capabilities necessary for tracking the spread of diseases and toxic agents. Additionally, HHS will identify providers of critical resources and ensure a ready stockpile of vital medicines for use in an emergency.

Explore options for incentives to increase security spending

In partnership with state health departments, HHS will examine legal and regulatory impediments that could prevent critical health facilities from providing critical services during a crisis. HHS will also explore possible incentives to encourage increased investment in the physical security of facilities in the public health sector. The current federally sponsored investment program to improve critical hospital capabilities within local communities provides an appropriate point of departure for this effort.

EMERGENCY SERVICES

The emergency services infrastructure consists of fire, rescue, emergency medical service (EMS), and law enforcement organizations that are employed to save lives and property in the event of an accident, natural disaster, or terrorist incident.

Emergency Services Sector Challenges

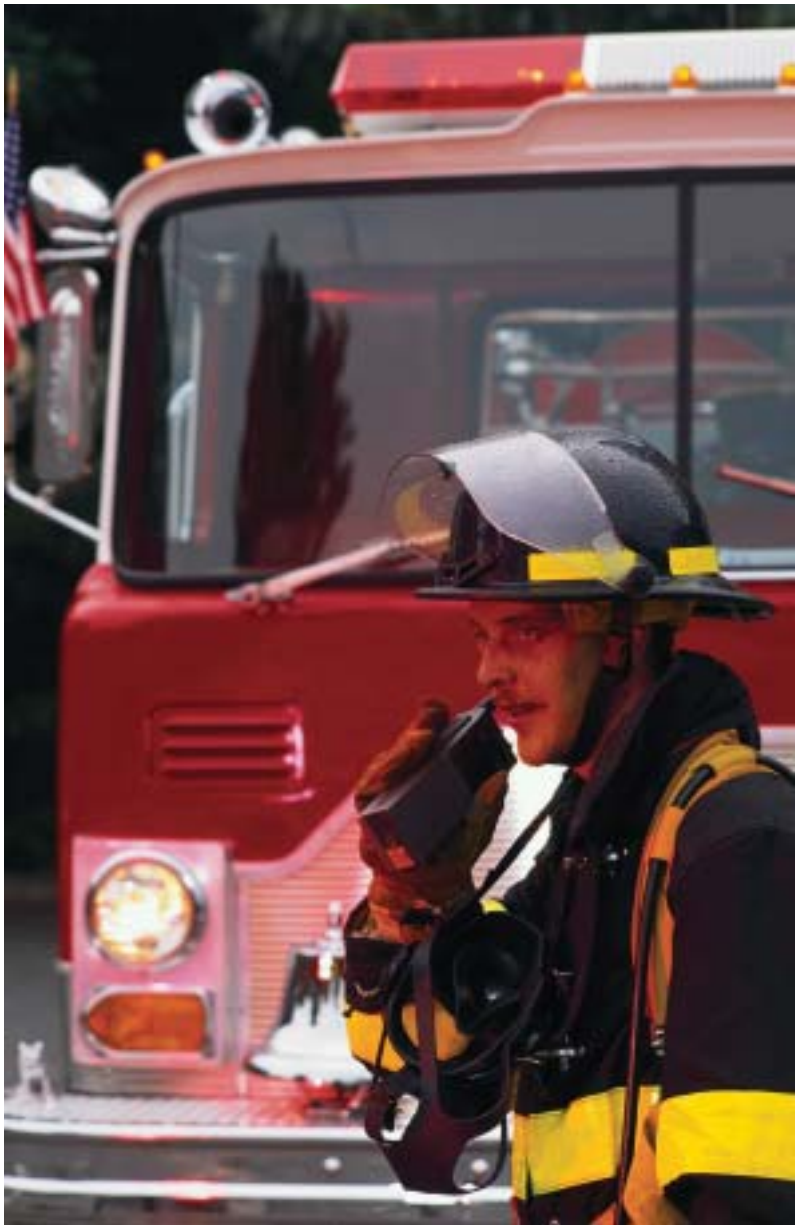
Lessons learned from the September 11 attacks indicate that the most pressing problems to be addressed in this sector include: inadequate information sharing between different organizations—particularly between law enforcement and other first responders; telecommunications problems, such as a lack of redundant systems; and the challenge of enhancing force protection through such measures as stronger crime scene control and enhanced security to mitigate secondary attacks.

Terrorists pose a major challenge to our national emergency response network. Although the existing infrastructure is sufficient for dealing with routine accidents and regional disasters, the September 11 attacks revealed shortfalls in its specific capabilities to respond to large-scale terrorist incidents and other catastrophic disasters requiring extensive cooperation among local, state, and federal emergency response organizations. Most pressing among these shortfalls has been the inability of multiple first-responder units, such as police and fire departments, to coordinate their efforts—even when they originate from the same jurisdiction.

Major emergencies require cooperation by multiple public agencies and local communities. Systems supporting emergency response personnel, however, have been specifically developed and implemented with respect to the unique needs of each agency. Such specification complicates interoperability, thereby hindering the ability of various first responder organizations to communicate and coordinate resources during crisis situations.

Robust communications systems are essential for personnel safety and the effective employment of human resources during a crisis or an emergency. Failure of communications systems during a crisis impedes the speed of response and puts the lives of responders at risk. Another important issue is the extent to which emergency response communications depend on key physical nodes, such as a central dispatcher, firehouse, or 911-call center.

Unlike most critical infrastructures, which are closely tied to physical facilities, the emergency services sector consists of highly mobile teams of specialized personnel and equipment. Another challenge for the emergency services sector, therefore, is assuring the protection of first responders and critical resources during emergency response operations. Future terrorist incidents could present unseen hazards at incident sites, including the risk of exposure to CBR agents. Moreover, past experience indicates that emergency services response infrastructure and personnel can also be the targets of deliberate direct or secondary attacks, a bad scenario that could be made worse by communication difficulties and responding units that are ill-prepared for such a likelihood.



Preparedness exercises serve to provide experience and feedback on preparation for response and emergency management activities. Various state and local governments and federal agencies have hosted local or regional exercises. The approaches used vary widely—a fact that could impede the effectiveness of multi-jurisdictional response efforts.

Faced with the threat of a major terrorist attack, no single jurisdiction has the ability to maintain or assemble all of the resources necessary to provide an effective response. Mutual aid agreements facilitate the flow of public safety personnel, equipment, and other vital resources across jurisdictional boundaries to enable local communities to help each other during emergencies and disasters.

Emergency Services Sector Initiatives

Emergency services sector protection and response initiatives include efforts to:

Adopt interoperable communications systems

DHS and DoJ will work with state and local governments and other appropriate entities to study and resolve important communications interoperability issues. This problem is already widely recognized and accepted as a valid concern at the state and local government level. The common, overriding need to assure effective communications during an emergency can be used as a catalyst to drive individual agencies toward a solution.

Develop redundant communications networks

DHS will work with state and local officials to develop redundant emergency response networks to improve communications availability and reliability, especially during a major disruption.

Implement measures to protect our national emergency response infrastructure

DHS will inventory and analyze the vulnerability of our national emergency response infrastructure, including critical personnel, facilities, systems, and functions. DHS will work with states, localities, and other entities to develop plans to assure the safety of personnel during response efforts, as well as the protection of our emergency response critical infrastructure.

Coordinate national preparedness exercises

DHS will work with state and local governments to develop a coordinated national emergency response exercise program. Coordinated preparedness exercises would promote consistency in protection planning and response protocols and capabilities at the regional and national levels, as well as provide a forum for sharing lessons learned and best practices.

Enhance and strengthen mutual aid agreements among local jurisdictions

DHS will work with officials from local communities to strengthen existing mutual aid agreements and develop new ones in regions across the U.S. where needed. Furthermore, it will promote discussion regarding the adoption of common standards and terminology for equipment and training.

DEFENSE INDUSTRIAL BASE

Our nation's defense and military strength rely primarily on the DoD and the private sector defense industry that supports it. Without the important contributions of the private sector, DoD cannot effectively execute its core defense missions, including mobilization and deployment of our nation's military forces abroad. Conversely, private industry and the public at large rely on the federal government to provide for the common defense of our Nation and protect our interests both domestically and abroad.

Success in the war on terrorism depends on the ability of the United States military to mount swift, calculated offensive and defensive operations. Ensuring that our military is well trained and properly equipped is critical to maintaining that capability. Private industry manufactures and provides the majority of the equipment, materials, services, and weaponry used by our armed forces. For several decades, DoD has worked to identify its own critical assets and systems. It has also begun to address its dependency on the defense industrial base, and is now taking the concerns of private industry into consideration in its critical infrastructure protection assessment efforts.

Market competition, consolidations, globalization, and attrition have reduced or eliminated redundant sources of products and services and therefore increased risk for DoD. Outsourcing and complex domestic and foreign corporate mergers and acquisitions have made it even more difficult for DoD to be assured that its prime contractors' second-, third-, and fourth-tier subcontractors understand its security requirements and are prepared to support them in a national emergency.

Defense Industrial Base Challenges

Over the past 20 years, DoD's dependency on the private sector has greatly increased. Outsourcing has caused the department to rely increasingly on contractors to perform many of the tasks that were once under the exclusive purview and control of the military. Even the utilities that service many of the nation's important military installations are being privatized. Because of market competition and attrition, DoD now relies more and more on a single or very limited number of private-sector suppliers to fulfill some of its most essential needs. DoD, unlike other federal government agencies, requires strict adherence to military product specification and unique requirements for services. Select private-industry vendors may be the only

suppliers in the world capable of satisfying these unique requirements. Many of these sources have single manufacturing and distribution points that warrant additional security review and assessment.

A related problem involves the current process through which DoD contracts with the private sector to provide critical services and supplies. Most often the procurement process is based on cost and efficiency. Such an approach may not always take into account the vendor's critical infrastructure protection practices (e.g., workforce hiring, supplier base) and its ability to supply products and services and provide surge response during an emergency or exigent circumstances.

Finally, there are also growing concerns within the private sector regarding the potential for additional costs and risks resulting from federal mandates that require private industry to implement enhanced infrastructure protection measures.

Defense Industrial Base Initiatives

The infrastructures of the private defense industry and DoD are already integrated on many levels. DoD, in concert with DHS, will continue working with the private sector to identify critical installations and infrastructures, and, subsequently, to delineate specific protection requirements. Furthermore, DoD and DHS will collaborate with key defense industrial base

organizations to integrate and build upon their individual existing protection plans.

Additional defense industrial base protection initiatives include efforts to:

Build critical infrastructure protection requirements into contract processes and procedures

DoD will collaborate with the defense industry to review contract processes and procedures to determine how to include provisions that address critical infrastructure protection needs. Contracts will specifically address national emergency situation requirements, such as contractor response times, supply and labor availability, and direct logistic support. When appropriate, contracts will also include language regarding program manager accountability for the protection of supporting infrastructures. Sensitive contractual documents will receive greater scrutiny and revision prior to public posting. Additionally, DoD will give specific scrutiny to its potential dependency on foreign commercial operators and suppliers.

Incorporate security concerns into production and distribution processes and procedures

DoD and industry will explore ways to eliminate key production and distribution bottlenecks.

Develop an effective means of sharing security-related information between defense organizations and private-sector service providers

DoD will work with DHS and the intelligence and law enforcement communities to establish the necessary policies and mechanisms to facilitate a productive exchange of security-related information with the defense industry.

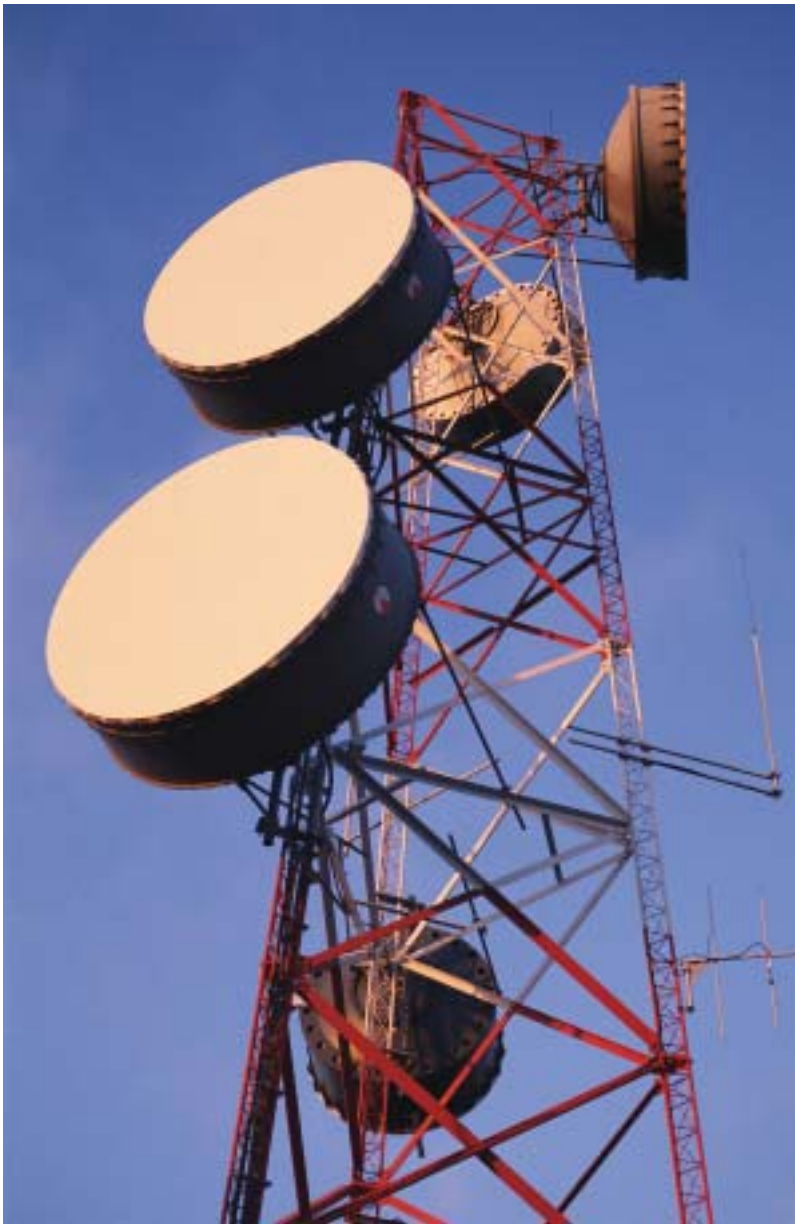
TELECOMMUNICATIONS

The composition of the telecommunications sector evolves continuously due to technology advances, business and competitive pressures, and changes in the regulatory environment. Despite its dynamic nature, the sector has consistently provided robust and reliable communications and processes to meet the needs of businesses and governments. In the new threat environment, the sector faces significant challenges to protect its vast and dispersed critical assets, both cyber and physical. Because the government and critical-infrastructure industries rely heavily on the public telecommunications infrastructure for vital communications services, the sector's protection initiatives are particularly important.

The telecommunications sector provides voice and data service to public and private users through a complex and diverse public-network infrastructure encompassing the Public Switched Telecommunications Network (PSTN), the Internet, and private enterprise networks. The PSTN provides switched circuits for telephone, data, and leased point-to-point services. It consists of physical facilities, including over 20,000 switches, access tandems, and other equipment. These components are connected by nearly two billion miles of fiber and copper cable. The physical PSTN remains the backbone of the infrastructure, with cellular, microwave, and satellite technologies providing extended gateways to the wireline network for mobile users. Supporting the underlying PSTN are Operations, Administration, Maintenance, and Provisioning systems, which provide the vital management and administrative functions, such as billing, accounting, configuration, and security management.

Advances in data network technology and the increasing demand for data services have spawned the rapid proliferation of the Internet infrastructure. The Internet consists of a global network of packet-switched networks that use a common suite of protocols. Internet Service Providers (ISPs) provide end-users with access to the Internet. Larger ISPs use Network Operation Centers (NOCs) to manage their high capacity networks, linking them through Internet peering points or network access points. Smaller ISPs usually lease their long-haul transmission capacity from the larger ISPs and provide regional and local Internet access to end-users via the PSTN. Internet access providers interconnect with the PSTN through points of presence, typically a switch or a router, located at carrier central offices. International PSTN and Internet traffic travels via underwater cables that reach the United States at various cable landing points.

In addition to the PSTN and the Internet, enterprise networks are an important component of the telecommunications infrastructure. Enterprise networks are dedicated networks supporting the voice and data needs and operations of large enterprises. These networks comprise a combination of leased lines or services from the PSTN or Internet providers.



The Telecommunications Act of 1996 opened local PSTN service to competition. It required incumbent carriers to allow their competitors to have open access to their networks. As a result, carriers began to concentrate their assets in collocation facilities and other buildings known as telecom hotels, collocation sites, or peering points instead of laying down new cable. ISPs also gravitated to these facilities to reduce the costs of exchanging traffic with other ISPs. Open competition, therefore, has caused the operation of the PSTN and the Internet (including switching, transport, signaling, routing, control, security, and management) to become increasingly interconnected, software driven, and remotely managed, while the industry's physical assets are increasingly concentrated in shared facilities.

The telecommunications infrastructure is undergoing a significant transformation that involves the convergence of traditional circuit-switched networks with broadband packet-based IP networks, including the Internet. Eventually, the packet networks will subsume the circuit-switched networks, leading to the establishment of a public, broadband, diverse, and scaleable packet-based network known as the Next Generation Network (NGN). Additionally, the evolution of the telecommunications infrastructure has included steady growth in mobile wireless services and applications. Wireless telecommunications providers transmit messages using an infrastructure of base stations and radio-cell towers located throughout the wireless provider's service area. Wireless services consist of digital mobile phones and emerging data services, including Internet communications, wireless local-area networks, and advanced telephony services.

Convergence, the growth of the NGN, and emergence of new wireless capabilities continue to introduce new physical components to the telecommunications infrastructure. Government and industry consistently work together to develop strategies to ensure that the evolving infrastructure remains reliable, robust, and secure. Public-private partnerships and organizations currently addressing telecommunications security include the President's National Security Telecommunications Advisory Committee and Critical Infrastructure Protection Board (PCIPB), the Government Network Security Information Exchanges, the Telecommunications ISAC, and the Network Reliability and Interoperability Council of the FCC. Recommendations by these bodies and collaboration among industry and government will shape the security and reliability of the evolving infrastructure.

Telecommunications Sector Challenges

Every day the sector must contend with traditional natural and human-based threats to its physical infrastructure, such as weather events, unintentional cable cuts, and the insider threat (e.g., physical and cyber sabotage). The September 11 attacks revealed the threat terrorism poses to the telecommunications sector's physical infrastructure. While it was not a direct target of the attacks, the telecommunications sector suffered significant collateral damage. In the future, certain concentrations of key sector assets themselves could become attractive direct targets for terrorists, particularly with the increased use of collocation facilities. The telecommunications infrastructure withstood the September 11 attacks in overall terms and demonstrated remarkable resiliency because damage to telecommunications assets at the attack sites was offset by diverse, redundant, and multifaceted communications capabilities.

Priorities for telecommunications carriers are service reliability, cost balancing, security, and effective risk management postures. The government places high priority on the consistent application of security across the infrastructure. Although private- and public-sector

stakeholders share similar objectives, they have different perspectives on what constitutes acceptable risk and how to achieve security and reliability. Therefore, an agreement on a sustainable security threshold and corresponding security requirements remains elusive.

Because of growing interdependencies among the various critical infrastructures, a direct or indirect attack on any of them could result in cascading effects across the others. Such interdependencies increase the need to identify critical assets and secure them against both physical and cyber threats. Critical infrastructures rely upon a secure and robust telecommunications infrastructure. Redundancy within the infrastructure is critical to ensure that single points of failure in one infrastructure will not adversely impact others. It is vital that government and industry work together to characterize the state of diversity in the telecommunications architecture. They must also collaborate to understand the topography of the physical components of the architecture to establish a foundation for defining a strategy to ensure physical and logical diversity.

Despite significant challenges, the telecommunications marketplace remains competitive, and customer demand for services is steady, if not increasing. An economic upturn within the industry could rapidly accelerate service demands. The interplay of market forces and FCC oversight will ensure the continuance of service delivery to sustain critical telecommunications functions. Nevertheless, recent economic distress has forced companies to spend their existing resources on basic network operations rather than re-capitalizing, securing, and enhancing the infrastructure, which could amplify the financial impact of necessary infrastructure protection investments.

Telecommunications Sector Initiatives

Given the reality of the physical and cyber threats to the telecommunications sector, government and industry must continue to work together to understand vulnerabilities, develop countermeasures, establish policies and procedures, and raise awareness necessary to mitigate risks. The telecommunications sector has a long, successful history of collaboration with government to address concerns over the reliability and security of the telecommunications infrastructure.

The sector has recently undertaken a variety of new initiatives to further ensure both reliability and quick recovery and reconstitution. Within this environment of increasing emphasis on protection issues, public-private partnership can be further leveraged to address a number of key telecommunications initiatives, including efforts to:

Define an appropriate threshold for security

DHS will work with industry to define an appropriate security threshold for the sector and develop a set of requirements derived from that definition. DHS will work with industry to close the gap between respective security expectations and requirements. Reaching agreement on a methodology for ensuring physical diversity is a key element of this effort.

Expand infrastructure diverse routing capability

DHS will leverage and enhance the government's capabilities to define and map the overall telecommunications architecture. This effort will identify critical intersections among the various infrastructures and lead to strategies that better address security and reliability.

Understand the risks associated with vulnerabilities of the telecommunications infrastructure

The telecommunications infrastructure, including the PSTN, the Internet, and enterprise networks, provides essential communications for governments at all levels and other critical infrastructures. DHS will work with the private sector to conduct studies to understand physical vulnerabilities within the telecommunications infrastructure and their associated risks. Studies will focus on facilities where many different types of equipment and multiple carriers are concentrated.

Coordinate with key allies and trading partners

More than ever our Nation has a common reliance on vital communications circuits and processes with our key allies and trading partners. DHS will work with other nations to consider innovative communications paths that provide priority communications processes to link our governments, global industries, and networks in such a manner that vital communications are assured.

ENERGY

Energy drives the foundation of many of the sophisticated processes at work in American society today. It is essential to our economy, national defense, and quality of life.

The energy sector is commonly divided into two segments in the context of critical infrastructure protection: electricity and oil and natural gas. The electric industry services almost 130 million households and institutions. The United States consumed nearly 3.6 trillion kilowatt hours in 2001. Oil and natural gas facilities and assets[1] are widely distributed, consisting of more than 300,000 producing sites, 4,000 off-shore platforms, more than 600 natural gas processing plants, 153 refineries, and more than 1,400 product terminals, and 7,500 bulk stations.

ELECTRICITY

Almost every form of productive activity—whether in businesses, manufacturing plants, schools, hospitals, or homes—requires electricity. Electricity is also necessary to produce other forms of energy, such as refined oil. Were a widespread or long-term disruption of the power grid to occur, many of the activities critical to our economy and national defense—including those associated with response and recovery—would be impossible.

The North American electric system is an interconnected, multi-nodal distribution system that accounts for virtually all the electricity supplied to the United States, Canada, and a portion of Baja California Norte, Mexico. The physical system consists of three major parts: generation, transmission and distribution, and control and communications.

Generation assets include fossil fuel plants, hydroelectric dams, and nuclear power plants. Transmission and distribution systems link areas of the national grid. Distribution systems manage and control the distribution of electricity into homes and businesses. Control and communications systems operate and monitor critical infrastructure components.

In addition to these components, the electric infrastructure also comprises ancillary facilities and systems that guarantee fuel supplies necessary to support electricity generation, some of which involve the handling of hazardous materials. The electricity sector also depends heavily on other critical infrastructures for power generation, such as telecommunications and transportation.

The North American electric system is the world's most reliable, a fact that can be attributed to industry-led efforts to identify single points of failure and system interdependencies, and institute appropriate back-up processes, systems, and facilities.

After New York's power blackout in 1965, the industry established the North American Electric Reliability Council (NERC) to develop guidelines and procedures for preventing similar incidents. NERC is a nonprofit corporation made up of 10 regional reliability councils, whose voluntary membership represents all segments of the electricity industry, including public and private utilities from the U.S. and Canada. Through NERC, the electricity sector coordinates programs to enhance security for the electricity industry.

The electricity sector is highly regulated even as the industry is being restructured to increase competition. The Federal Energy Regulatory Commission (FERC) and state utility regulatory commissions regulate some of the activities and operations of certain electricity industry participants. The Nuclear Regulatory Commission (NRC) regulates nuclear power reactors and other civilian nuclear facilities, materials, and activities.[2]

Electricity Sector Challenges

The electricity sector is highly complex, and its numerous component assets and systems span the North American continent. Many of the sector's key assets, such as generation facilities, key substations, and switchyards, present unique protection challenges.

Increased competition and structural changes currently taking place within the sector may alter security incentives and responsibilities of electricity market participants. These stakeholders are diverse in size, capabilities, and focus. Currently, individual companies pay for levels of protection that are consistent with their resources and customer expectations. Typically, these companies seek to recover the costs of new security investments through proposed rate or price increases. Under current federal law, however, there is no assurance that electricity industry participants would be allowed to recover the costs of federally mandated security measures through such rate or price increases.

Another challenge for the electricity industry is effective, sector-wide communications. The owners and operators of the electric system are a large and heterogeneous group. Industry associations serve as clearing houses for industry-related information, but not all industry owners and operators belong to such organizations. Data needed to perform thorough analyses on the infrastructure's interdependencies is not readily available. A focused analysis of time-phased effects of one infrastructure on another, including loss of operations metrics, would help identify dependencies and establish protection priorities and strategies.

For certain transmission and distribution facilities, providing redundancy and increasing generating capacity provide greater reliability of electricity service. However, this approach faces several challenges. Long lead times, possible denials of rights-of-way, state and local siting requirements, "not-in-my-backyard" community perspectives, and uncertain rates of return when compared to competing investment needs are hurdles that may prevent owners and operators of electricity facilities from investing sufficiently in security and service assurance measures.

Building a less vulnerable grid represents another option for protecting the national electricity infrastructure. Work is ongoing to develop a national R&D strategy for the electricity sector. Additionally, FERC has developed R&D guidelines, and the Department of Energy's (DoE's) National Grid Study contains recommendations focused on enhancing physical and cyber security for the transmission system.

Electricity Sector Initiatives

The electricity industry has a history of taking proactive measures to assure the reliability and availability of the electricity system. Individual enterprises also work actively in their communities to address public safety issues related to their systems and facilities. Since September 11, 2001, the sector has reviewed its security guidelines and initiated a series of intra-industry working groups to address specific aspects of security. It has created a utility-sector security committee at the chief executive officer level to enhance planning, awareness, and resource allocation within the industry.

The sector as a whole, with NERC as the sector coordinator, has been working in collaboration with DOE since 1998 to assess its risk posture in light of the new threat environment, particularly with respect to the electric system's dependence on information technology and networks. In the process, the sector has created an awareness program that includes a *"Business Case for Action"* for industry senior executives, a strategic reference document, *"An Approach to Action for the Electric Power Sector,"* and security guidelines related to physical and cyber security.

With respect to managing security information, the sector has established an indications, analysis, and warning program that trains utilities on incident reporting and alert notification procedures. The sector has also developed threat alert levels for both physical and cyber events, which include action-response guidelines for each alert level. The industry has also established an ISAC to gather incident information, relay alert notices, and coordinate daily briefs between the federal government and electric grid operators around the country.

Power management control rooms are probably the most protected aspect of the electrical network. NERC's guidelines require a backup system and/or manual work-arounds to bypass damaged systems. FERC is also working with the sector to develop a common set of security requirements for all enterprises in the competitive electric supply market.

Additional electricity sector protection initiatives include efforts to:

Identify equipment stock pile requirements

DHS and DoE will work with the electricity sector to inventory components and equipment critical to electric-system operations and to identify and assess other approaches to enhance restoration and recovery to include standardizing equipment and increasing component interchangeability.

Re-evaluate and adjust nationwide protection planning, system restoration, and recovery in response to attacks

The electric power industry has an excellent process and record of reconstitution and recovery from disruptive events. Jointly, industry and government need to evaluate this system and its processes to support the evolution from a local and regional system to an integrated national response system. DHS and DoE will work with the electricity sector to ensure that existing coordination and mutual aid processes can effectively and efficiently support protection, response, and recovery activities as the structure of the electricity sector continues to evolve.

Develop strategies to reduce vulnerabilities

DHS and DoE will work with state and local governments and the electric power industry to identify the appropriate levels of redundancy of critical parts of the electric system, as well as requirements for designing and implementing redundancy in view of the industry's realignment and restructuring activities.

Develop standardized guidelines for physical security programs

DHS and DOE will work with the sector to define consistent criteria for criticality, standard approaches for vulnerability and risk assessments for critical facilities, and physical security training for electricity sector personnel.

OIL & NATURAL GAS

The oil and natural gas industries are closely integrated. The oil infrastructure consists of five general components: oil production, crude oil transport, refining, product transport and distribution, and control and other external support systems. Oil and natural gas production include: exploration, field development, on- and offshore production, field collection systems, and their supporting infrastructures. Crude oil transport includes pipelines (160,000 miles), storage terminals, ports, and ships. The refinement infrastructure consists of about 150 refineries that range in size and production capabilities from 5,000 to over 500,000 barrels per day. Transport and distribution of oil includes pipelines, trains, ships, ports, terminals and storage, trucks, and retail stations.

The natural gas industry consists of three major components: exploration and production, transmission, and local distribution. The U.S. produces roughly 20 percent of the world's natural gas supply. There are 278,000 miles of natural gas pipelines and 1,119,000 miles of natural gas distribution lines in the U.S. Distribution includes storage facilities, gas processing, liquid natural gas facilities, pipelines, citygates, and liquefied petroleum gas storage facilities. Citygates are distribution pipeline nodes through which gas passes from interstate pipelines to a local distribution system. Natural gas storage refers to underground aquifers, depleted oil and gas fields, and salt caverns.

The pipeline and distribution segments of the oil and natural gas industries are highly regulated. Oversight includes financial, safety, and siting regulations. The exploration and production side of the industry is less regulated, but is affected by safety regulations and restrictions concerning property access.

Oil and Natural Gas Sector Challenges

Protection of critical assets requires both heightened security awareness and investment in protective equipment and systems. One serious issue is the lack of metrics to determine and justify corporate security expenditures. In the case of natural disasters or accidents, there are well-established methods for determining risks and cost-effective levels of investments in protective equipment, systems, and methods for managing risk (e.g., insurance). It is not clear what levels of security and protection are appropriate and cost effective to meet the risks of terrorist attack.

The first government responders to a terrorist attack on most oil and natural gas sector facilities will be local police and fire departments. In general, these responders need to improve their capabilities and preparedness to confront well-planned, sophisticated attacks, particularly those involving CBR weapons. Fortunately, because of public-safety requirements related to their operations and facilities, the oil and natural gas industries have substantial protection programs already in place.

Quick action to repair damaged infrastructure in an emergency can be impeded by a number of hurdles, including the long lead time needed to obtain local, state, and federal construction permits or waivers; requirements for environmental reviews and impact statements; and lengthy processes for obtaining construction rights-of-way for the placement of pipelines on adjoining properties if a new path becomes necessary. The availability of necessary materials and equipment, and the uniqueness of such equipment are also impediments to rapid reconstitution of damaged infrastructure.

The current system for locating and distributing replacement parts needs to be enhanced significantly. The components themselves range from state-of-the-art systems to mechanisms that are decades old. While

newer systems are standardized, many of the older components are unique and must be custom-manufactured. Moreover, there is extensive variation in size, ownership, and security across natural gas facilities. There are also a large number of natural gas facilities scattered over broad geographical areas—a fact that complicates protection.

Oil and Natural Gas Sector Initiatives

Oil and natural gas sector protection initiatives include efforts to:

Plan and invest in research and development for the oil and gas industry to enhance robustness and reliability

Utilizing the federal government's national scientific and research capabilities, DHS and DoE will work with oil and natural gas sector stakeholders to develop an appropriate strategy for research and development to support protection, response, and recovery requirements.

Develop strategies to reduce vulnerabilities

DHS and DoE will work with state and local governments and industry to identify the appropriate levels of redundancy of critical components and systems, as well as requirements for designing and enhancing reliability.

Develop standardized guidelines for physical security programs

DHS and DoE will work with the oil and natural gas industry representatives to define consistent criteria for criticality, standard approaches for vulnerability and risk assessments for various facilities, and physical security training for industry personnel.

Develop guidelines for measures to reconstitute capabilities of individual facilities and systems

DHS and DoE will convene an advisory task force of industry representatives from the sector, construction firms, equipment suppliers, oil-engineering firms, state and local governments, and federal agencies to identify appropriate planning requirements and approaches.

Develop a national system for locating and distributing critical components in support of response and recovery activities

DHS and DoE will work with industry to develop regional and national programs for identifying spare parts, requirements, notifying parties of their availability, and distributing them in an emergency.

---

1 Pipelines that transport oil and gas supplies are components of the transportation sector's critical infrastructure and are regulated by the Department of Transportation (DoT) for safety purposes. Their protection is discussed in further detail on pages 58-59 of the *Transportation Sector Section* of this document.

2 Nuclear power plants are an important component of the energy sector's critical infrastructure. Because of the potential public health and safety consequences an attack on a nuclear facility could cause, specific issues related to their protection are included on page 74 of the *Protecting Key Assets* chapter of this document.

TRANSPORTATION

The transportation sector consists of several key modes: aviation, maritime traffic, rail, pipelines, highways, trucking and busing, and public mass transit. The diversity and size of the transportation sector makes it vital to our economy and national security, including military mobilization and deployment. As a whole, its infrastructure is robust, having been developed over decades of both private and public investment. Together the various transportation modes provide mobility of our population and contribute to our much-cherished individual freedom. The transportation infrastructure is also convenient. Americans rely on its easy access and reliability in their daily lives.

Interdependencies exist between transportation and nearly every other sector of the economy. Consequently, a threat to the transportation sector may impact other industries that rely on it. Threat information affecting transportation modes must be adequately addressed through communication and coordination among multiple parties who use or rely on these systems.

AVIATION

The aviation mode is vast, consisting of thousands of entry points. It also has symbolic value, representing the freedom of movement that Americans value so highly as well as the technological and industrial prowess that have made the United States a world power. The Nation's aviation system consists of two main parts:

- Airports and the associated assets needed to support their operations, including the aircraft that they serve; and
- Aviation command, control, communications, and information systems needed to support and maintain safe use of our national airspace.

Before September 11, the security of airports and their associated assets was the responsibility of private carriers and state and local airport owners and operators. In the months following the September 11 attacks, Congress passed legislation establishing the Transportation Security Administration as the responsible authority for assuring aviation security.

Aviation Mode Challenges

As the events of September 11 illustrated, aviation's vital importance to the U.S. economy and the freedom it provides our citizens make its protection an important national priority. Aviation faces several unique protection challenges. Its distribution and open access through thousands of entry points at home and abroad make it difficult to secure. Furthermore, components of the aviation infrastructure are not only attractive

terrorist targets, but also serve as potential weapons to be exploited. Together, these factors make the U.S. aviation infrastructure a potential target for future terrorist strikes.

Additional unique protection challenges for aviation include:

- *Volume:* U.S. air carriers transport millions of passengers every day and at least twice as many bags and other cargo.
- *Limited capabilities and available space:* Current detection equipment and methods are limited in number, capability, and ease of use.
- *Time-sensitive cargo:* "Just-in-time" delivery of valuable cargo is essential for many businesses—any significant time delay in processing and transporting such cargo would negatively affect the U.S. economy.
- *Security versus convenience:* Maintaining security while limiting congestion and delays complicates the task of security and has important financial implications.
- *Accessibility:* Most airports are open to the public; their facilities are close to public roadways for convenience and to streamline access for vehicles delivering passengers to terminals.

Another concern for the aviation industry is the additional cost of increased security during sustained periods of heightened alert. Since September 11, 2001, airports across the country have-in effect-been working at surge capacity to meet the security requirements of the current threat environment. Some cash-strapped operators must now balance providing higher levels of security with staying in business.

Aviation Mode Initiatives

Airport security failures on September 11 have placed the aviation industry under intense public scrutiny. To regain the public's confidence in air travel, public and private organizations have made substantial investments to increase airport security. Much work remains. DHS, as the federal lead department for the transportation sector, will work with DoT, industry, and state and local governments to organize, plan, and implement needed protection activities.

Aviation mode protection initiatives include efforts to:

Identify vulnerabilities, interdependencies, and remediation requirements

DHS and DoT will work with representatives from state and local governments and industry to implement or facilitate risk assessments to identify vulnerabilities, interdependencies, and remediation requirements for operations and coordination-center facilities and systems, such as the need for redundant telecommunications for air traffic command and control centers.

Identify potential threats to passengers

DHS and DoT will work with airline and airport security executives to develop or facilitate new methods for identifying likely human threats while respecting constitutional freedoms and privacy.

Improve security at key points of access

DHS and DoT will work with airline and airport security executives to tighten security or facilitate increased security at restricted access points within airport terminal areas, as well as the perimeter of airports and associated facilities, including operations and coordination centers.

Increase cargo screening capabilities

DHS and DoT will work with airline and airport security officials to identify and implement or facilitate technologies and processes to enhance airport baggage-screening capacities.

Identify and improve detection technologies

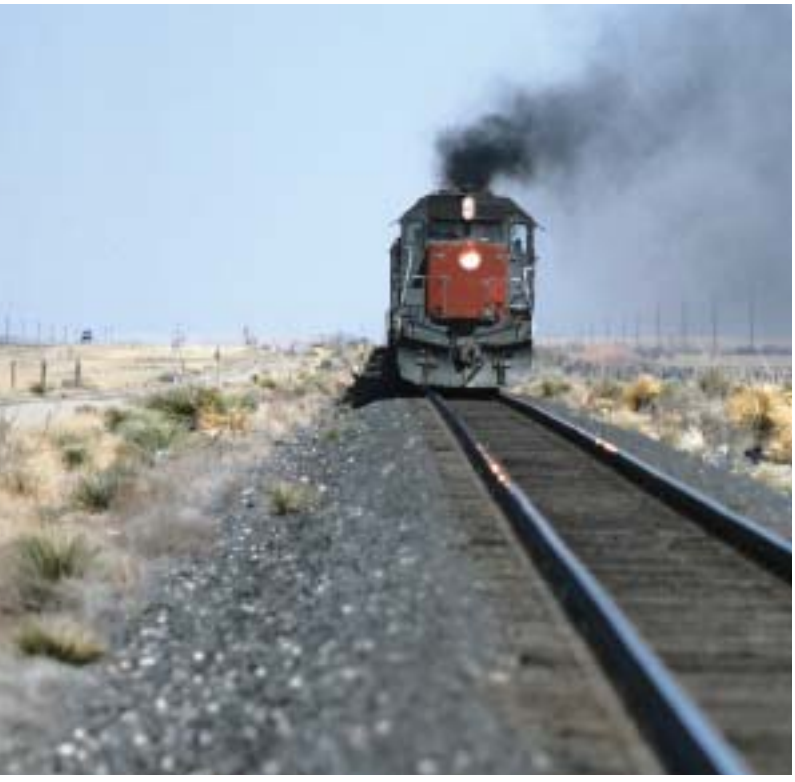
DHS and DoT will work with airline and airport security executives to implement or facilitate enhanced technologies for detecting explosives. Such devices will mitigate the impact of increased security on passenger check-in efficiency and convenience, and also provide a more effective and efficient means of assuring vital aviation security.

PASSENGER RAIL AND RAILROADS

During every hour of every day, trains traverse the United States, linking producers of raw materials to manufacturers and retailers. They carry mining, manufacturing, and agriculture products; liquid chemicals and fuels; and consumer goods. Trains carry 40 percent of intercity freight—a much larger portion than is moved by any other single mode of transportation. About 20 percent of that freight is coal, a critical resource for the generation of electricity. More than 20 million intercity travelers use the rail system annually, and 45 million passengers ride trains and subways operated by local transit authorities. Securing rail-sector assets is critical to protecting U.S. commerce and the safety of travelers.

Rail Mode Challenges

Our Nation's railway system is vast and complex, with multiple points of entry. Differences in design, structure, and purpose of railway stations complicate the sector's overall protection framework. The size and breadth of the sector make it difficult to react to threats effectively or efficiently in all scenarios. This fact complicates protection efforts, but it also offers certain mitigating potential in the event of a terrorist attack. For example, trains are confined to specific routes and are highly controllable. If hijacked, a train can be shunted off the mainline and rendered less of a threat. Similarly, the loss of a bridge or tunnel can impact traffic along major corridors; however, the potential for national-level disruptions is limited.



The greater risk is associated with rail transport of hazardous materials. Freight railways often carry hazardous materials that are essential to other sectors and public services. The decision-making process regarding their transport is complex and requires close coordination between industry and government. A sector-wide information sharing process could help prevent over-reactive security measures, such as restricting the shipment of critical hazardous materials nationwide as a blanket safety measure in response to a localized incident.

Security solutions to the container shipping challenge should recognize that, in many cases, commerce, including essential national security materials, must continue to flow. Stifling commerce to meet security needs simply swaps one consequence of a security threat for another. In the event that a credible threat were to necessitate a shutdown, well-developed continuity of operations procedures can mitigate further unintentional negative consequences. For example, contingency planning can help determine how quickly commerce can be resumed; whether rerouting provides a measure of protection; or what specific shipments should be exempt from a shutdown, such as national defense critical materials.

An additional area of concern is the marking of container cars to indicate the specific type of hazardous materials being transported. During an emergency response, placards on rail cars help to alert first responders to hazardous materials they may encounter. Planners must take care, however, to devise a system of markings that terrorists cannot easily decipher.

Like the aviation sector, the rail industry also faces the additional costs of sustaining increased security during periods of heightened alert. Since the events of September 11, the railroads across the country have—in effect—been working at surge capacity to meet the security requirements of the increased threat environment, which entails assigning overtime and hiring temporary security personnel. Such reservoirs of capacity are costly to maintain. Nevertheless, the rail sector has had to adopt these heightened security levels as the new "normal" state. Some cash-strapped operators now face trade-offs between providing increased levels of security and going out of business.

Railroads have well-developed contingency plans and backups for dispatch, control, and communications equipment that are sufficient for localized or minor disruptions. Developing this type of backup to enable

continuation of operations after a cataclysmic event is problematic given the costs associated with extensive structural enhancements.

Rail Mode Initiatives

The rail mode has been working actively with DoT to assess the risk environment. As a result, it has developed a comprehensive modal risk assessment and established a surface transportation ISAC to facilitate the exchange of information related to both cyber and physical threats specific to the railroads.

Since September 11, many rail operators have added investments to their security programs. Additional rail mode protection initiatives include efforts to:

Develop improved decision-making criteria regarding the shipment of hazardous materials

DHS and DoT, coordinating with other federal agencies, state and local governments, and industry will facilitate the development of an improved process to assure informed decision-making with respect to hazardous materials shipment.

Develop technologies and procedures to screen intermodal containers and passenger baggage

DHS and DoT will work with sector counterparts to identify and explore technologies and processes to enable efficient and expeditious screening of rail passengers and baggage, especially at inter-modal stations.

Improve security of intermodal transportation

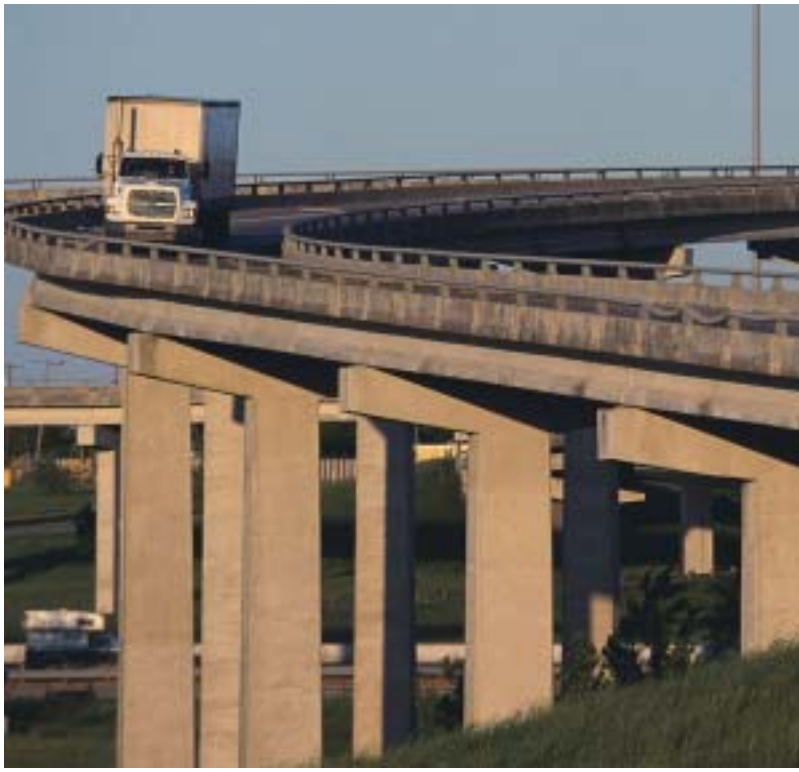
DHS and DoT will work with sector counterparts to identify and facilitate the development of technologies and procedures to secure inter-modal containers and detect threatening content.

DHS and DoT will also work with the rail industry to devise or enable a hazardous materials identification system that supports the needs of first responders, yet avoids providing terrorists with easy identification of a potential weapon.

Clearly delineate roles and responsibilities regarding surge requirements

DHS and DoT will work with industry to delineate infrastructure protection roles and responsibilities to enable the rail industry to address surge requirements for resources in the case of catastrophic events.

Costs and resource allocation remains a contentious issue for the rail sector. DHS and DoT will also convene a working group consisting of government and industry representatives to identify options for the implementation of surge capabilities, including access to federal facilities and capabilities in extreme emergencies.



HIGHWAYS, TRUCKING, AND BUSING

The trucking and busing industry is a fundamental component of our national transportation infrastructure. Without the sector's resources, the movement of people, goods, and services around the country would be greatly impeded. Components of this infrastructure include highways, roads, inter-modal terminals, bridges, tunnels, trucks, buses, maintenance facilities, and roadway border crossings.

Highways, Trucking, and Busing Mode Challenges

Because of its heterogeneity in size and operations and the multitude of owners and operators nationwide, the trucking and busing infrastructure is highly resilient, flexible, and responsive to market demand. For the same reason, the sector is fractionated and regulated by multiple jurisdictions at state, federal, and—sometimes—local levels. The size and pervasive nature of the trucking and busing infrastructure pose significant protection challenges.

Transportation choke points (e.g., bridges and tunnels, inter-modal terminals, border crossings, and highway interchanges) present unique protection challenges. Overall understanding of infrastructure choke points is limited. Common criteria for identifying critical choke points are therefore difficult to establish. We must undertake a comprehensive, systematic effort to identify key assets, particularly those whose destruction or

disruption would entail significant public health and safety consequences or significant economic impact.

Although many states have conducted risk assessments of their respective highway infrastructures, no true basis for comparison among them exists to determine relative criticality. Likewise, there is no coordinated mechanism for assessing choke-point vulnerabilities or conducting and evaluating risk mitigation planning. A major reason for this lack of synchronization within the sector is a paucity of funds to promote communication among industry members and facilitate cooperation for joint protection planning efforts. As a result, the sector as a whole has neither a coherent picture of industry-wide risks, nor a set of appropriate security criteria on which to baseline its protection planning efforts, such as what conditions constitute threats for the sector, or standards for infrastructure protection or threat reduction. The sector's diverse and widely distributed constituency complicates this situation.

Given the number of public and private small-business owners and operators in this sector, the cost of infrastructure protection is also a major challenge. Like the rail mode, in addition to the financial concerns associated with new security investments, highway, trucking, and busing organizations also regard the possibility of security-related delays at border crossings as a potential problem of major financial significance.

Another challenge is the way in which sector security incidents are handled across multiple jurisdictions. Because different law enforcement agencies differ in their approaches to crimes like truck theft, law enforcement responses to security incidents in this sector are inconsistent across jurisdictional lines.

Highways, Trucking, and Busing Mode Initiatives

Like the other major transportation modes, the highways, trucking, and busing mode has assessed its own security programs in light of the September 11 attacks. However, the sector's vast, heterogeneous nature requires further expanded coordination among stakeholder organizations to assure a more consistent, integrated national approach. Additionally, a better understanding of the overall system would lead to more adaptable, less intrusive, and more cost-effective security processes. Highways, trucking, and busing protection initiatives include efforts to:

Facilitate comprehensive risk, threat, and vulnerability assessments

DHS, working closely with DoT and other key sector stakeholders, will facilitate comprehensive risk, threat, and vulnerability assessments for this mode.

Develop guidelines and standard criteria for identifying and mitigating chokepoints

DHS, working with DoT and other sector key stakeholders, will develop guidelines and standard criteria for identifying and mitigating choke points, both nationally and regionally.

Harden industry infrastructure against terrorism through technology

DHS will work jointly with industry and state and local governments to explore and identify potential technology solutions and standards that will support analysis and afford better and more cost effective protection against terrorism.

Create national transportation operator security education and awareness programs

DHS and DoT will work with industry to create national operator security education and awareness programs to provide the foundation for greater cooperation and coordination within this highly diverse mode.

PIPELINES

The United States has a vast pipeline industry, consisting of many hundreds of thousands of miles of pipelines, many of which are buried underground. These lines move a variety of substances such as crude oil, refined petroleum products, and natural gas.

Pipeline facilities already incorporate a variety of stringent safety precautions that account for the potential effects a disaster could have on surrounding areas. Moreover, most elements of pipeline infrastructures can be quickly repaired or bypassed to mitigate localized disruptions. Destruction of one or even several of its key components would not disrupt the entire system. As a whole, the response and recovery capabilities of the pipeline industry are well proven, and most large control-center operators have established extensive contingency plans and backup protocols.

Pipeline Mode Challenges

Pipelines are not independent entities, but rather integral parts of industrial and public service networks. Loss of a pipeline could impact a wide array of facilities and industrial factories that depend on reliable fuel delivery to operate.

Several hundred thousand miles of pipeline span the country, and it is not realistic to expect total security for all facilities. As such, protection efforts focus on infrastructure components whose impairment would have significant effects on the energy markets and the economy as a whole. For the pipeline industry,

determining *what* to protect and *when* to protect it is a factor in cost-effective infrastructure protection. During periods of high demand—such as the winter months—pipeline systems typically operate at peak capacity and are more important to the facilities and functions they serve.

The pipeline industry as a whole has an excellent safety record, as well as in-place crisis management protocols to manage disruptions as they occur. Nevertheless, many of the products that pipelines deliver are inherently volatile. Hence, their protection is a significant issue.

Pipelines cross numerous state and local, as well as international jurisdictions. The number and variety of stakeholders create a confusing, and sometimes conflicting, array of regulations and security programs for the industry to manage, especially with respect to the ability of pipeline facilities to recover, reconstitute, and re-establish service quickly after a disruption.

The pipeline industry's increasing interdependencies with the energy and telecommunications sectors necessitate cooperation with other critical infrastructures during protection and response planning. Individually, companies have difficulty assessing the broader implications of an attack on their critical facilities. These interdependencies call for cross-sector coordination for to be truly responsive to national concerns. Additionally, some issues concerning recovery or reconstitution will require at least regional planning within the industry, as well as the sharing of sensitive business information that may run into proprietary concerns.

Pipeline Mode Initiatives

Historically, individual enterprises within this sector have invested in the security of their facilities to protect their ability to deliver oil and gas products. Representatives from major entities within this sector have examined the new terrorist risk environment. As a result, they have developed a plan for action, including industry-wide information sharing. In addition to industry efforts, DoT has developed a methodology for determining pipeline facility criticality and a system of recommended protective measures that are synchronized with the threat levels of the Homeland Security Advisory System. Additional pipeline mode protection initiatives include efforts to:

Develop standard reconstitution protocols

DHS, in collaboration with DoE, DoT, and industry, will initiate a study to identify, clarify, and establish authorities and procedures as needed to reconstitute facilities as quickly as possible after a disruption.

Develop standard security assessment and threat deterrent guidelines

DHS, in collaboration with DoE and DoT, will work with state and local governments and the pipeline industry to develop consensus security guidance on assessing vulnerabilities, improving security plans, implementing specific deterrent and protective actions, and upgrading response and recovery plans for pipelines.

Work with other sectors to manage risks resulting from interdependencies

DHS, in collaboration with DoE and DoT, will convene cross-sector working groups to develop models for integrating protection priorities and emergency response plans.

MARITIME

The maritime shipping infrastructure includes ports and their associated assets, ships and passenger transportation systems, costal and inland waterways, locks, dams and canals, and the network of railroads and pipelines that connect these waterborne systems to other transportation networks. There are 361 seaports in the United States, and their operations range widely in size and characteristics.

Most ports have diverse waterside facilities that are owned, operated, and accessed by diverse entities. State and local governments control some port authority facilities, while others are owned and operated by private corporations. Most ships are privately owned and operated. Cargo is stored in terminals at ports and loaded onto ships or other vehicles that pass through on their way to domestic and international destinations. DoD has also designated certain commercial seaports as strategic seaports, which provide facilities and services needed for military deployment.

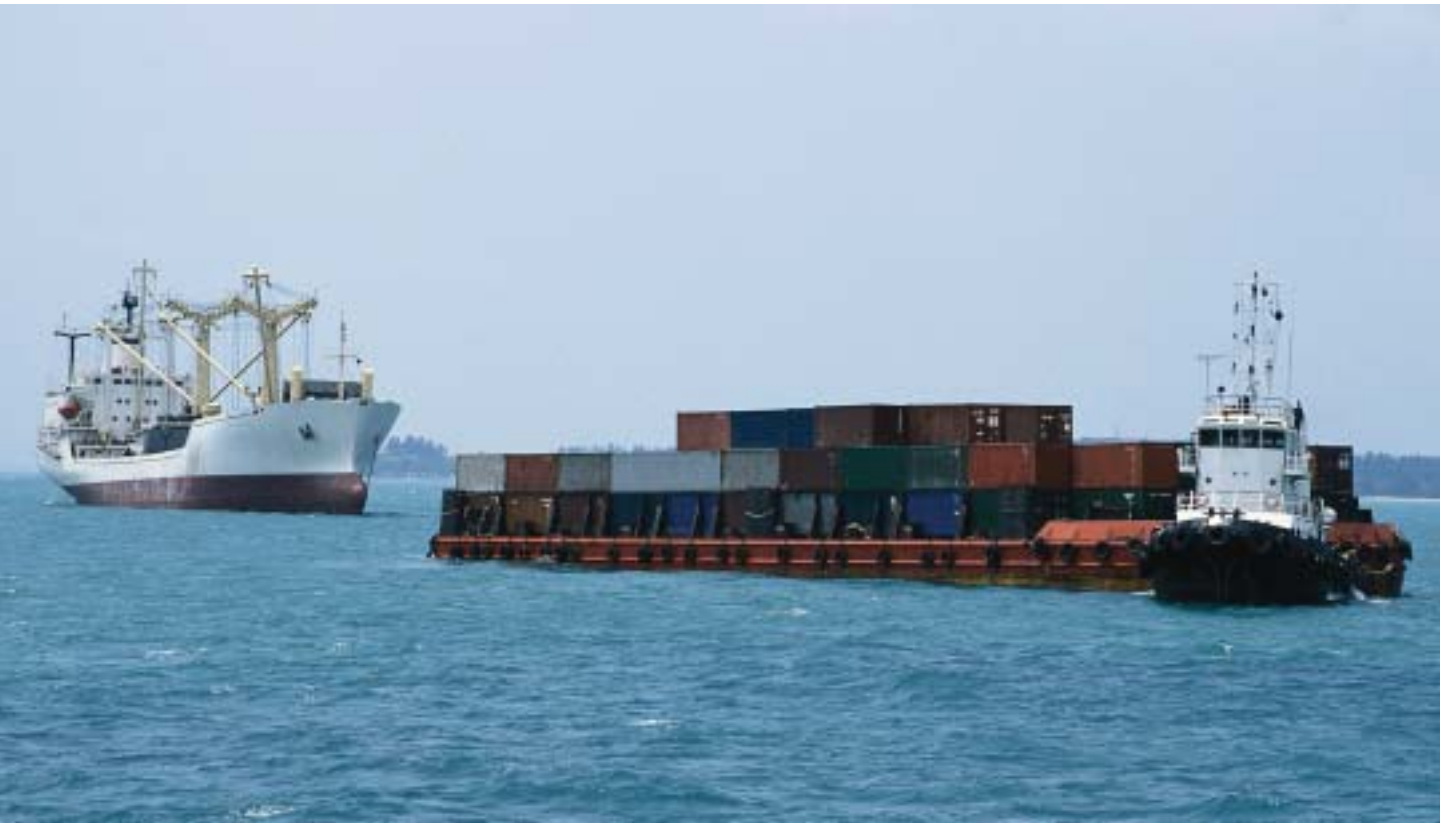
Maritime Mode Challenges

The size, diversity, and complexity of this infrastructure make the inspection of all vessels and cargo that passes through our ports an extremely difficult undertaking. Current inspection methods—both physical and technological—are limited and costly. As with other modes of transportation that cross international borders, we must manage the tension between efficient processing of cargo and passengers and adequate security.

Major portions of the maritime industry's operations are international in nature and are governed by international agreements and multinational authorities, such as the International Maritime Organization. Negotiation of maritime rules and practices with foreign governments lies within the purview of DoS. Often these international efforts involve extended negotiation timelines.

DoT currently recommends guidelines for passenger vessel and terminal security, including passenger and baggage screening and training of crews. The industry requires R&D for cost-effective technologies for the rapid detection of explosives and other hazardous substances, as well as for new vessel designs to minimize the likelihood of a ship sinking if it were attacked.

Much of the port system represents a significant protection challenge, particularly in the case of high consequence cargo. Physical and operational security guidelines have undergone a comprehensive review, from which DoT and DHS will issue guidance and recommendations for appropriate protective actions. Efforts to increase the security of the maritime industry must also consider infrastructures subject to



multi-agency jurisdictions and the international framework in which the industry operates.

Maritime Mode Initiatives

Following the September 11 attacks, initial risk assessments were conducted for all ports. These assessments have helped refine critical infrastructure and key asset designations, assess vulnerabilities, guide the development of mitigation strategies, and illuminate best practices. Most port authorities and private facility owners have also reexamined their security practices. Based on these preliminary risk assessments, DoT increased vessel notification requirements to shift limited resources to maintain positive control of movement of high-risk vessels carrying high-consequence cargoes and large numbers of passengers. DoT and the U.S. Coast Guard have also established a Sea Marshal program and deployable Maritime Safety and Security Teams to implement these activities.

Additionally, DoT has participated in efforts to expedite compliance with existing international standards and to develop additional standards to enhance port, vessel, and facility security. DoT is also working with the U.S. Customs Service to implement the *Container Security Initiative* to ensure the security of the shipping supply chain. Shippers who do not comply with outlined rules and regulations will be subject to greater scrutiny and delays when entering U.S. ports.

Additional maritime mode protection initiatives include efforts to:

Identify vulnerabilities, interdependencies, best practices, and remediation requirements

DHS and DoT will undertake or facilitate additional security assessments to identify vulnerabilities and interdependencies, enable the sharing of share best practices, and issue guidance or recommendations on appropriate mitigation strategies.

Develop a plan for implementing security measures corresponding to varying threat levels

DHS and DoT will work closely with other appropriate federal departments and agencies, port security committees, and private-sector owners and operators to develop or facilitate the establishment of security plans to minimize security risks to ports, vessels, and other critical maritime facilities.

Develop processes to enhance maritime domain awareness and gain international cooperation

DHS and DoT will work closely with other appropriate federal departments and agencies, port security committees, and port owners and operators, foreign governments, international organizations, and commercial firms to establish a means for identifying potential threats at ports of embarkation and monitor identified vessels, cargo, and passengers en route to the U.S.

Develop a template for improving physical and operational port security

DHS and DoT will collaborate with appropriate federal departments and agencies and port owners and operators to develop a template for improving physical and operational port security. A list of possible guidelines will include workforce identification measures, enhanced port-facility designs, vessel hardening plans, standards for international container seals, guidance for the research and development of noninvasive security and monitoring systems for cargo and ships, real-time and trace-back capability information for containers, prescreening processes for high-risk containers, and recovery plans. Activities will include reviewing the best practices of other countries.

Develop security and protection guidelines and technologies for cargo and passenger ships

DHS and DoT will work with international maritime organizations and industry to study and develop appropriate guidelines and technology requirements for the security of cargo and passenger ships.

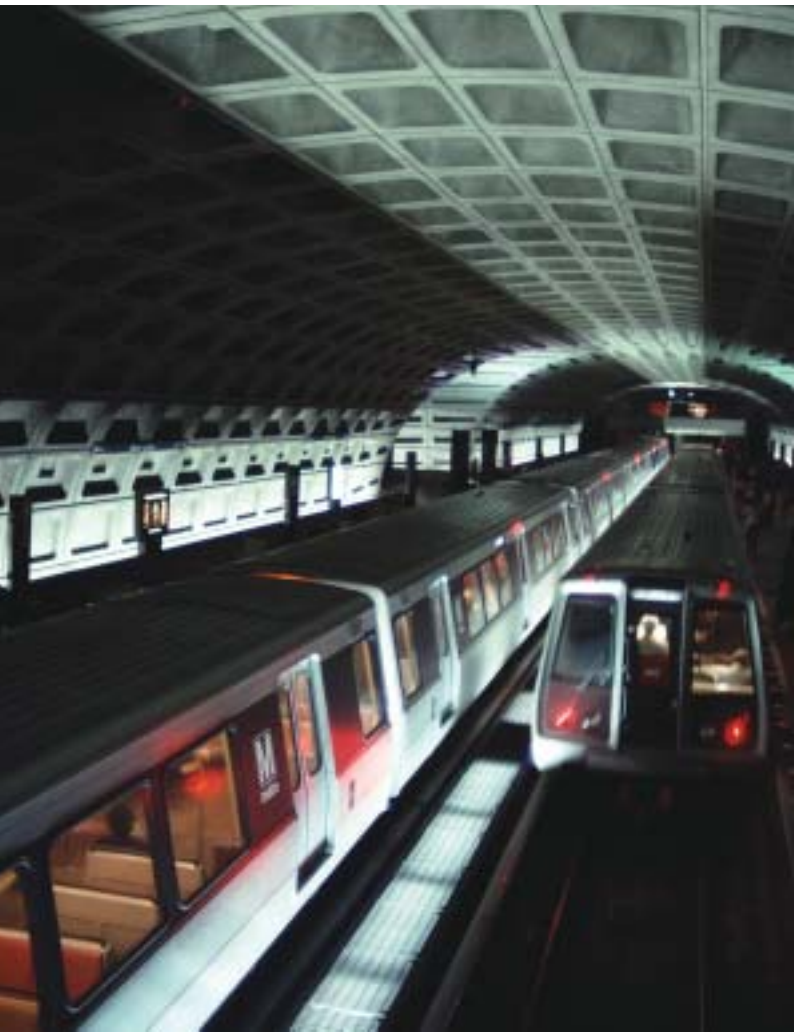
Improve waterway security

DHS and DoT, working with state and local government owners and operators, will develop guidelines and identify needed support for improving security of waterways, such as developing electronic monitoring systems for waterway traffic; modeling shipping systems to identify and protect critical components; and identifying requirements and procedures for periodic waterway patrols.

MASS TRANSIT SYSTEMS

Each year passengers take approximately 9.5 billion trips on public transit. In fact, mass transit carries more passengers in a single day than air or rail transportation. If the effect on air transportation resulting from the September 11 attacks is an indicator, then a terrorist attack on a major mass transit system could have a significant regional and national economic impact.

Mass transit systems are designed to be publicly accessible. Most are owned and operated by state and local agencies. A city relies on its mass transit system to serve a significant portion of its workforce in addition to being a means of evacuation in case of emergency. Protection of mass transit systems is, therefore, an important requirement.



Mass Transit Mode Challenges

Mass transit is regulated by various agencies. These agencies must communicate and work together effectively to allow transit to work as a system rather than in separate modes. Mass transit is funded and managed at the local level, and operated as a not-for-profit entity. The Federal Transit Authority has limited legislative authority to oversee the security planning and operations of transit systems.

Mass transit systems were designed for openness and ease of public access, which makes monitoring points of entry and exit difficult. Protecting them is also expensive. Transit authorities must have the financial resources to respond to emergencies and maintain adequate security levels to deter attacks over broad geographic areas. The cost of implementing new security requirements could result in significant financial consequences for the industry.

Each city and region has a unique transit system, varying in size and design. No one security program or information sharing mechanism will fit all systems. Despite these differences, as a general rule, basic planning factors are relatively consistent from system to system.

Mass Transit Mode Initiatives

Since transit is localized and varies significantly in size and design from system to system, identifying critical guidelines and standards for planning is key to unifying mass transit security activities. Panels in the Transit Cooperative Research Program have recommended and are overseeing 10 research projects in the areas of prevention, mitigation, preparedness, and response. Their recommendations can provide additional input to the development of these planning areas.

Additional mass transit protection initiatives include efforts to:

Identify critical planning areas and develop appropriate guidelines and standards

DHS, working closely with DoT and other federal, state, and local mass transit officials, will identify critical planning areas and develop appropriate guidelines and standards to protect mass transit systems. Such critical planning areas and guidelines include design and engineering standards for facilities and rail and bus vehicles; emergency guidance for operations staff; screening methods and training programs for operators; security planning oversight standards; mutual aid policies; and continuity of operations planning.

Identify protective impediments and implement security enhancements

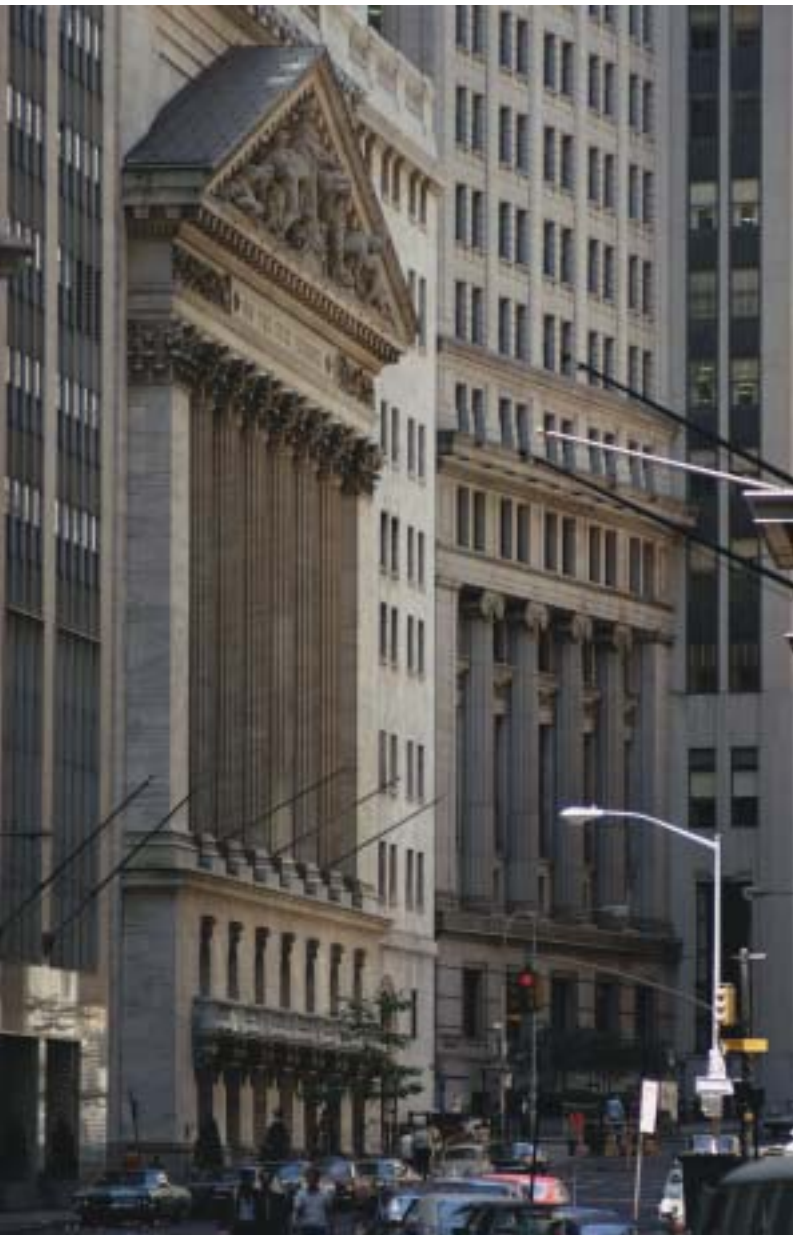
DHS, working closely with DoT and mode representatives, will review legal, legislative, and statutory regimes to develop an overall protective architecture for mass transit systems and to identify impediments to implementing needed security enhancements.

Work with other sectors to manage unique risks resulting from interdependencies

DHS, in collaboration with DoT, will convene cross-sector working groups to develop models for integrating priorities and emergency response plans in the context of interdependencies between mass transit and other critical infrastructures.

BANKING AND FINANCE

The banking and financial services sector infrastructure consists of a variety of physical structures, such as buildings and financial utilities, as well as human capital. Most of the industry's activities and operations take place in large commercial office buildings. Physical structures to be protected house retail or wholesale banking operations, financial markets, regulatory institutions, and physical repositories for documents and financial assets. Today's financial utilities, such as payment and clearing and settlement systems, are primarily electronic, although some physical transfer of assets does still occur. The financial utilities infrastructure includes such electronic devices as computers, storage devices, and telecommunication networks. In addition to the sector's key physical components, many financial services employees have highly specialized skills and are, therefore, considered essential elements of the industry's critical infrastructure.



The financial industry also depends on continued public confidence and involvement to maintain normal operations. Financial institutions maintain only a small fraction of depositors' assets in cash on hand. If depositors and customers were to seek to withdraw their assets simultaneously, severe liquidity pressures would be placed on the financial system. With this in mind, federal safeguards are in place to prevent liquidity shortfalls. In times of crisis or disaster, maintaining public confidence demands that financial institutions, financial markets, and payment systems remain operational or that their operations can be quickly restored.

Additionally, in times of stress the Secretary of the Treasury, the Chairman of the Federal Reserve, and the Securities and Exchange Commission proactively address public confidence issues, as was done following the September 11 terrorist attacks. The Department of the Treasury and federal and state regulatory communities have developed emergency communications plans for the banking and finance sector.

With regard to retail financial services, physical assets are well distributed geographically throughout the industry. The sector's retail niche is characterized by a high degree of substitutability, which means that one type of payment mechanism or asset can be easily replaced with another during a short-term crisis. For example, in retail markets, consumers can make payments through cash, checks, or credit cards.

The banking and financial services industry is highly regulated and highly competitive. Industry professionals and government regulators regularly engage in identifying sector vulnerabilities and take appropriate protective measures, including sanctions for institutions that do not consistently meet standards.

Banking and Finance Sector Challenges

Like the other critical sectors, the banking and financial services sector relies on several critical infrastructure industries for continuity of operations, including electric power, transportation, and public safety services. The sector also specifically relies on computer networks and telecommunications systems to assure the availability of its services. The potential for disruption of these systems is an important concern. For example, the equity securities markets remained closed for four business days following September 11, not because any markets or market systems were inoperable, but because the telecommunications lines in lower Manhattan that connect key market participants were heavily damaged and could not be restored immediately. As a mitigation measure, financial institutions have made great strides to build redundancy and backup into their systems and operations.

Overlapping federal intelligence authorities involved in publicizing threat information cause confusion and duplication of effort for both industry and government. The Department of the Treasury organized the Financial and Banking Information Infrastructure Committee (FBIIC) as a standing committee of the PCIPB. The FBIIC comprises representatives from 13 federal and state financial regulatory agencies.[1] The FBIIC is currently working with the National Infrastructure Protection Center, the Financial Services ISAC (FS-ISAC), and the OHS to improve the information dissemination and sharing processes.

Banking and Finance Sector Initiatives

The attacks in New York City on September 11 showed that the financial services industry is highly resilient. The strong safeguards and back-up systems the industry had in place performed well. Since 1998, the sector has been working with the Department of the Treasury to organize itself to address the risks of the emerging threat environment, particularly cyber intrusions. It was also the first sector to establish an ISAC to share security-related information among members of the industry.

Major institutions in this sector continue to perform ongoing assessments of their security programs. After the September 11 attacks, the industry and its associations initiated lessons-learned reviews to identify corrective actions for the improvement of security and response and recovery programs, as well as to provide a forum for sharing best practices through their trade associations and other interdisciplinary groups. The sector as a whole, with the support of the Department of the Treasury, has also initiated a sector-wide risk review. In addition to sector-wide efforts, individual institutions have stepped up their investments because of their better understanding of the threat.

Additional banking and finance sector protection initiatives include efforts to:

Identify and address the risks of sector dependencies on electronic networks and telecommunications services

The financial services sector's reliance on information systems and networks has resulted in a number of concerns for the industry. The Department of the Treasury, in concert with DHS, will convene a working group consisting of representatives from the telecommunications and financial services sectors, as well as other federal agencies, to study and address the risks that arise from the sector's dependencies on electronic networks and telecommunications services.

Enhance the exchange of security-related information

DHS will work with the Department of Treasury, the FBIIC, and the FS-ISAC to improve federal government communications with sector members and streamline the mechanisms through which they exchange threat information on a daily basis as well as during an incident.

---

1 The FBIIC includes representatives of the federal and state financial regulatory agencies, including: the Commodity Futures Trading Commission, the Conference of State Bank Supervisors, the Federal Deposit Insurance Corporation, the Federal Housing Finance Board, the Federal Reserve Bank of New York, the Federal Reserve Board, the National Association of Insurance Commissioners, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Office of Federal Housing Enterprise Oversight, the Offices of Homeland and Cyberspace Security, the Office of Thrift Supervision, and the Securities and Exchange Commission.

CHEMICAL INDUSTRY AND HAZARDOUS MATERIALS

The chemical sector provides products that are essential to the U.S. economy and standard of living. The industry manufactures products that are fundamental elements of other economic sectors. For example, it produces fertilizer for agriculture, chlorine for water purification, and polymers that create plastics from petroleum for innumerable household and industrial products. Additionally, more than $97 billion of the sector's products go to health care alone.

Currently, the chemical sector is the Nation's top exporter, accounting for 10 cents out of every dollar. The industry is also one of our country's most innovative. It earns one out of every seven patents issued in the U.S., a fact that enables our country to remain competitive in the international chemical market.

The sector itself is highly diverse in terms of company sizes and geographic dispersion. Its product and service-delivery system depends on raw materials, manufacturing plants and processes, and distribution systems, as well as research facilities and supporting infrastructure services, such as transportation and electricity products.

Public confidence is important to the continued economic robustness and operation of the chemical industry. Uncertainty regarding the safety of a product impacts producers as well as the commercial users of the product. With respect to process safety, numerous federal laws and regulations exist to reduce the likelihood of accidents that could result in harm to human health or the environment. However, there is currently no clear, unambiguous legal or regulatory authority at the federal level to help ensure comprehensive, uniform security standards for chemical facilities.

In addition to the economic consequences of a successful attack on this sector, there is also the potential of a threat to public health and safety.[1] Therefore, the need to reduce the sector's vulnerability to acts of terrorism is important to safeguard our economy and protect our citizens and the environment.

Chemical Industry and Hazardous Materials Sector Challenges

Assurance of supply is critical to downstream users of chemical products for various reasons. Many large municipal water works maintain only a few days supply of chlorine for disinfecting their water supplies. Agricultural chemicals, particularly fertilizers, must be applied in large volumes during very short time periods. Some products cannot be transferred between transportation modes. Facilities with "just-in-time" delivery systems maintain fewer and smaller chemical stockpiles.

The industry's ability to protect and assure the quality of its own chemical stockpiles is also important. Because chemicals are vital to many applications, contamination of key chemical stocks could impact a wide range of other industries, thereby affecting public health and the economy. In addition to the risk of contamination at product storage facilities, many chemicals are also inherently hazardous and, therefore, represent potential risks to public health and safety in a malicious context. Improving security can be expensive,

but there are cost-effective steps that industry can take to reduce vulnerabilities. Unfortunately, the risk profiles of chemical plants differ tremendously because of differences in technologies, product mix, design, and processes. Therefore, no single, specific security regime would be appropriate or effective for all chemical facilities.

Many current statutes related to the handling of highly toxic substances were created decades ago and may no longer be effective for monitoring and controlling access to dangerous substances. For example, although licensed distributors of pesticides can only sell them to licensed purchasers, license requests, which are granted at the state level by county extension agents, are fairly easy to obtain. In addition, the basis for licensing varies from state to state.

As in most other industries, the chemical industry relies on the availability, continuity, and quality of service and supplies from other critical infrastructures. For example, the chemical industry is the Nation's third largest consumer of electricity. An assured supply of natural gas at competitive prices is another crucial resource for the sector.

Chemical Industry and Hazardous Materials Sector Initiatives

Currently, parts of the industry have taken positive, voluntary steps to protect sector infrastructure. For example, several trade associations have developed or are developing security codes[2] to help their members address the need to reduce vulnerabilities. These commendable efforts will make important contributions to protecting key elements of the chemical and hazardous materials infrastructure against terrorist attack. These efforts are in the early stages of implementation. However, it should be also noted that a significant percentage of companies that operate major hazardous chemical facilities do not abide by voluntary security codes developed by other parts of the industry.

Chemicals and hazardous materials sector protection initiatives include efforts to:

Promote enhanced site security

DHS, in concert with EPA, will work with Congress to enact legislation that would require certain chemical facilities, particularly those that maintain large quantities of hazardous chemicals in close proximity to population centers, to undertake vulnerability assessments and take reasonable steps to reduce the vulnerabilities identified.

Review current laws and regulations that pertain to the sale and distribution of pesticides and other highly toxic substances

EPA, in consultation with DHS and other federal, state, and local agencies, as well as with other appropriate stakeholders, will review current practices and existing statutory requirements on the distribution and sale of highly toxic pesticides and industrial chemicals. This process will help identify whether additional measures may be necessary to address security issues related to those substances.

Continue to develop the chemical ISAC and recruit sector constituents to participate

The purpose of the chemical sector's ISAC, which is in the early stages of development, is to facilitate advanced warnings on security threats and the sharing of other security-related data. DHS and EPA, in concert with chemical industry officials, will promote the ISAC concept within the sector in order to draw increased participation from the industry at large.

---

1 Specific chemical and hazardous materials facilities may fall within the definitional context of "key assets," however, their specific protection issues relate directly to the entire sector and are therefore discussed in this chapter.

2 For example, the American Chemistry Council's Responsible Care® Security Code of Management Practices.

POSTAL AND SHIPPING

Americans depend heavily on the postal and shipping sector. Each day, we place more than two-thirds of a billion pieces of mail into the U.S. postal system; and each day more than 300,000 city and rural postal carriers deliver that mail to more than 137 million delivery addresses nationwide. In all, the vast network operated by the United States Postal Service (USPS) consists of a headquarters in Washington, D.C., tens of thousands of postal facilities nationwide, and hundreds of thousands of official drop-box locations. USPS employs more than 749,000 full-time personnel in rural and urban locations across the country and generates more than $60 billion in revenues each year. Together, USPS and private-industry mailing and shipping revenues exceed $200 billion annually.

The postal system is highly dependent on and interconnected with other key infrastructure systems, especially the transportation system. USPS depends on a transportation fleet composed of both service-owned and contactor-operated vehicles and equipment. Mail also travels daily by commercial aircraft, truck, railroad, and ship. Because of these dependencies, many key postal facilities are collocated with other transportation modalities at various points across the United States.

The expansiveness of the national postal facilities network presents a significant, direct protection challenge. Additionally, the size and pervasiveness of the system as a whole have important implications in terms of the potential secondary effects of a malicious attack. The Fall 2001 anthrax attacks underscore this concern. In addition to localized mail stoppages across the U.S., the tainted mail caused widespread anxiety that translated into significant economic impact.

Historically, the American public has placed great trust, confidence, and reliance on the integrity of the postal sector. This trust and confidence are at risk when the public considers the mail service to be a potential threat to its health and safety. Consequently, USPS continues to focus on the specific protection issues facing its sector and is working diligently to find appropriate solutions to increase postal security without hampering its ability to provide fast, reliable mail service.

Postal and Shipping Sector Challenges

The protection challenges and initiatives discussed in this section relate specifically to the efforts undertaken by USPS. Commercial postal and shipping companies are in the process of organizing themselves as a sector to identify and address specific protection issues within their industry. While the USPS has worked with many of these companies to address critical infrastructure protection issues, there is further work to be done in this area. Assisted by USPS, DHS will engage the industry's major players in an effective dialogue to address critical infrastructure protection issues that cross the entire sector.

USPS has identified five areas of concern for the postal system:

- Points of entry and locations of key facilities;
- The mail's chain of custody;
- Unique constitutional and legal issues;
- Interagency coordination; and
- The ability to respond in emergency situations.

The fact that there are numerous points of entry into the postal system complicates its protection. Compounding this problem is the fact that these access points are geographically dispersed, including the multitude of postal drop boxes nationwide. Effective, affordable technology to scan mail and provide early warning of potential hazards is under current evaluation.

The location of many key postal service facilities can also aggravate risk-management challenges. Several major USPS facilities are collocated with or adjacent to other government agencies or major transportation hubs. Relocating these facilities to mitigate risk is often constrained by limited resources, a lack of available, alternative sites, and other pressing local imperatives.

Another factor affecting postal security is the fact that USPS does not always maintain control of the mail during its entire chain of custody. Oftentimes, independent contractors transport mail for USPS. Because USPS utilizes hundreds of long-haul mail carriers, mail moves into and out of USPS control along its route. To address this issue, USPS transportation purchasing requirements call for all transportation vendors, their employees, and subcontractors to submit to criminal and drug background checks. These checks include fingerprinting and follow-up if necessary by the Postal Inspection Service.

USPS security efforts face constitutional and legal challenges that are unique to the postal and shipping sector. Specifically, the Fourth-Amendment prohibition of unreasonable search and seizure and the sanctity of the postal seal make it necessary to justify the scanning or x-ray of a parcel for hazardous materials. Regardless, some technology vendors resist developing or marketing advanced sensing equipment out of concern that they would be held liable if their device failed to detect an actual threat. The *Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act*, enacted as part of the *Homeland Security Act of 2002*, reduces these risks by providing strong product liability protection for manufacturers of anti-terrorism devices.

Ensuring that USPS is able to respond effectively in emergency situations is another challenge for the sector. While USPS has worked extensively with vendors and the White House Office of Science and Technology Policy to develop solutions, currently there is no recognized set of standards to guide USPS and the private shipping industry in evaluating products for detecting, decontaminating, and remediating the effects of certain hazards. Furthermore, there are inadequate stockpiles of equipment and materials to enable sustained response activities. For instance, the supply of chemicals used to decontaminate facilities affected by the Fall 2001 anthrax incidents depended on a few companies, each of which produces only one of the compound's constituent parts.

In responding to the anthrax incidents, USPS worked with various federal agencies and state and local governments and continues to coordinate and plan with these groups. Further coordination and planning will be necessary to ensure that protection measures developed are effective across the entire sector. The federal authority to implement certain protective and response measures related to the actual or potential transmission of certain biological agents across state lines is not widely understood. Resolving these ambiguities in advance of a crisis situation would contribute greatly to the coordination of protection and emergency response efforts.

Postal and Shipping Sector Initiatives

DHS will work with private shipping and mail firms to enable them to incorporate their protection issues into a more comprehensive approach to critical infrastructure protection for this sector.

Additionally, the USPS has outlined six core initiatives in its emergency preparedness plans: prevention; protection and health-risk reduction; detection and identification; intervention; decontamination; and investigation. Specific key action areas that support these initiatives include efforts to:

Improve protection and response capabilities

DHS and USPS will conduct planning to increase reserve stockpiles of equipment and materials needed for emergency-incident response, particularly for CBR contaminants. They will also review requirements for manufacturing surge capacity for certain materials.

DHS and USPS will also work with other federal agencies and state and local authorities to facilitate coordinated planning efforts to develop and implement risk avoidance and reduction measures, as well as to establish common protocols for incident response and remediation.

Assure security of international mail

DHS and USPS will work with other appropriate agencies to clarify and formalize responsibilities for assuring the security of mail transiting U.S. borders, both inbound and outbound (e.g., between the USPS and U.S. Customs Service).

Promote and support ISAC participation

DHS will promote the postal and shipping sector's participation within an appropriate information sharing structure. This structure must include key government- and private-sector stakeholders involved with the delivery of air and ground mail, private parcels, and heavy cargo.

Conduct enhanced risk analyses of key facilities

DHS, USPS, and U.S. Postal Inspection Service will conduct assessments of postal facilities that are collocated with other high-risk facilities requiring more thorough risk analyses. These more rigorous assessments, which must take into account terrorist capabilities and motivations and facility vulnerabilities, will provide both indications and justification for the relocation of high-risk USPS facilities.

Improve customer identification and correlation with their mail

USPS will implement customer identification and correlation mechanisms at designated mail intake points and improve passive, nonintrusive parcel inspections for the detection of hazardous material.

Identify conflicts with respect to coordinated multi-jurisdictional responses

DHS, USPS, and DOJ will work together with state and local governments to identify and address conflicts in federal, state, and local laws and regulations that impair the abilities of multi-jurisdictional entities, like the USPS, to respond effectively in emergency situations.