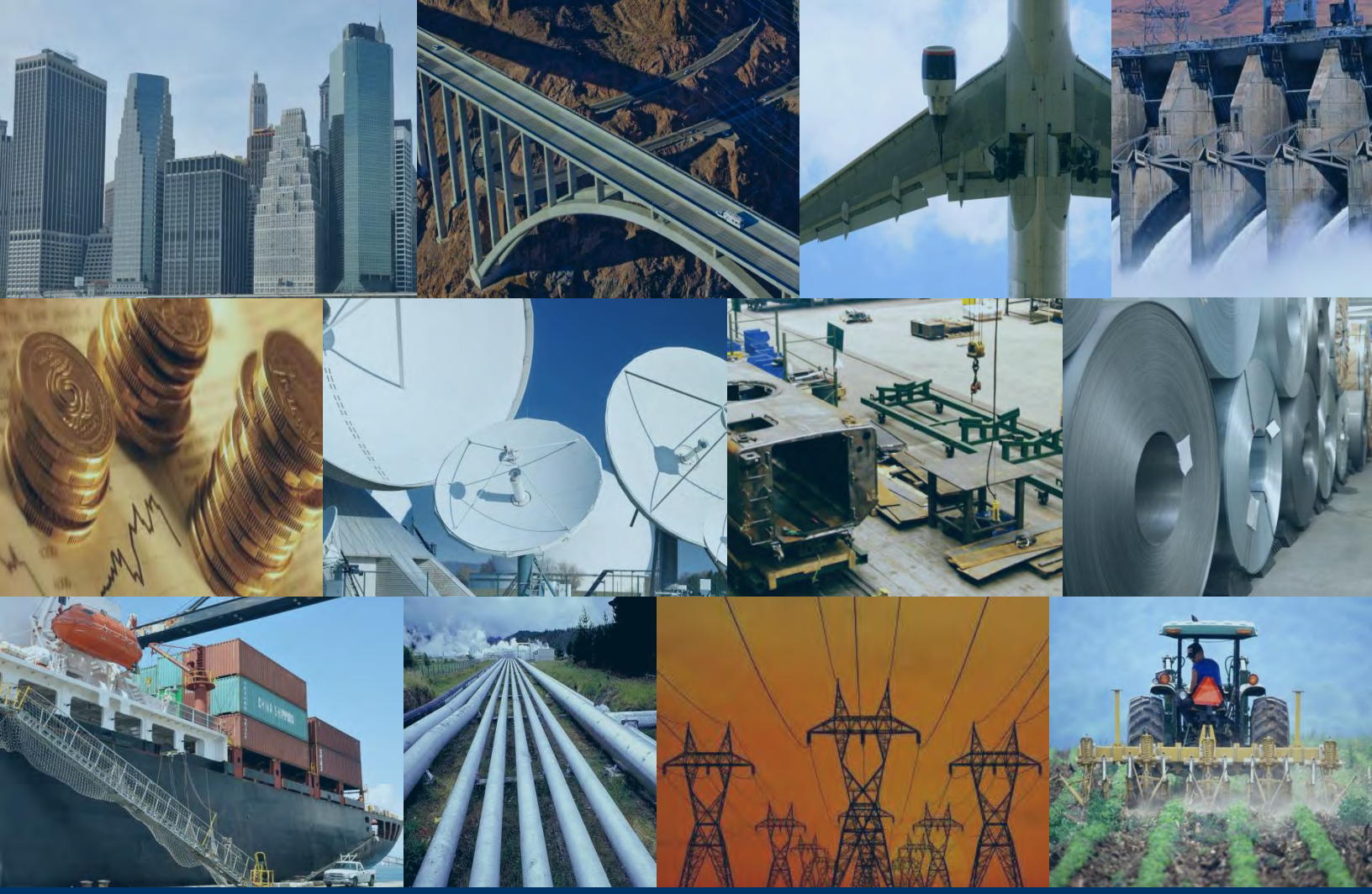


Sector Risk Snapshots

May 2014

Homeland Security

Sector Risk Snapshots

Introduction

Ensuring the security and resilience of critical infrastructure—those assets, systems, and networks that underpin American society—is essential to the Nation's security, public health and safety, economic vitality, and way of life. Managing risks to critical infrastructure requires an integrated approach across the whole-of-community to:

- Identify, deter, detect, and prepare for threats and hazards to the Nation's critical infrastructure;
- Reduce vulnerabilities of critical assets, systems, and networks; and
- Mitigate the potential consequences to critical infrastructure of incidents or adverse events that do occur.

Mission

Strengthen the security and resilience of the Nation's critical infrastructure by managing physical and cyber risks through the collaborative and integrated efforts of the critical infrastructure protection community.

National Infrastructure Protection Plan (NIPP), 2013

Presidential Policy Directive 21 (*PPD-21)* on *Critical Infrastructure Security and Resilience*, builds on the extensive work done to date to protect critical infrastructure, and identifies 16 critical infrastructure sectors:

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems

This compendium of Sector Risk Snapshots provides a brief overview and risk profile of the 16 critical infrastructure sectors, the Education, Electric, and Oil and Natural Gas Subsectors, and the seven Transportation Systems Modes. The Snapshots provide an introduction to the diverse array of critical infrastructure sectors, touching on some of the key threats and hazards concerning the sectors, and highlighting the common, first-order dependencies and interdependencies between sectors. The Snapshots are intended to serve as quick reference aids for homeland security partners, particularly State and local partners, and fusion center analysts, and each Snapshot includes a list of resources that partners can go to for more comprehensive sector information.

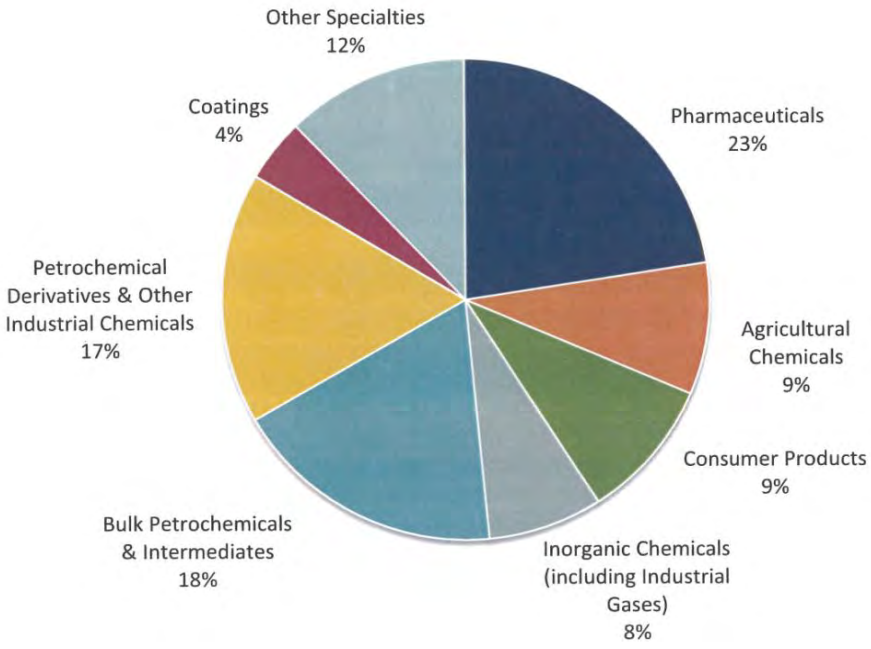
Prepared by the DHS Office of Cyber and Infrastructure Analysis (OCIA). For more information, contact OCIA at OCIA@hq.dhs.gov or visit our Website at www.dhs.gov/office-cyber-infrastructure-analysis.

Homeland Security

Chemical Sector Sector Risk Snapshot

Figure 1: Approximately 13,500 Chemical Manufacturing Facilities are in the U.S., owned by more than 9,000 Companies. *Source: Environmental Protection Agency (EPA, 2011)*

Figure 2: Global Chemical Shipments by Segment (as a percent of total shipments)



Chemical Sector Overview

- **The Chemical Sector is an integral component of the U.S. economy, employing nearly 1 million people, and earning annual revenues between $600 and $700 billion.**
- **Chemical Sector facilities typically belong to one or more of four key functional areas: (1) manufacturing plants, (2) transport systems, (3) warehousing and storage systems, and (4) chemical end users. In addition, companies may operate facilities across multiple functional areas, for example, a chemical manufacturer may also own a trucking and distribution operation.**
- **While the key functional areas primarily describe their physical characteristics and activities, each of the four functional areas depends on cybersystems for a variety of purposes, including operating manufacturing processes, tracking inventory, and storing customer information.**
- **As one of the oldest industries in the country, the chemical industry has a long history of resilience, based on the sector's ability to adapt to, prevent, prepare for, and recover from all hazards, including natural disasters, fluctuating markets, or a change in regulatory programs.**
- **To maintain operational resilience, successful businesses identify their critical dependencies and interdependencies and develop appropriate strategies to manage critical systems disruptions, should they occur.**
- **The DHS Chemical Facility Anti-Terrorism Standards (CFATS) program identifies and regulates high-risk chemical facilities to ensure they have security measures in place to reduce the risks associated with these chemicals. Upon review of more than 44,000 preliminary assessments from facilities with chemicals of interest, 4,275 facilities are now covered by CFATS (DHS, 2013).**

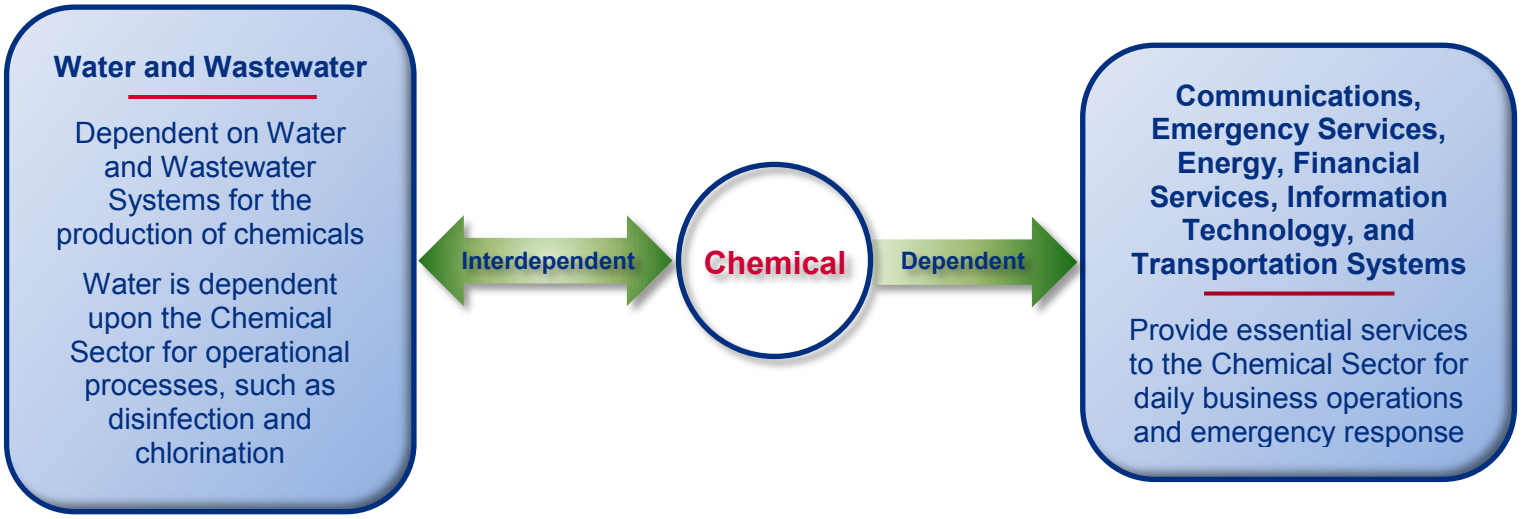
Threats and Hazards of Significant Concern

- **Cyberthreats**
  - The Chemical Sector is vulnerable to the threat of malicious actors physically or remotely manipulating network-based systems designed to control chemical manufacturing processes or process safety systems.
  - The physical disruption inflicted upon industrial assets in 2010 by the Stuxnet worm is evidence that control systems are vulnerable to increasingly destructive attacks and that the U.S. critical infrastructure may face cyberattacks of increasing sophistication.
- **Insider Threat**
  - While a facility can increase its physical security measures substantially, insiders with access who choose to intentionally cause harm will continue to contribute risk to the Chemical Sector. (CFATS, 2010, www.federalregister.gov/articles/2010/04/13/2010-8312/national-protection-and-programs-directorate-chemical-facility-anti-terrorism-standards-personnel#h-10)
  - Factors that improve management of this risk include greater cooperation and less competition among owners and operators within the sector and relatively higher cooperation between owners and operators and their workforces. (NIAC, *Insider Threat*, 2008, www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf)
- **Natural Disasters and Accidents**
  - Natural disasters and accidents contribute to the ongoing risk of exposing the environment and the population to chemicals.
  - Accidents such as the 2013 West Fertilizer Company explosion—an ammonium nitrate explosion that resulted in 15 deaths, over 160 injuries, and more than 150 damaged or destroyed buildings in West, Texas—demonstrate the significant potential consequences of incidents involving harmful chemicals.

For More Information

- Sector-Specific Agency: DHS, Office of Infrastructure Protection, chemicalsector@hq.dhs.gov and www.dhs.gov/chemical-sector
- DHS, *National Risk Pro*file, OCIA@hq.dhs.gov.
- National Infrastructure Protection Plan, www.dhs.gov/national-infrastructure-protection-plan
- Maritime Transportation Security Act of 2002, www.tsa.gov/assets/pdf/MTSA.pdf
- Chemical Facility Anti-Terrorism Standards (CFATS), www.dhs.gov/chemical-facility-anti-terrorism-standards

Figure 3: Common, First-order Dependencies and Interdependencies of the Chemical Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Commercial Facilities Sector
Sector Risk Snapshot

Critical Infrastructure Protection Issues

- Owners and operators are responsible for the day-to-day protection of commercial facilities, in close cooperation with local law enforcement.
- The Government has various programs and efforts to support the protection of commercial facilities. Activities include providing timely threat indications and warnings, and working with organizations to identify vulnerabilities and mitigate risks through protective programs and training.
- Given the national-level visibility and potential human and economic consequences of prominent commercial facilities, it is important for the Federal Government and the Commercial Facilities Sector to work together to ensure the protection of the Nation's prominent business centers and public gathering places.

The Department of Homeland Security oversees the implementation and execution of protective measures programs across the Commercial Facilities Sector. Some of the programs currently underway include:

Risk Self-Assessment Tool (RSAT): Delivers an all-hazard analysis of a facility's current risk level and offers options for consideration on reducing and managing potential vulnerabilities.

Protective Security Advisor (PSA) Program: PSAs are critical infrastructure protection and vulnerability assessment specialists with a wealth of anti-terrorism and security experience deployed across the U.S.

Bomb-making Materials Awareness Program (BMAP): Assist commercial retailers, commercial service providers, and chemical distributers/wholesalers in identifying suspicious purchases of materials used in home-made explosive or improvised explosive device manufacturing.

Protective Measures Guides: An overview of possible threats, vulnerabilities, and protective measures designed to assist facility owners and operators in planning and managing security specific to their venue to maintain a safer environment for guests and employees.

Suspicious Activity Videos: Designed to raise the level of awareness for hotel and retail employees by highlighting the indicators of suspicious activity.

Commercial Facilities Sector Overview

- **Commercial Facilities Sector operates on the principle of open public access, meaning that the general public can move freely throughout these facilities without the deterrent of highly visible security barriers.**
- **The majority of the facilities in this sector are privately owned and operated, with minimal interaction with the Federal Government and other regulatory entities.**
- **The Commercial Facilities Sector consists of the following eight subsectors:**

1. **Public Assembly (e.g., arenas, stadiums, aquariums, zoos, museums, convention centers);**
2. **Sports Leagues (e.g., professional sports leagues and federations);**
3. **Gaming (e.g., casinos);**
4. **Lodging (e.g., hotels, motels, conference centers);**
5. **Outdoor Events (e.g., theme and amusement parks, fairs, campgrounds, parades);**
6. **Entertainment and Media (e.g., motion picture studios, broadcast media);**
7. **Real Estate (e.g., office and apartment buildings, condominiums, mixed-use facilities, self-storage); and**
8. **Retail (e.g., retail centers and districts, shopping malls).**

Threats and Hazards of Significant Concern

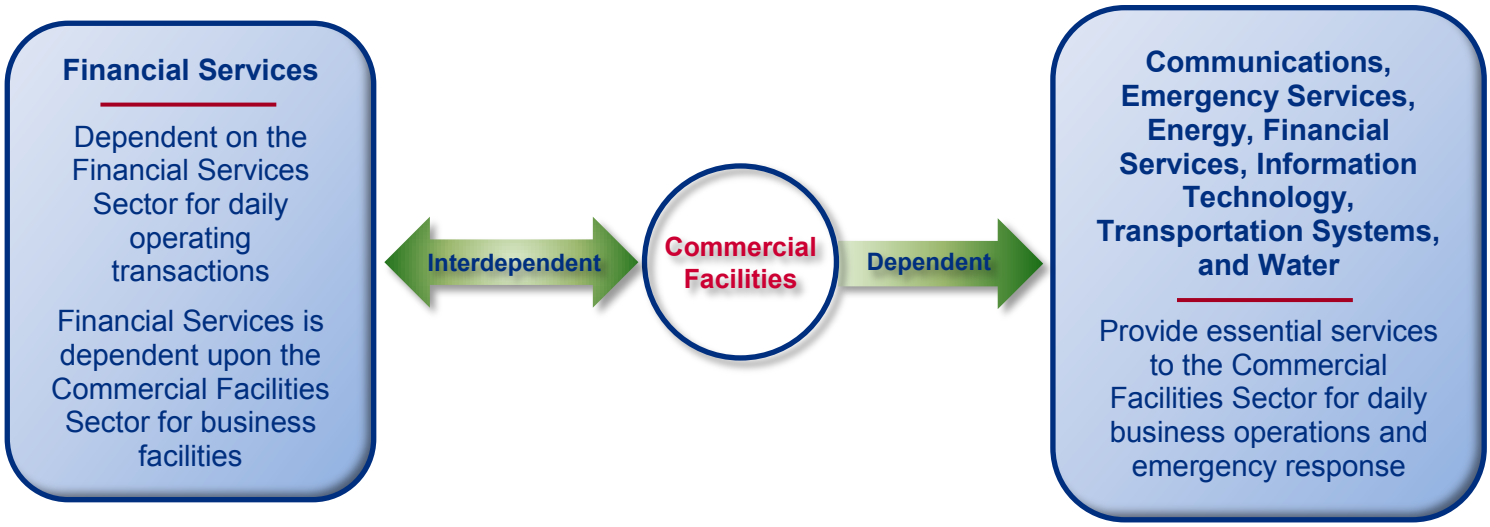
The Commercial Facilities Sector operates through a principle of open public access, which can increase the vulnerability to many types of attack methodologies. In addition, many Commercial Facilities Sector venues are highly recognizable, thus increasing the potential attractiveness to an adversary. These characteristics increase the risk to the Commercial Facilities Sector.

- **Bombings**
  - The adversary has expressed interest, and has a history of the use of explosive attacks against the Commercial Facilities Sector.
  - This attack methodology has the potential for creating mass casualties.
- **Active Shooter**
  - While a small arms attack may produce fewer casualties then an explosive attack, this attack methodology requires fewer resources and planning.
  - As in the case with bombings, the sector's open public access and population density make commercial facilities vulnerable to small arms attacks, resulting in an increased risk to the sector.
- **Chemical, Biological, Radiological (CBR) Attacks**
  - Some terrorist organizations have expressed interest in acquiring and using CBR weapons. Given the nature of mass gathering, and open public access of the Commercial Facilities Sector, there are unique vulnerabilities to either the distribution of CBR materials through ventilation systems or through liquid distribution in an open arena type environment.
  - Outdoor facilities, such as public assemblies or sporting events, are also at risk. Al-Qaeda has previously expressed interest in obtaining crop dusters, which could be used to disseminate aerosolized CBR agents over large areas and gatherings.

For More Information

- Sector-Specific Agency: DHS, Office of Infrastructure Protection, www.dhs.gov/commercial-facilities-sector
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov.
- Commercial Facilities Resources: www.dhs.gov/commercial-facilities-resources

Figure 1: Common, First-order Dependencies and Interdependencies of the Commercial Facilities Sector



May 2014

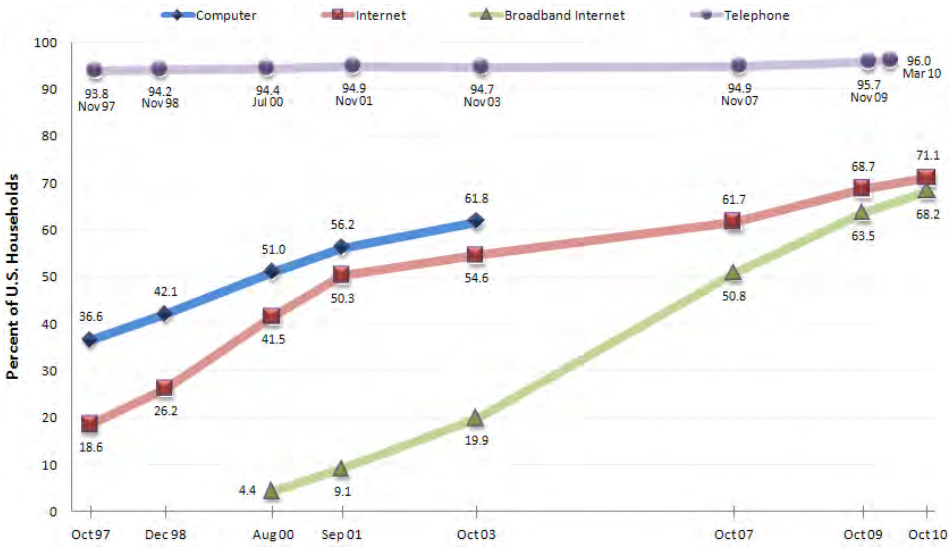
Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Communications Sector Sector Risk Snapshot

Figure 1: U.S. Households with Computers, Telephone Subscriptions, and Internet Access, Selected Years, 1997-2010



*Note: 2001-2012 use 2000 Census-based weights and earlier years use 1990 Census-based weights
Source: National Telecommunications and Information Administration, February 2011

Types of Communications Infrastructure

- **Wireline Communications**: Consists primarily of the public switched telephone network (PSTN) and includes cable networks and enterprise networks. Wireline networks also are being redefined by next generation networks (NGNs), which are high-speed, converged circuit-switched and packet-switched networks capable of transporting and routing a multitude of services, including voice, data, video, and other multimedia, across various platforms. The wireline component also includes the Internet infrastructure and submarine cable infrastructure.
- **Wireless Communications:** Consists primarily of cellular telephone, paging, personal communications services, high-frequency radio, unlicensed wireless, and other commercial and private radio services, including numerous law enforcement, public safety, and land mobile radio systems.
- **Satellite Communications:** Satellite communications systems deliver data, voice, and video services. Networks may be private and independent of the terrestrial infrastructure or may share common facilities (e.g., a teleport) and be combined with terrestrial services to deliver information to the intended recipient(s). Important satellite network components include ground stations; telemetry, tracking, and command links (TT&Cs); very small aperture terminals (VSATs); and data links.
- **Cable:** Cable communications systems are wireline networks that offer analog and digital video programming services, digital telephone service, and high-speed Internet access service. Cable systems use a mixture of fiber and coaxial cable that provide two-way signal paths to the customer.
- **Broadcasting:** Broadcasting systems consist of free, over-the-air radio and television stations that offer analog and digital audio and video programming services and data services.

Communications Sector Overview

- **The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government. Over the last 25 years, the Sector has evolved from predominantly a provider of voice services into a diverse, competitive, and interconnected industry, using terrestrial, satellite, and wireless transmission systems.**
- **The transmission of these services has become very interconnected; satellite, wireless, and wireline providers depend on each other to carry and terminate their traffic, and companies routinely share facilities and technology to ensure interoperability and efficiency.**
- **The private sector, as owners and operators of the majority of communications infrastructure, is the primary entity responsible for protecting Sector infrastructure and assets.**
- **Working with the Federal Government, the private sector is able to predict, anticipate, and respond to Sector outages and understand how they might affect the ability of the national leadership to communicate during times of crisis, impact the operations of other Sectors, and affect response and recovery efforts.**
- **The Communications Sector is closely linked to a number of other Sectors, including Energy, Information Technology, Financial Services, Emergency Services, and Postal and Shipping.**

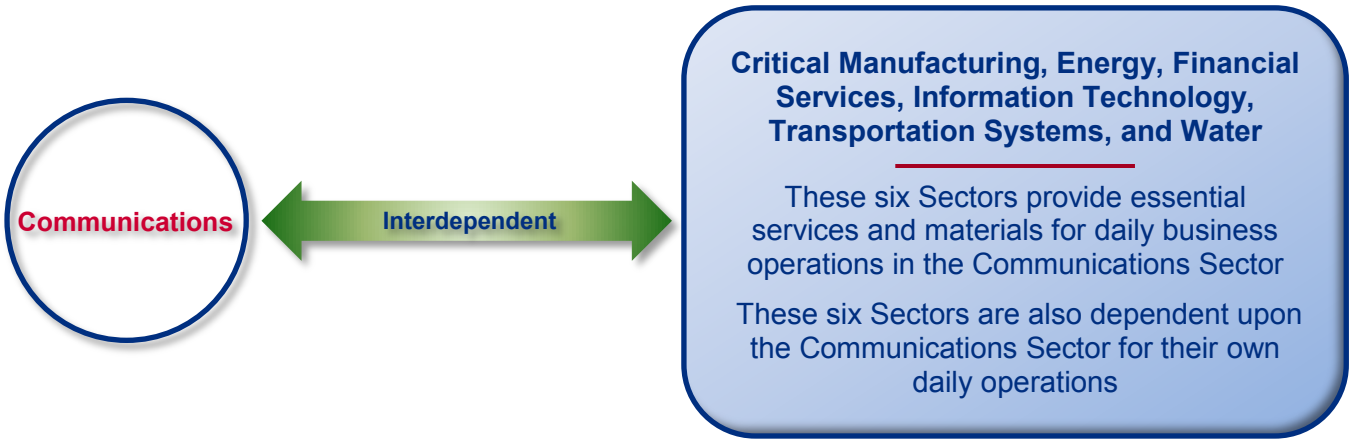
Threats and Hazards of Significant Concern

- **Single physical incidents**, such as nuclear detonations, major earthquakes, hurricanes, and space weather are likely to significantly disrupt the Sector over large regions. The Sector hardens systems and applies the principle of diversity (employing various primary and alternative routing and systems) and the principle of redundancy (using backup or multiple capabilities to sustain operations) to mitigate these and other threats (e.g., those that could cause potential damage to underground infrastructure from digging).
  - Space weather, such as severe solar geomagnetic storms, can cause high-power transformers to fail and electrical systems to possibly collapse. Because of the dependence of communications systems on electrical power, communications networks would soon fail in the event of a long-term, large-scale electrical network collapse. Solar weather can also directly degrade communications satellites and disrupt global positioning system (GPS) functionality (interfering with GPS satellites and their signals). Short-term loss or disruption of GPS will have minimal impacts on the underlying infrastructure, but medium- to long-term loss will degrade GPS-reliant services provided through the wireless, satellite, cable, and broadcast networks.
- **Cyber-disruptions** of communications systems present unique challenges due to global connectivity. The exploitation of vulnerabilities halfway around the world can begin affecting critical U.S. communications components in a matter of minutes.
- **Malicious actors** pose one of many human risks, which can impact data, networks, and components, as well as create financial losses for organizations.
  - The use of high-altitude electromagnetic pulse (EMP) weapons, source region EMP weapons, intentional electromagnetic interference devices, and high-energy radio frequency weapons could damage both electrical and communications systems.
  - Breached supply chain integrity could also result in disruption of service and network availability, loss of network control, loss of confidentiality and integrity of communications, unauthorized access, and disruption of emergency telecommunications, as well as fraud and theft of service.

For More Information

- Sector-Specific Agency: DHS, Office of Cybersecurity and Communications, www.dhs.gov/office-cybersecurity-and-communications
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS, www.dhs.gov/communications-sector

Figure 2: Common, First-order Interdependencies of the Communications Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Critical Manufacturing Sector
Sector Risk Snapshot

Figure 1: Manufacturing's Role in the U.S. Economy

* Exports data from 2010. R&D Data from 2009, the last available. All other data from 2011.
Source: U.S. Department of the Treasury

Several characteristics of today's manufacturing environment are common across each of the key functional areas within the Critical Manufacturing Sector. Examples include the following:

1. **Most manufacturing enterprises are integrated into complex, interdependent supply chains.** Few businesses operate independently. Nearly all manufacturers are part of a chain of suppliers, vendors, partners, integrators, contractors, and customers that link to other industries and businesses.
2. **Supply chains have been optimized for productivity and efficiency.** Competitive pressures cause businesses to optimize their manufacturing processes through highly coordinated business arrangements that enable manufacturers to maintain low inventories of raw materials and intermediate and end products.
3. **Manufacturers have become highly reliant on global information and communication systems.** Automation, control, information, processing, robotics, telecommunications, and the Internet have radically improved industrial productivity and have reshaped the operations and asset base of manufacturers.
4. **Globalization and outsourcing have linked U.S. manufacturers with foreign suppliers, vendors, and customers through highly interdependent supply networks.** Manufacturers have increasingly turned to foreign markets for raw materials, component manufacturing, equipment and machinery, labor, and customers as a way to reduce overall costs.
5. **Manufacturers rely heavily on energy sources for heat, power, and raw materials.** While all businesses are dependent on energy, manufacturers typically require large amounts of these resources, much of it in the form of hard-to-store electricity and natural gas.

Critical Manufacturing Sector Overview

- **The Critical Manufacturing Sector is crucial to the economic prosperity and continuity of the United States. Products designed, produced, and distributed by U.S. manufacturers make up 12 percent of the U.S. gross domestic product and directly employ nearly 12 million of the Nation's workforce.**
- **The Critical Manufacturing Sector identified the following industries to serve as the core of the Sector:**
  - **Primary Metal Manufacturing**
  - **Machinery Manufacturing**
  - **Electrical Equipment, Appliance, and Component Manufacturing**
  - **Transportation Equipment Manufacturing**
- **These key functional areas depend upon physical, cyber, and human elements to perform their missions:**
  - **Physical elements include the facilities supporting each functional area.**
  - **Human elements include the personnel associated with each function.**
  - **The cyber-elements include electronic systems for processing the information necessary for management and operation or for automatic control of physical processes.**
- **Each key functional area has unique markets, assets, business models, and competitive conditions that shape the critical manufacturing risk profile.**
- **Products made by these manufacturing industries are essential in varying capacities to many other critical infrastructure sectors.**

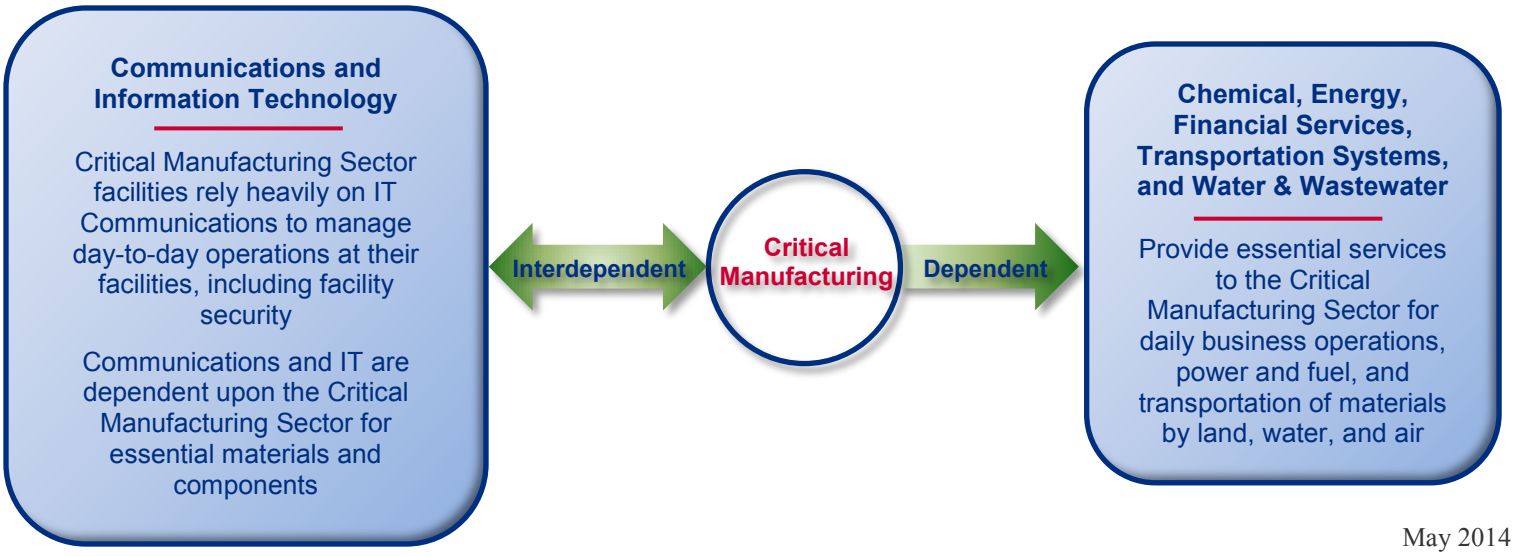
Threats and Hazards of Significant Concern

- **Supply Chain Vulnerability**
  - Supply chains at key inbound transportation nodes are of particular concern because incidents are likely at nodes, such as domestic ports. There is also a potential for large-scale consequences to the many industries that rely on the importation of materials and products.
  - Lean inventory and just-in-time practices, as well as greater distances from components or raw materials required for production to the delivery of finished products to markets, have made the Critical Manufacturing Sector more sensitive to transportation disruptions and fuel costs.
  - Supply chain systems are also more vulnerable because fewer basic metals and minerals are mined and processed in the United States, thereby increasing our dependence on foreign countries to provide these materials.
- **Cyberthreats**
  - Unauthorized on-site or remote intrusion into sector industrial control systems and supervisory control and data acquisition systems poses a growing threat and contributes to risk for the Critical Manufacturing Sector.
  - Supply chain systems are more vulnerable because of increased reliance on advanced information technology (IT) systems. Critical infrastructure owners and operators are also slow to adopt security and risk management measures for systems. Nation-states and other actors could potentially defeat competition and/or obtain competitive secrets through cyberintrusion.
- **Insider Threat**
  - The sector's systems are complex and increasingly dependent on information technology, making the sector highly susceptible to exploitation by current and former industry employees and contractors with malicious intent and unique knowledge of, and access to, these systems.
  - Threats posed by malicious insiders may include sabotage, theft or diversion, cyberattacks, or terrorism against critical manufacturing facilities.

For More Information

- Sector-Specific Agency: DHS, Office of Infrastructure Protection, www.dhs.gov/about-office-infrastructure-protection
- DHS, Sector Specific Profile: www.dhs.gov/critical-manufacturing-sector-critical-infrastructure
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov

Figure 2: Common, First-order Dependencies and Interdependencies of the Critical Manufacturing Sector



May 2014

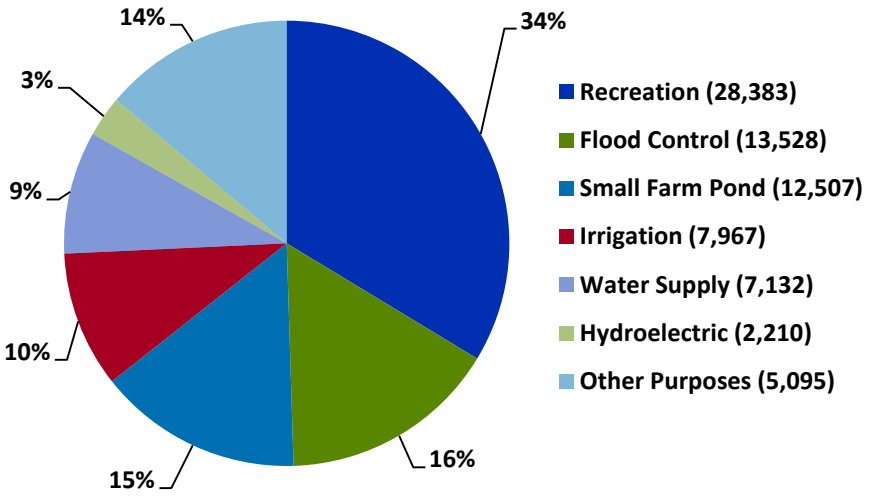
Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Dams Sector Sector Risk Snapshot

Figure 1: Primary Purpose or Benefit of U.S. Dams



Dams Sector assets are vital components of the Nation's infrastructure. Some examples of the benefits derived from sector assets are:

Water Storage and Irrigation: Dams create reservoirs that supply water for a multitude of industrial, municipal, agricultural, and recreational uses throughout the United States.

Electricity Generation: Dams in the United States produce more than 270,000 gigawatt-hours of the Nation's electricity, representing 70 percent of the Nation's renewable energy generation, and over 6 percent of U.S. electricity generation overall.

"Black Start" Capabilities: There are 4,316 megawatts of "incremental" hydropower available at sites with existing hydroelectric facilities. Incremental is defined as capacity additions or improved efficiency at existing hydro projects.

Recreation: Dams and other sector assets provide prime recreational facilities throughout the United States.

Navigation: The U.S. waterway system, which includes 236 lock chambers at 192 lock sites owned and/or operated by the U.S. Army Corps of Engineers (USACE).

Flood Risk Reduction: Many dams and levees function as flood control projects, thereby reducing the potential human health and economic impacts of flooding.

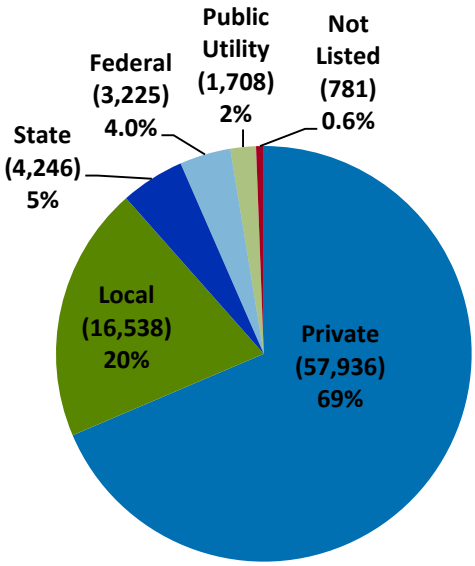
Sediment Control: Some dams enhance environmental protection by controlling detrimental sedimentation.

Impoundment of Mine Tailings and Industrial Waste Materials: More than 1,500 mine tailings and industrial waste impoundments controlled by dams in the Nation facilitate mining and processing of coal and other vital minerals.

Dams Sector Overview

- **The Dams Sector comprises assets that include dam projects, hydropower generation facilities, navigation locks, levees, dikes, hurricane barriers, mine tailings, industrial waste impoundments, and other similar water retention and water control facilities.**
- **The Dams Sector is a vital and beneficial part of the Nation's infrastructure. It continuously provides a wide range of economic, environmental, and social benefits, including hydroelectric power, river navigation, water supply, wildlife habitat, waste management, flood control, and recreation.**
- **There are more than 84,000 dams in the United States; approximately 69 percent are privately owned, and more than 85 percent are regulated by State dam safety offices.**

Figure 2: Dam Ownership in the U.S.



Source Figures 1-2: DHS, Dams Sector-Specific Plan, *2010, www.dhs.gov/dams-sector.*

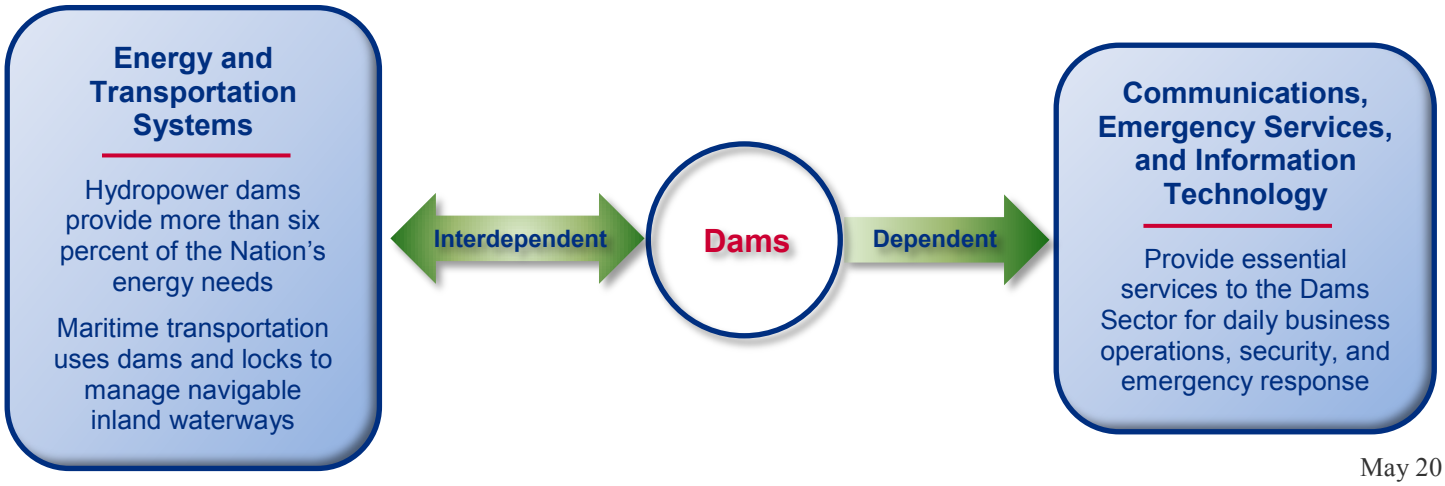
Threats and Hazards of Significant Concern

- **Natural Hazards**
  - Extreme flooding and severe storm surges can overwhelm the flood storage capacity of reservoirs and levee systems and lead to breaching or overtopping.
  - The consequences of extreme levee failure were seen in the aftermath of Hurricanes Katrina and Rita in 2005, which resulted in the deaths of more than 1,800 people and more than $200 billion in economic damages.
  - Earthquake ground motion may also lead to severe damage or failure, as evidenced by the failure of Fujinuma Dam in Japan following the Tōhoku earthquake in March 2011.
- **Malicious Actors**
  - With the necessary capabilities and resources, adversaries could potentially achieve catastrophic failure and severely disrupt missions through the use of improvised explosive devices (IEDs), increasing risk for the Sector.
  - Dams Sector assets have experienced at least 20 kinetic attacks worldwide over the last decade, and adversaries could exploit the inherent vulnerabilities of these public facilities (Source: National Consortium for the Study of Terrorism and Responses to Terrorism, Global Terrorism Database, 2011).
  - Adversaries could bypass land-based security measures with water-borne IEDs and strike dams, locks, or levees. Vehicle-borne IEDs (VBIEDs) could also reach the crest of dams or levees, particularly those with roads providing vehicular access. An assault team could overpower security forces, seize a facility's control room, and detonate IEDs, as occurred in a July 2010 attack against a Russian hydropower station.
  - The increasing use of standardized industrial control systems (ICS) technology increases the sector's potential vulnerability to direct cyberattacks and intrusions, which are a constant potential threat across the critical infrastructure community.
- **Aging Infrastructure**
  - Some dams, inland waterways, and levees are in increasingly poor condition as a result of aging, deterioration, and maintenance backlogs. This increases the risk to the Dams Sector, as its infrastructure continues to age.
  - The average age of the 84,000 dams in the country is 52 years old. The number of deficient dams is estimated at more than 4,000, which includes 2,000 deficient high-hazards dams. In addition, 91 percent of U.S. levees are not in acceptable condition (Source: American Society of Civil Engineers, *Infrastructure Report Card,* 2013).

For More Information

- Sector-Specific Agency: DHS, Office of Infrastructure Protection, www.dhs.gov/dams-sector
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov
- DHS, *Dams Sector: Roadmap to Secure Control Systems,*2010
- USACE, National Inventory of Dams, http://nid.usace.army.mil

Figure 3: Common, First-order Dependencies and Interdependencies of the Dams Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

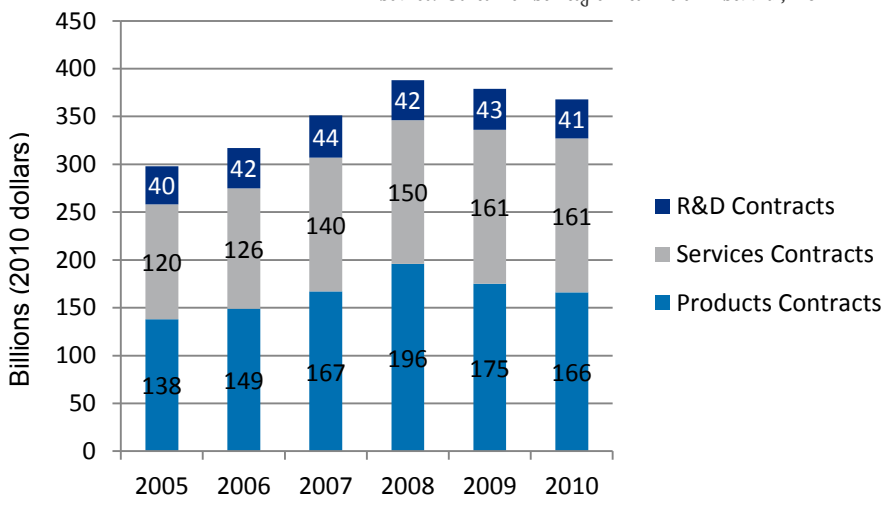
Homeland Security

Defense Industrial Base Sector
Sector Risk Snapshot

The Defense enterprise is the largest and most complex organization in the world. In addition to managing roughly three million employees, a budget of more than $600 billion, operating almost 5,000 locations, and providing healthcare for 9.6 million military members, retirees, and their families, the DOD also executes a multibillion dollar global supply chain that manages an inventory of five million line items.

Figure 1: U.S. Department of Defense Contract Spending and the Supporting Industrial Base

Source: Center for Strategic International Studies, 2011



Defense Industrial Base Sector Goals

Sector Risk Management: Use an all-hazards approach to manage the risk-related dependency on critical DIB assets.

Collaboration, Information Sharing, and Training: Improve collaboration within a shared knowledge environment in the context of statutory, regulatory, proprietary, and other pertinent information-sharing constraints and guidance.

Personnel Security: Mitigate the risk created by personnel with unescorted physical or logical access to critical DIB assets in conformance with pertinent industry best practices, including regulatory and statutory requirements.

Physical Security: Manage the risk created by threats to and vulnerabilities of critical DIB physical assets.

Information Security [Cybersecurity/Information Assurances (CS/IA)]: Manage risk to information that identifies or describes characteristics or capabilities of DIB critical infrastructure and key resources, or that by nature would represent a high risk/high impact to critical infrastructure, resources, or DIB assets.

Defense Industrial Base Sector Overview

- **The Defense Industrial Base (DIB) is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts to meet U.S. military requirements.**
- **Only a small fraction of DIB facilities are DOD-owned. The government component of DIB consists of certain laboratories, special-purpose manufacturing facilities, capabilities for production of uniquely military material such as arsenals and ammunition plants, and other services.**
- **The private sector component of the DIB consists of hundreds of thousands of independent, competing domestic and foreign companies and supply chains, delivering a vast array of products and services to DOD. DIB defense-related products and services equip, inform, mobilize, deploy, and sustain U.S. military and allied military forces worldwide. The DIB companies also deliver national security products and services to other Federal agencies.**
- **DIB does not include commercial infrastructure, such as communications, transportation, power, or other utilities, which serve as critical dependencies of the DIB Sector.**
- **The DIB Sector vision is to collaboratively eliminate or mitigate unacceptable levels of risk to physical, human, and cyber infrastructures, thus ensuring that DOD continues to fulfill its mission, and that DIB activities supporting national security objectives, public health and safety, and public confidence are effective.**

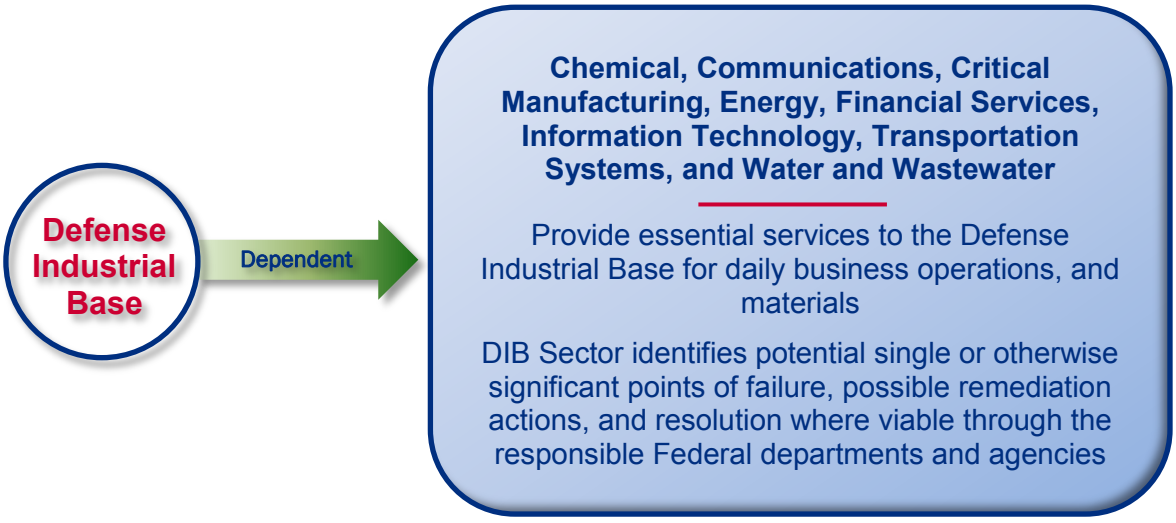
Threats and Hazards of Significant Concern

- **Cyberthreats**
  - The DIB Sector has become heavily dependent on cyber infrastructure, operating within an increasingly information-driven environment.
  - Cyber infrastructure is vulnerable to denial-of-service attacks and malicious modification of information, along with more mundane yet disruptive events, such as system malfunctions, power outages, and human error.
  - These vulnerabilities, combined with the increasing frequency and severity of cyberattacks across the critical infrastructure community, contribute greatly to the risk to the Sector. Foreign entities and non-state actors are also expected to continue seeking to acquire access to sensitive and classified DIB Sector information and technologies by expanding their cyber-collection activities [DOD, *Strategy for Operating in Cyberspace*, July 2011].
- **Loss of Supply Chain Integrity**
  - Due in part to a lack of traceability from foreign producers, potential loss of supply chain integrity (including related manufacturing and material availability) increases risk for the Sector.
  - This is highlighted by the ongoing infiltration of counterfeit electronics into the Sector. Lack of supply chain integrity could lead to the introduction of counterfeit materials, components, and technology into military equipment, which could, in turn, lead to equipment failures and increase risk in the field.

For More Information

- Sector-Specific Agency: Department of Defense, www.defense.gov
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS, www.dhs.gov/defense-industrial-base-sector
- Defense Industrial Base, *Sector Specific Plan (SSP),* 2010, www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base-2010.pdf
- DOD, Defense Critical Infrastructure Program (DCIP), http://dcip.dtic.mil/index.html

Figure 2: Common, First-order Dependencies of the Defense Industrial Base Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Energy Sector
Electricity Subsector
Sector Risk Snapshot

Figure 1: U.S. Electric Transmission Grid

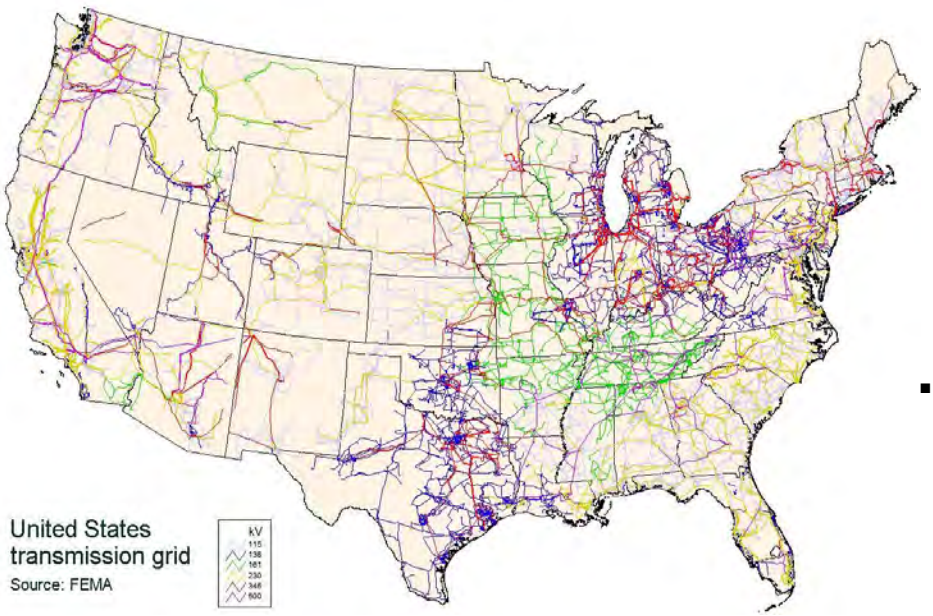
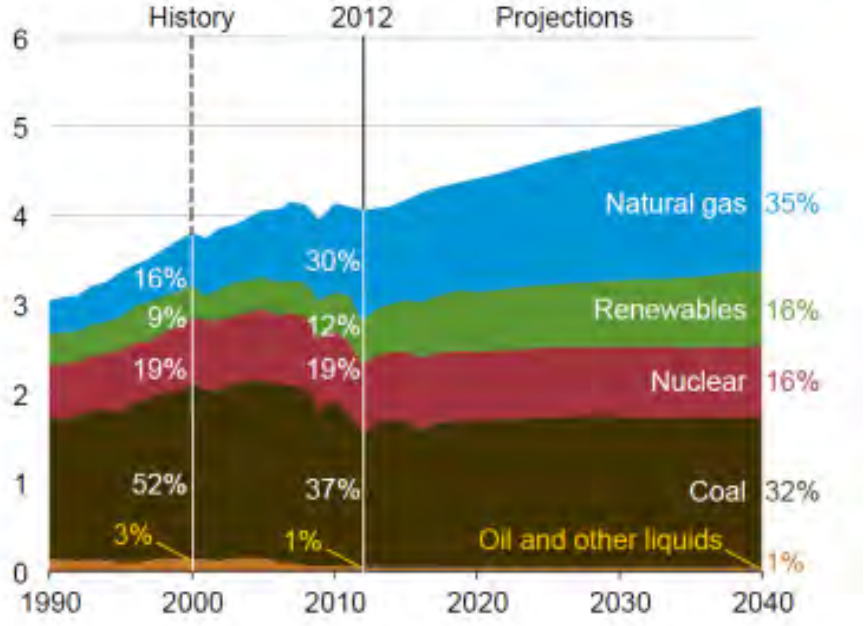


Figure 2: U.S. Electricity Generation by Fuel, 1990-2040 (trillion kilowatt hours)



Source: EIA, *Annual Energy Outlook Early Release Overview*, December 16, 2013, www.eia.gov/forecasts/aeo/er/index.cfm.

Electricity Subsector Overview

- **U.S. energy infrastructure fuels the economy of the 21st century. Without a stable energy supply, health and welfare are threatened, and the U.S. economy cannot function. More than 80 percent of the country's energy infrastructure is owned by the private sector, supplying fuels to the transportation industry, electricity to households and businesses, and other sources of energy that are integral to the Nation's growth and production.**
- **The Energy Sector is divided into three interrelated segments: electricity, petroleum, and natural gas. According to the Energy Information Administration (EIA), in 2011 there were 18,530 power generation facilities with a combined nameplate capacity of 1,153 gigawatts.**
- **More than 98 percent of electricity is generated domestically, although some significant regional differences exist and some of the fuels used to generate electricity are imported.**
- **The primary fuel for electric power generation is coal (37 percent), followed by natural gas (30 percent), nuclear (19 percent), renewable energy sources such as hydro, solar, or wind (12 percent), and other (1 percent). (Source: EIA, 2013)**
- **The electricity infrastructure is highly automated and controlled by utilities and regional grid operators, using sophisticated energy management systems, such as supervisory control and data acquisition systems (SCADA) or distributed control systems, to keep the system in balance.**
- **The reliance of virtually all industries and modes on electric power means that all Sectors have some dependence on the Energy Sector.**

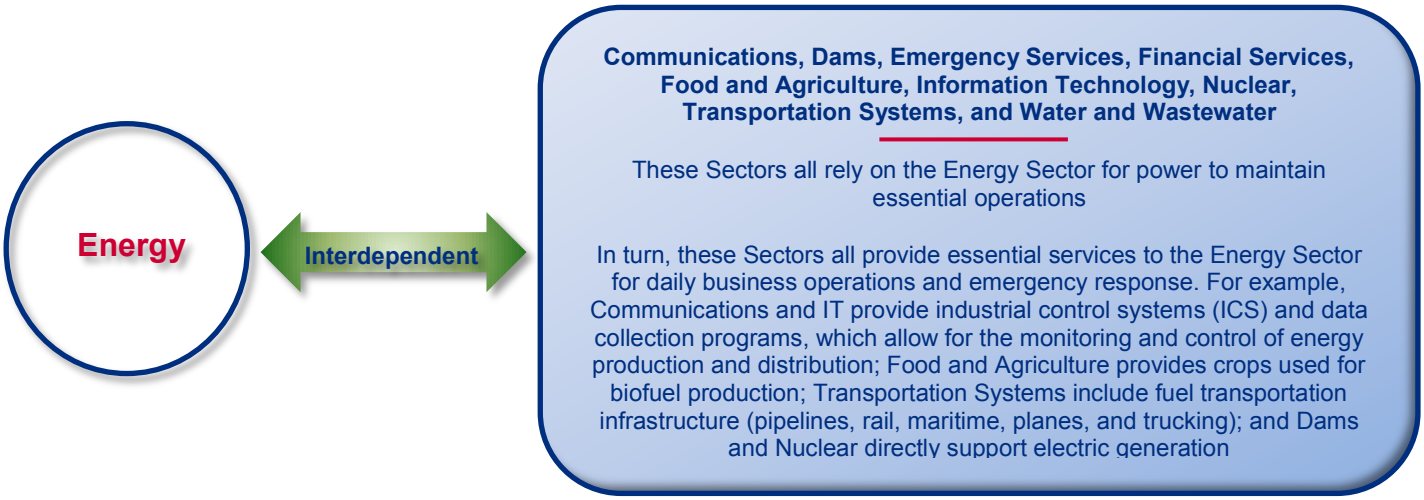
Threats and Hazards of Significant Concern

- **Cyberthreats**
  - Electricity infrastructure is highly automated and controlled by utilities and regional grid operators that rely on sophisticated energy management systems. For example, assets may be vulnerable if the Electricity Subsector's control system networks are connected to the corporate business network, which, in turn, is connected to the Internet. These connections increase the network's vulnerability to direct cyberattacks that could potentially disrupt power and increase risk to the Sector.
  - Insider threats, such as cyber-hacks initiated by current or former employees, increase the risk to the Electricity Subsector. These vulnerabilities are addressed to varying degrees across the Electricity Subsector, through a mix of voluntary and mandatory security standards that apply to electricity grid owners and operators.
- **Physical Attacks**
  - Physical attacks are a risk for the Sector's continued reliable operations. Coordinated physical attacks in the United States could produce wide-ranging impacts to both infrastructure and the reliability of the system.
  - Worldwide, terrorists have executed 2,523 attacks against energy infrastructure since 2004, leaving 1,852 dead and 4,653 wounded (National Counterterrorism Center, *Worldwide Incident Tracking System*, 2011). Moreover, successful strikes against individual Sector assets could lead to regional or nationwide impacts.
- **Natural Disasters**
  - Natural events, such as hurricanes, earthquakes, winter storms, wildfires, and solar flares, are a key risk of the Electricity Subsector, as these events occur regularly and have the capacity to cause extensive and widespread damage, impacting an area from days to weeks.
  - As all other Sectors have some degree of dependency upon the Electricity Subsector for normal operations, electric power restoration is a top priority following a natural disaster.

For More Information

- Sector-Specific Agency: Department of Energy, http://energy.gov/
- EIA, www.eia.gov
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS, www.dhs.gov/energy-sector

Figure 3: Common, First-order Interdependencies of the Energy Sector



May 2014

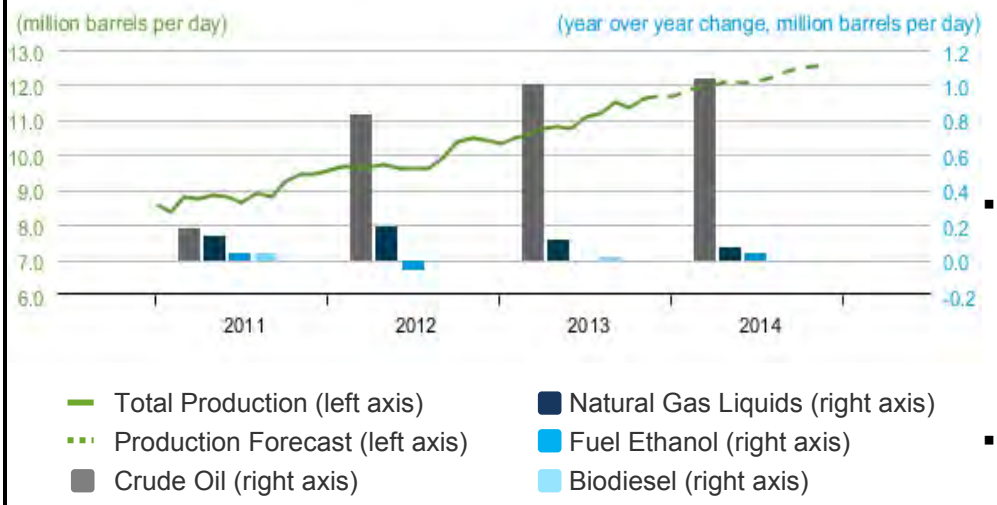
Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

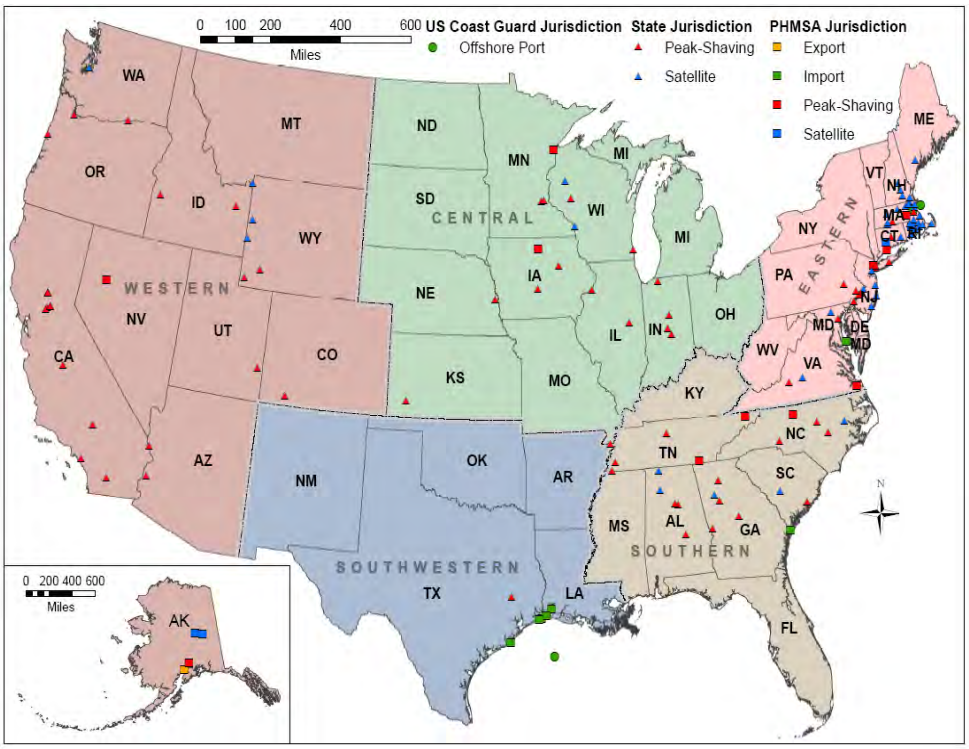
Energy Sector
Oil and Natural Gas Subsector
Sector Risk Snapshot

Figure 1: U.S. Crude Oil and Liquid Fuels Production



Source: U.S. Energy Information Administration, Short-Term Energy Outlook, 2013

Figure 2: U.S. Liquefied Natural Gas (LNG) Facilities Connected to Natural Gas Pipeline Systems



Source: U.S. Department of Transportation

Oil and Natural Gas Subsector Overview

- The petroleum section entails the exploration, production, storage, transport, and refinement of crude oil. The crude oil is refined into petroleum products that are then stored and distributed to key economic sectors throughout the United States.
- Key petroleum products include motor gasoline, jet fuel, distillate fuel oil, residual fuel oil, and liquefied petroleum gases. In the United States, there are more than 536,000 crude oil-producing wells, 30,000 miles of gathering pipeline, and 55,000 miles of crude oil pipeline.
- There are 150 operable petroleum refineries, 64,000 miles of product pipeline, and over 1,400 petroleum terminals.
- Natural gas is produced, piped, stored, and distributed in the United States. Imports of liquefied natural gas (LNG) fell 23 percent in 2012 due to unprecedented levels of domestic natural gas production, and companies are now applying to the Department of Energy to export domestic LNG to foreign countries. There are more than 514,000 gas production and condensate wells and 19,000 miles of gathering pipeline in the United States. There are almost 304,000 miles of interstate and intrastate pipeline for the transmission of natural gas.
- Natural gas is distributed to homes and businesses over 1,200,000 miles of distribution pipelines. The heavy reliance on pipelines to distribute products across the Nation highlights the interdependencies between the Energy and Transportation Systems Sectors.
- The reliance of virtually all industries and modes on fuels means that all Sectors have some dependence on the Energy Sector.

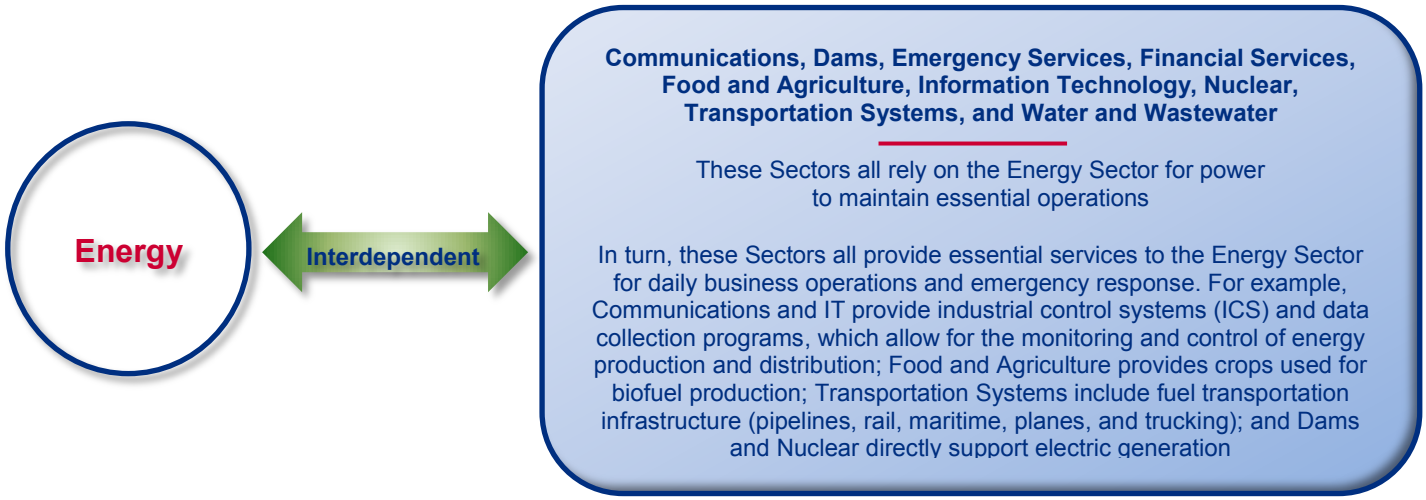
Threats and Hazards of Significant Concern

- **Cyberthreats**
  - Oil and natural gas infrastructure is highly automated and controlled by pipeline operators, terminal owners, and natural gas utilities that rely on sophisticated energy management systems. Assets may be vulnerable if these industrial control systems are connected to the Internet, either directly or indirectly. For example, control system networks may be connected to the corporate business network, which, in turn, is connected to the Internet. These connections increase the network's vulnerability to direct cyberattacks that could potentially disrupt movement and increase risk to the Sector.
  - Insider cyberthreats, such as those initiated by current or former employees, create risk to the Oil and Natural Gas Subsector. Cyber-actors can target industrial control systems (ICS) and gain control of a process within a refinery, pipeline, or terminal. A cyber-actor could manipulate the production, storage, and transportation aspects of oil and natural gas. These vulnerabilities are addressed to varying degrees across the Oil and Natural Gas Subsector, through a mix of voluntary and mandatory security standards that apply to owners and operators.
- **Physical Attacks**
  - Physical attacks are a risk for the Sector's continued reliable operation. Coordinated physical attacks in the United States could produce wide-ranging impacts to both infrastructure and the reliability of the system.
  - Worldwide, terrorists have executed 2,523 attacks against energy infrastructure since 2004, leaving 1,852 dead and 4,653 wounded (National Counterterrorism Center, *Worldwide Incident Tracking System*, 2011). Successful strikes against individual Sector assets could lead to cascading regional or nationwide impacts.
- **Natural Disasters**
  - Many natural disasters can affect the Oil and Natural Gas Subsector. Hurricanes are the most frequent disruptive natural hazard for the Subsector, often causing the preemptive shutdown of facilities in an area, even if the facilities themselves are not directly affected by the storm. Hurricanes Ike and Gustav impacted almost 65 million barrels of crude oil production and 400 billion cubic feet of the natural gas supply (Energy Information Administration, *2010 Outlook for Hurricane-Related Production Outages in the Gulf of Mexico*, 2010).

For More Information

- Sector-Specific Agency: Department of Energy, http://energy.gov/
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS, www.dhs.gov/energy-sector
- U.S. Department of Pipeline and Hazardous Materials Safety Administration (PHMSA), www.phmsa.dot.gov

Figure 3: Common, First-order Interdependencies of the Energy Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Emergency Services Sector Sector Risk Snapshot

Function/Discipline	Roles and Responsibilities
Law Enforcement	Maintaining law and order and protecting the public from harm. Law enforcement activities may include investigation, prevention, response, court security, and detention, as well as other associated capabilities and duties.
Fire and Emergency Services	Prevention and minimizing loss of life and property during incidents resulting from fire, medical emergencies, and other all-hazards events.
Emergency Medical Services	Providing emergency medical assessment and treatment at the scene of an incident, during an infectious disease outbreak, or during transport and delivery of injured or ill-individuals to a treatment facility as part of an organized EMS system.
Emergency Management	Leading efforts to mitigate, prepare for, respond to, and recover from all types of multijurisdictional incidents.
Public Works	Providing essential emergency functions, such as assessing damage to buildings, roads, and bridges; clearing, removing, and disposing of debris; restoring utility services; and managing emergency traffic.

Emergency Services Infrastructure

- Large, geographically distributed base of facilities, equipment, and highly skilled personnel who provide services in both paid and volunteer capacities.
- Largely organized at the State, local, tribal, and territorial levels of government, corresponding to the scales on which emergencies generally occur. The complex and dispersed nature of the Sector makes it difficult to disable the entire system; it also presents challenges in coordinating emergency responses across disciplines, regions, and levels of government.
- Relies heavily on complex communication and information technology systems to enable robust communications and appropriate coordination and management of diverse elements during emergency situations.
- Uses specialized transportation vehicles and secure transportation routes to facilitate Sector operations because personnel, equipment, aid, and victims must be moved to and from scenes of emergencies.
- The Sector focuses primarily on the protection of other sectors and people, rather than protecting the Sector itself, which presents unique challenges in addressing the protection of Emergency Services as a critical infrastructure sector.
- ESS involves primarily the public sector, but also includes private sector holdings, such as industrial fire departments, sworn private security officers, and private EMS providers.

Emergency Services Sector Overview

- **The Emergency Services Sector (ESS) comprises five disciplines: Law Enforcement, Fire and Rescue Services, Emergency Medical Services (EMS), Emergency Management, and Public Works.**
- **In addition, there are specialized capabilities: Explosive Ordnance Disposal, Hazardous Materials Response, Special Weapons and Tactics and Tactical Operations, Search and Rescue, Aviation Units, and Public Safety Answering Points.**
- **Through partnerships with public and private sector entities, this Sector's mission is to save lives, protect property and the environment, assist communities impacted by disasters (natural or manmade), and aid recovery from emergency situations.**
- **ESS assets, systems, networks, and functions are critical to maintain, protect, and preserve the Nation's safety and health in case of naturally occurring or manmade threats and hazards. By protecting these elements, the Sector is better able to support all critical infrastructure, essential governmental missions, and public services.**
- **The Sector has dependencies and interdependencies with multiple critical infrastructure sectors and the National Response Framework's Emergency Support Functions that support both ESS operations and protection of ESS assets.**

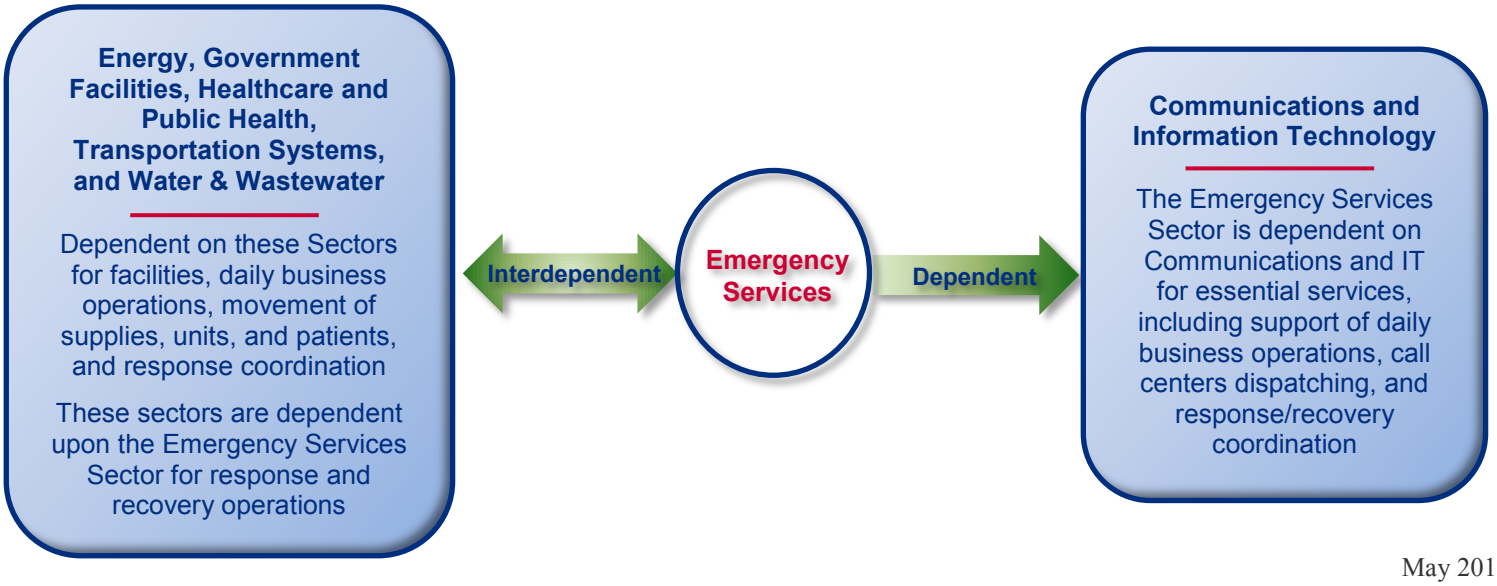
Threats and Hazards of Significant Concern

- **Communications Vulnerabilities**
  - Communication channels and equipment standards have improved dramatically in the last several years. However, many jurisdictions still struggle to use standardized emergency call codes and police radio codes, have difficulty obtaining bandwidth to transmit communications, lack interoperable communications equipment, and do not share frequencies among the various member organizations of the Sector (e.g., police and fire). All of these contribute to ongoing risk for the Sector.
- **Cyberthreats**
  - The dependence of the ESS on information technology also contributes to risk. For example, cyberdisruption of communications systems, computer networks in service vehicles, or GPS during an emergency operation could dramatically disrupt or delay the initial response to an event.
- **Malicious Actors**
  - Contribute significant risk to the Sector. Fire, police, hazardous materials, and other emergency service units respond to criminal threats, violent extremists, suspected terrorist events (e.g., mailed letters and packages containing white powders that could be anthrax), and the aftermath of terrorist attacks (e.g., the bombing of the Oklahoma City Murrah Federal Building, the events of September 11, 2001, and the anthrax events of 2001).
  - As a result, emergency services personnel are exposed to substances of unknown composition, for which their personal protective equipment may not provide adequate protection and from which there may be long-term health implications. Adversaries may also target persons in positions of authority, as well as institutions that are symbolic of a functioning society. ESS representatives may be attacked with improvised explosive devices or targeted by active shooters for these same reasons.

For More Information

- Sector-Specific Agency: DHS, Office of Infrastructure Protection, www.dhs.gov/about-office-infrastructure-protection
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS, www.dhs.gov/emergency-services-sector

Figure 1: Common, First-order Dependencies and Interdependencies of the Emergency Services Sector



May 2014

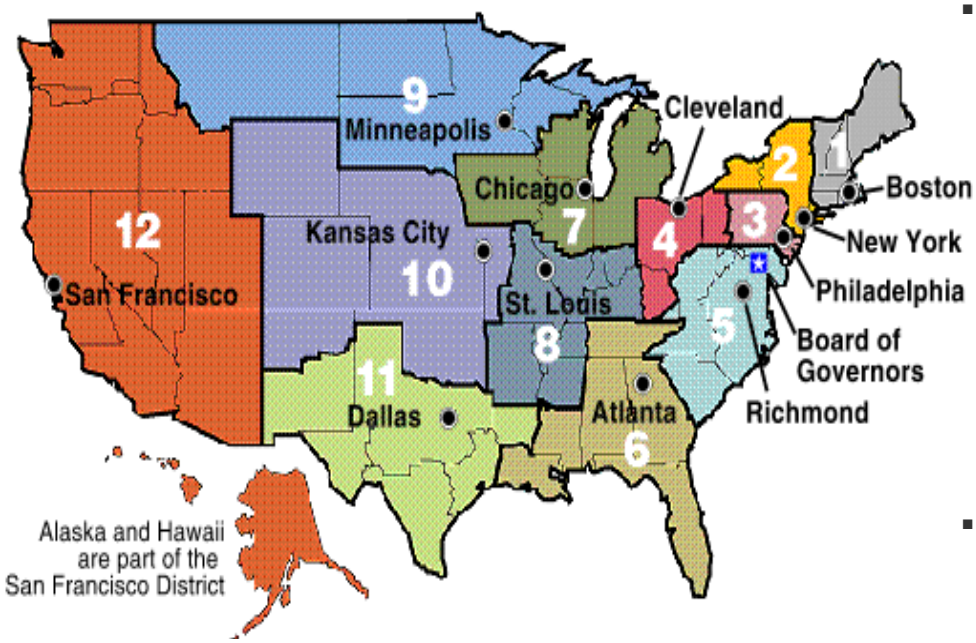
Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

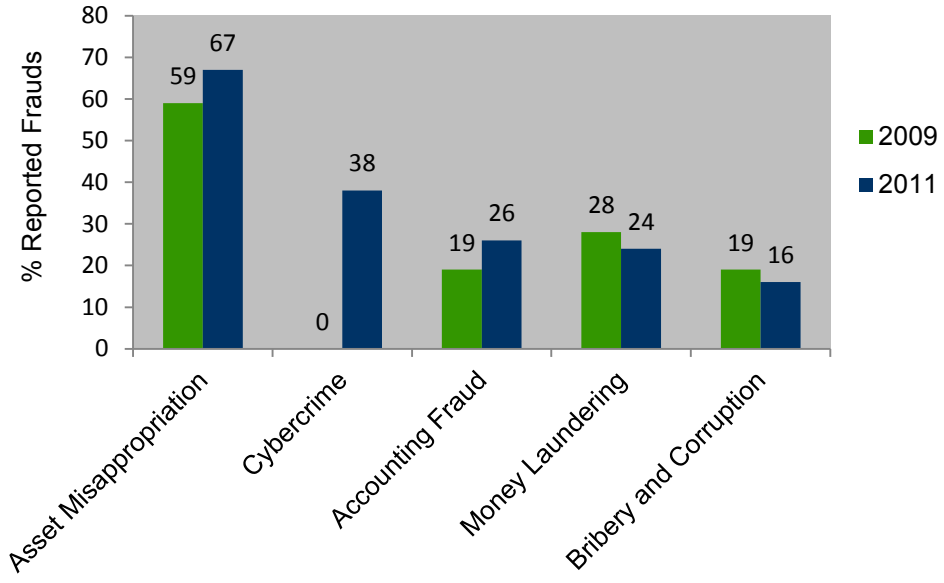
Financial Services Sector Sector Risk Snapshot

Figure 1: U.S. Federal Reserve Bank Locations and Districts



Source: The Federal Reserve Board, www.federalreserve.gov/otherfrb.htm

Figure 2: Top 5 Types of Economic Crimes Experienced by the Financial Services Sector, as Reported in a PwC 2011 Global Survey



Source: PricewaterhouseCoopers, LLP, *Fighting Economic Crime in the Financial Services Sector,* 2012, www.pwc.com/en_GX/gx/economic-crime-survey/pdf/fighting-economic-crime-in-the-financial-services-sector.pdf

Financial Services Sector Overview

- **The Financial Services Sector represents a vital component of the Nation's critical infrastructure. As the Sector-Specific Agency, the Department of the Treasury works with all relevant Federal Departments and agencies; State, local, and tribal governments; and the private sector to promote efforts to improve the Sector's ability to prepare for, respond to, prevent, and mitigate manmade threats, natural disasters, and other intentional or unintentional risks.**
- **Financial institutions provide a broad array of products from the largest institutions to the smallest community banks and credit unions. These products allow customers to do the following:**
  - **— Deposit funds and make payments to other parties;**
  - **— Provide credit and liquidity to customers;**
  - **— Invest funds for both long and short periods; and**
  - **— Transfer financial risks between customers.**
- **Financial institutions are organized and regulated, based on services provided by institutions. Within the sector, there are more than 18,800 federally insured depository institutions; thousands of providers of various investment products, including roughly 18,440 broker-dealer, investment adviser, and investment company complexes; providers of risk transfer products, including 7,948 domestic U.S. insurers; and thousands of other credit and financing organizations.**

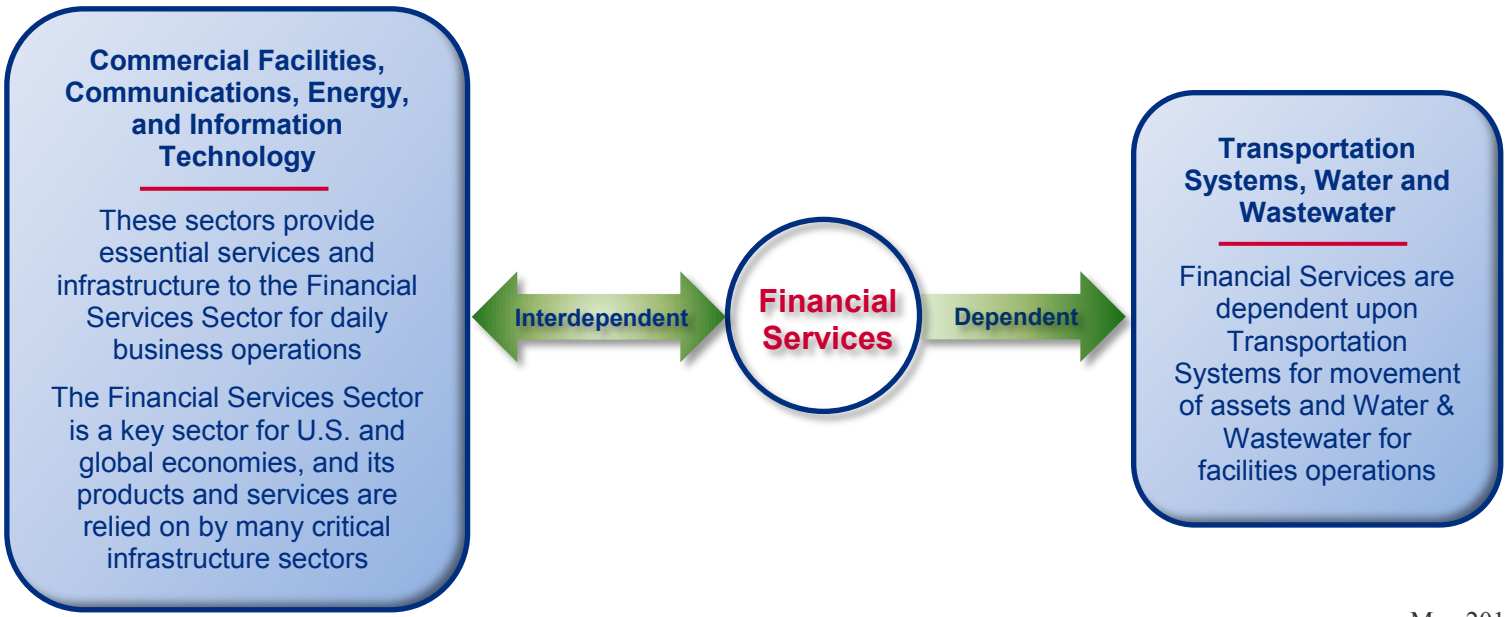
Threats and Hazards of Significant Concern

- **Cyberthreats**
  - Terrorists, transnational criminals, and foreign intelligence services are becoming aware of and using computer viruses, Trojan horses, worms, logic bombs, eavesdropping sniffers, and other tools that can destroy, intercept, degrade the integrity of, or deny access to data.
  - Other potential cyberthreats to the Sector include confidentiality and identity breaches, emerging technology, professionalization of cyber-criminals, and continued globalization of the Sector.
- **Insider Threats**
  - These threats could come from individuals or groups with malicious intent, including but not limited to disgruntled employees and organized crime members, or those with unwitting intent.
  - Insider threats pose a significant concern since these individuals often have knowledge that allows them to gain unrestricted access and inflict damage, steal, and/or move assets without possessing a great deal of knowledge about computer intrusions. Unwitting employees or third parties may also unintentionally damage, destroy, or steal data.
- **Large-scale Physical Events**
  - Natural hazards or terrorist attacks could cause significant economic losses to the Sector and to the Nation.
  - Regulators responsible for safety and soundness of financial services issue guidelines and specific regulations requiring redundancy and security in physical and financial systems. They have long required banking institutions to address operating and security risks in their contingency plans.

For More Information

- Sector-Specific Agency: Department of the Treasury, www.treasury.gov
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS, www.dhs.gov/banking-and-finance-sector
- Financial Services Information Sharing and Analysis Center (FS-ISAC), https://www.fsisac.com/

Figure 3: Common, First-order Dependencies and Interdependencies of the Financial Services Sector



May 2014

Homeland Security
Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Food and Agriculture Sector Sector Risk Snapshot

Food Defense

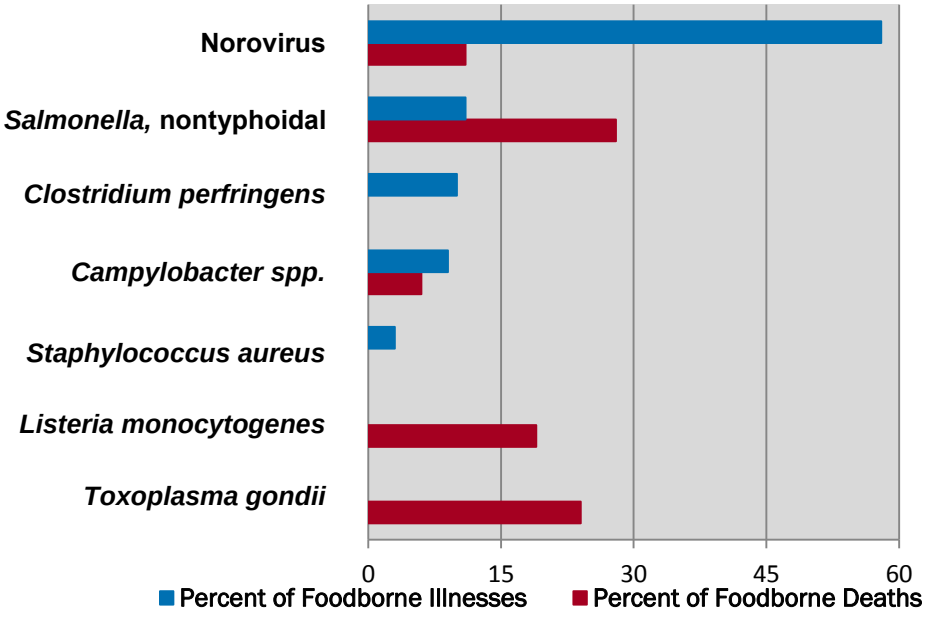
Activities associated with protecting the Nation's food supply from deliberate or intentional acts of contamination or tampering. This term encompasses other similar verbiage (e.g., bioterrorism or chemicalterrorism).

Food Safety

Activities associated with preventing the accidental contamination of food products by biological, chemical, or physical hazards. Focuses on the proper handling and preparation of food and agricultural products.

Figure 1: Top Pathogens Contributing to Domestically Acquired Foodborne Illnesses and Deaths, 2000-2008.

The Centers for Disease Control and Prevention (CDC) estimates that each year 1 in 6 Americans (or 48 million people) get sick, 128,000 are hospitalized, and 3,000 die of foodborne diseases.



Source: CDC, *2011 Estimates of Foodborne Illness in the United States*, www.cdc.gov/foodborneburden/2011-foodborne-estimates.html

Food And Agriculture Sector Overview

- **The Food and Drug Administration (FDA) and U.S. Department of Agriculture (USDA) jointly serve as the Sector Specific Agencies for the Food and Agriculture Sector.**
- **Composed of complex production, processing, and delivery systems and encompasses upwards of 4 million assets, including 2 million+ farms, 900,000+ restaurants, 100,000+ food retail establishments. As of February 19, 2014, there were 81,575 FDA registered domestic food facilities (warehouses, manufacturers, processors) and 115,753 FDA registered foreign food facilities. USDA regulates 6,805 establishments, including establishments for meat, poultry, processed egg products, imported products, and voluntary inspection services.**
- **Accounts for roughly one-fifth of the Nation's economic activity.**
- **The open nature and global interconnectivity of the sector presents unique security challenges, and leaves the sector vulnerable to a variety of all-hazards threats, including severe weather, pests and disease, and contamination with biological, chemical, or radiological agents.**
- **Direct attacks on the sector, such as the introduction of animal or plant disease, or deliberate food contamination, could result in devastating animal, plant, or public health and economic consequences.**

Food and Agriculture Infrastructure

- Food and Agriculture Sector infrastructure is unique, complex, broad-based, globally distributed, and highly integrated, and is seen as a system of systems (i.e., systems of individual assets that are closely dependent on each other).
- Many of the sector's systems defy traditional security practices because they are not brick-and-mortar entities, like buildings, bridges, or dams. Instead, they are open areas (i.e., farms, ranches, or livestock transport areas) and complex systems that span the globe.
- Many of these systems face natural threats, including livestock and crop diseases and foodborne pathogens, thus monitoring, early threat detection, and rapid response are key mitigation activities for the sector.
- Food and agriculture owners and operators must anticipate the possibility of a terrorist attack on their products and evaluate their preparedness and mitigation strategies to either thwart an attack or, at the very least, mitigate the damage, and recover from the animal, plant, public health, economic, and psychological impacts of an attack.

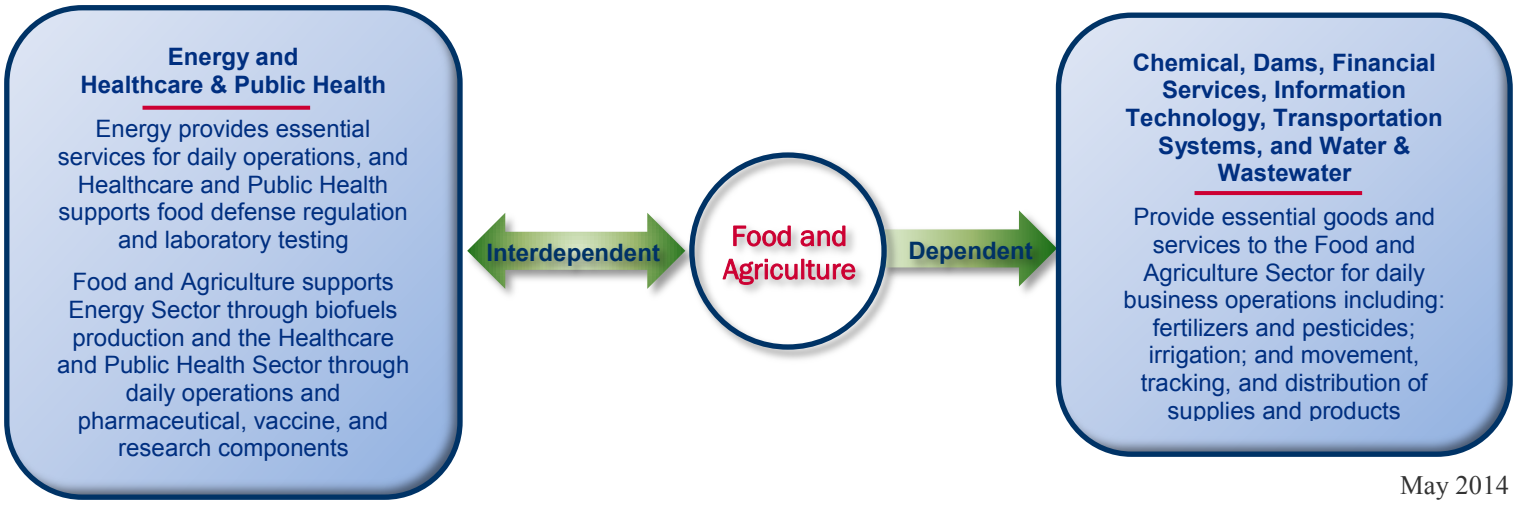
Threats and Hazards of Significant Concern

- **Food Contamination (whether by accidental or intentional means)**
  - Contaminated food in the United States is estimated to be responsible for over 47.8 million illnesses, 127,839 hospitalizations, and 3,037 deaths, costing the Nation more than $14 billion a year in terms of medical care, lost productivity, chronic health problems, and deaths (CDC, 2011).
  - Violent extremists and terrorists have indicated an interest in poisoning the food supply with biological and chemical agents, which has great potential to cause costly economic losses in the supply chain for implicated foodstuffs, creating public panic, and leading to a public health crisis with considerable mortality and morbidity (FBI, www.fbi.gov/stats-services/publications/law-enforcement-bulletin/february-2012/agroterrorism, 2012).
- **Disease and Pests**
  - The accessibility of crops and animals on the farm and the extensive international and interstate movement of animals and products increase the sector's vulnerability to rapidly spread disease.
  - Modeling estimates and historical evidence demonstrate that a domestic outbreak of a foreign animal disease, such as Foot and Mouth Disease, could cost the United States billions of dollars due to loss of livestock, production, and international trade.
- **Severe Weather (including droughts, floods, and climate variability)**
  - Natural hazards are an important risk to the Food & Agriculture Sector, and critically influence farm productivity.
  - Weather and climate characteristics such as temperature, precipitation, and water availability directly impact the health and well-being of plants and livestock, as well as pasture and rangeland production.
  - The harmful effects of severe weather coupled with global climate change are currently affecting U.S. water resources, agriculture, land resources, and biodiversity. This trend is expected to continue (USDA, 2013, www.usda.gov/oce/climate_change/effects.htm).

For More Information

- Sector-Specific Agencies: U.S. Department of Agriculture (USDA), Office of Homeland Security and Emergency Coordination, National Security Policy Staff, www.dm.usda.gov/ohsec/rpd/index.htm; and Department of Health and Human Services Food and Drug Administration (FDA), *Food Defense and Emergency Response*, www.fda.gov/Food/FoodDefense/default.htm
- DHS,www.dhs.gov/food-and-agriculture-sector
- DHS, *IP Note: Reducing the Vulnerability of the U.S. Food Supply to Intentional Contamination*, 10 August 2010
- DHS, USDA, FDA, *2010 Food and Agriculture Sector Specific Plan*, ww.dhs.gov/files/programs/gc_1179866197607.shtm
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov

Figure 2: Common, First-order Dependencies and Interdependencies of the Food & Agriculture Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Government Facilities Sector
Sector Risk Snapshot

Homeland Security

Government Facilities Security Levels

Because of the differences among Federal buildings and their security needs, U.S. Federal Marshals Services categorized Federal facilities into five classes based on building size, agency mission and function, tenant population, and the degree of public access to the facility, and developed security standards corresponding to the security level needed for each class.

Level I—buildings with no more than 2,500 square feet, 10 or fewer Federal employees, and limited or no public access

Level II—buildings with 2,500 to 80,000 square feet, 11 to 150 Federal employees, and moderate public access

Level III—buildings with 80,000 to 150,000 square feet or more, 151 to 450 Federal employees, and a moderate-to-high public access

Level IV—buildings with 150,000 square feet or more, more than 450 Federal employees, and a high level of public access

Level V—buildings that are similar to Level IV but are considered critical to national security

Critical Infrastructure Security and Resilience Issues

- Government facilities represent attractive and strategically important targets for both domestic and international terrorist groups, as well as criminals.
- These assets are often targeted because they provide unique services, often perform sensitive functions, and have significant symbolic value.
- Because of the high-profile nature of the sector, government facilities operate within a very dynamic risk environment requiring a variety of well-coordinated protective measures to ensure the safety and security of citizens and the continued availability of essential government functions.

Government Facilities Sector Overview

- **Comprises a wide variety of buildings, national monuments, and icons in the United States and overseas that are owned or leased by Federal, State, local, and tribal governments.**
- **The sheer size and scope of the Government Facilities Sector poses a challenge in providing for infrastructure protection efforts.**
- **The Federal Government alone manages approximately 3.35 billion square feet of space and more than 650 million acres of land across the United States. The Sector also includes the facilities owned and operated by the more than 87,000 municipal governments across the Nation and abroad.**
- **These facilities include general-use office buildings and special-use military installations, embassies, courthouses, and national laboratories that contain highly sensitive information, materials, processes, and equipment.**
- **Many government facilities are open to the public for business activities, commercial transactions, or recreational activities, while others are not.**
- **The Government Facilities Sector includes the Education Facilities Subsector, which covers pre-kindergarten through 12th grade schools, institutions of higher education, and business and trade schools.**
- **The National Monuments and Icons Subsector was consolidated within the Government Facilities Sector in 2013 under Presidential Policy Directive 21. The Subsector encompasses a diverse array of assets, networks, systems, and functions located throughout the United States. Many are listed in either the National Register of Historic Places of the List of National Historic Landmarks.**

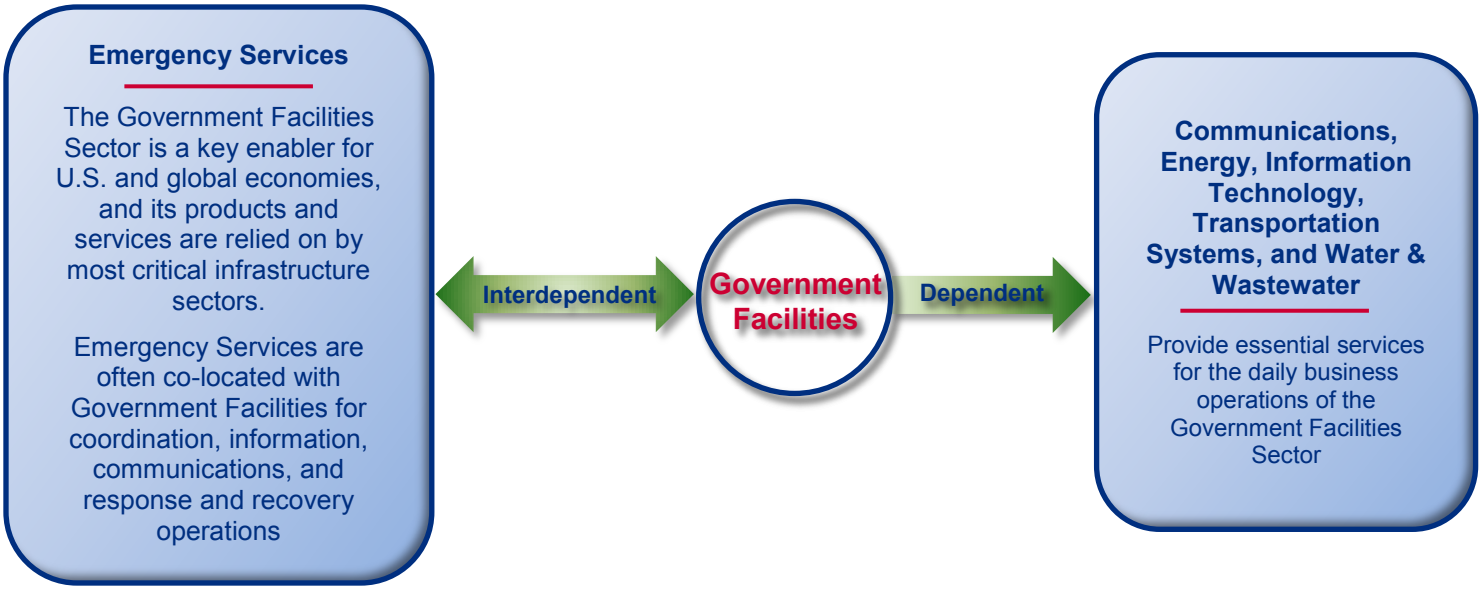
Threats and Hazards of Significant Concern

- **Terrorist Attacks**
  - The threat of terrorist attacks contributes significantly to the risks of the Government Facilities Sector. A major challenge in the protection of government facilities is balancing the need for security with the need for public access to government offices for services and transactions.
  - Global events and trends suggest that terrorists will likely continue to use improvised explosive device tactics—historically one of the most successful tactics—to attack U.S. critical infrastructure. Government facilities may also be targeted by active shooters, as occurred in the 2010 shooting at a Federal courthouse in Las Vegas. (Doherty, R., *Critical Research/Innovation Focus Area Document: Vehicle-Borne Improvised Explosive Devices (VBIED)* Detection, Washington, D.C.: U.S. Department of Homeland Security, Science and Technology Directorate, 2009)
- **Cyberthreats**
  - Cyberintrusions into automated security and supervisory control and data acquisition systems are risks. The increasing reliance on automated security systems and automated building management systems will likely increase vulnerabilities and the likelihood of cyberintrusion, especially in the form of sabotage by current or former insiders with malicious intent.
  - Cyberintrusion into the security systems of government facilities could compromise the protection of facilities, civil servants, and the general public and allow for exploitation and attacks with significant consequences.

For More Information

- Sector-Specific Agency: Department of Homeland Security Federal Protective Service www.dhs.gov/topic/federal-building-security, and the General Services Administration www.gsa.gov
- Government Facilities Sector, www.dhs.gov/government-facilities-sector
- National Infrastructure Protection Plan, www.dhs.gov/nipp
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov
- Contact NIPP@hq.dhs.gov or NIPP-GFS@hq.dhs.gov

Figure 1: Common, First-order Dependencies and Interdependencies of the Government Facilities Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

The Principles of School Emergency Management Planning

Must be supported by leadership. At the district and school levels, senior-level officials can help the planning process by demonstrating strong support for the planning team.
Uses assessments to customize plans to the building level. Effective planning is built around comprehensive, ongoing assessment of the school community, which customizes plans to the building level, taking into consideration the school's unique circumstances and resources.
Considers all threats and hazards. The planning process must take into account a wide range of possible threats and hazards that may impact the school, addressing safety needs before, during, and after an incident.
Provides for the access and functional needs of the whole school community. The "whole school community" includes children, individuals with disabilities and others with access and functional needs, those from religiously, racially, and ethnically diverse backgrounds, and people with limited English proficiency.
Considers all settings and all times. School EOPs must account for incidents that may occur during and outside the school day as well as on and off campus (e.g., sporting events, field trips).
Creating and revising a model Emergency Operations Plan is done by following a collaborative process.

Source: U.S. Department of Education, Readiness and Emergency Managements for Schools Technical Assistance Center, http://rems.ed.gov/Default.aspx (2014).

Number of U.S. Educational Institutions by Number and Control of Institution

Public Schools (2012)	**98,328**
Elementary	66,689
Secondary	24,357
Combined	6,311
Other[1]	971
Private Schools (2011)	**30,860**
Postsecondary Title IV Institutions (2013)	**7,253**
Degree-granting institutions	4,726
2-year colleges	1,700
4-year colleges	3,026

[1]Includes special education, alternative, and other schools not classified by grade span

Source: U.S. Department of Education, National Center for Education Statistics, *2013 Digest of Education Statistics* (2014, Advance Release).

Education Facilities Subsector Overview

- **The Education Facilities Subsector (EFS) encompasses pre-kindergarten (pre-K) through 12th grade and post-secondary public, private, and proprietary education facilities.**
- **The Department of Education serves at the Sector-Specific Agency for the Education Facilities Subsector.**
- **EFS assets and systems vary dramatically and include rural and urban, public and private education facilities ranging from fewer than a hundred students to many thousands of students. EFS assets also include pre-K through 12 and higher education campus grounds, increasing the number of facilities, the level of complexity, and the challenges to risk mitigation.**
- **The overall EFS vision is that all education facilities are ready to prevent, mitigate, prepare for, respond to, and recover from any natural or manmade hazard, by having a comprehensive, all-hazards plan to enhance safety, minimize disruption, and ensure continuity of the learning environment.**
- **For the EFS, comprehensive, all-hazards emergency management plans are the appropriate approach to mitigating risk and enhancing resilience for all of EFS' human, physical, and cyber assets.**
- **Comprehensive plans are based on the four phases of school emergency management (prevention and mitigation, preparedness, response, and recovery). Such plans are practiced and updated regularly, coordinated with appropriate State and local partners, and developed in close collaboration with first responders and the community.**
- **They include written plans for an infectious disease outbreak, support the National Incident Management System, contain measures to address food defense, and incorporate students and staff with special needs.**

Threats and Hazards of Significant Concern

- **Natural Hazards** (e.g., hurricanes, wildfires)
  - Weather events pose a risk to the safety of the personnel and students at these institutions. Significant damage can cause the institution to close in the short and long term.
- **Public Health Hazards** (e.g., Methicillin-Resistant Staphylococcus Aureus (MRSA), salmonella outbreaks , H1N1, and intentional adulteration of food)
  - Public health hazards pose a risk to the safety of the personnel and students at these institutions. Significant damage can cause the institution to close in the short and long term.
- **Active Shooter** (e.g., Columbine, Virginia Tech, and Sandy Hook Elementary School)
  - Shootings pose a threat to the safety of the personnel and students at these institutions. Schools are targets because shootings bring national attention to the individual or group. Public confidence and the continuity of school operations could be negatively affected.
- **Cyberthreats** (e.g., computer system hacking, phishing)
  - Higher education institutions often collect and store sensitive, personal student data and databases (Social Security numbers, health, financial, and educational data). Education facilities with emergency management data housed electronically require cybersecurity efforts to maintain the integrity of their plans (i.e., emergency management plans, floor plans).
  - Disruptions to institutional data systems could impact the capacity to effectively perform essential business operations and could cause a temporary to long-term school closure.
  - Although a cyberattack on an education facility would not likely impose cascading effects for the Nation, it can have such effects on the campus community through the compromise of personal data, security systems, and research facilities that rely on cyber elements or of emergency management data housed electronically.

For More Information

- Sector-Specific Agency: The Department of Education, www.ed.gov
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov
- DHS, 2010 Education Facilities Sector-Specific Plan, www.dhs.gov/xlibrary/assets/nipp-ssp-education-facilities-2010.pdf
- Readiness and Emergency Management for Schools, http://rems.ed.gov/

Figure 1: Common, First-order Dependencies of the Education Facilities Subsector

May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Healthcare and Public Health Sector Sector Risk Snapshot

Healthcare and Public Health Sector Overview

- **The Healthcare and Public Health (HPH) Sector is the lead Sector responsible for protecting and sustaining the Nation's health. The U.S. Department of Health and Human Services (HHS) serves as the Sector-Specific Agency for the HPH Sector.**
- **This widespread and diverse Sector includes acute care hospitals, ambulatory healthcare, public-private financial systems, Federal, State, and local public health systems; disease surveillance; and private sector industries that manufacture, distribute, and sell drugs, biologics, and medical devices.**
- **The Sector is vulnerable to a variety of all-hazards threats, and is especially concerned about potentially catastrophic impacts resulting from biological, cyber, vehicle-borne explosive devices, and insider threats.**
- **Such attacks could result in large numbers of illness and casualties, denial of service, or theft of confidential patient information.**
- **For the Sector, critical infrastructure protection is ultimately defined by the extent to which the Sector has been able to mitigate interruptions in the delivery of healthcare and public health services.**

Figure 1: Occurrence of Major Flu Pandemic or New Influenza Strain over the Past 100 years

Table 1: Major Flu Pandemics in the Past 100 Years, with Comparison to Seasonal Flu

	Virus Strain	First Identified	Ground Zero	Higher Risk/Age Group	Estimated Infection Rate	Mortality Rate	Estimated Deaths
Seasonal Flu	Seasonal variation	Seasonal variation	N/A	Very young, very old, and the infirm	5-15%	0.6%	0.25-0.5 million
Spanish Flu	H1N1	Spring 1918	Western Europe	Age 20-50	20-40%	2-2.5%	40-50 million
Asian Flu	H2N2	February 1957	China	School-aged children, elderly	30%	0.025%	2-4 million
Hong Kong Flu	H3N2	Early 1968	Hong Kong	Elderly	30%	0.02%	1-3 Million
Influenza A (H1N1)	H1N1	April 2009	Mexico	Children, teens, young adults	24%[1]	0.02%[1]	>18,500[1]

[1] World Health Organization (WHO), "Estimating age-specific cumulative incidence for the 2009 influenza pandemic: a meta-analysis of A(H1N1)pdm09 serological studies from 19 countries," *Influenza and Other Respiratory Viruses*, Vol:7, January 2013

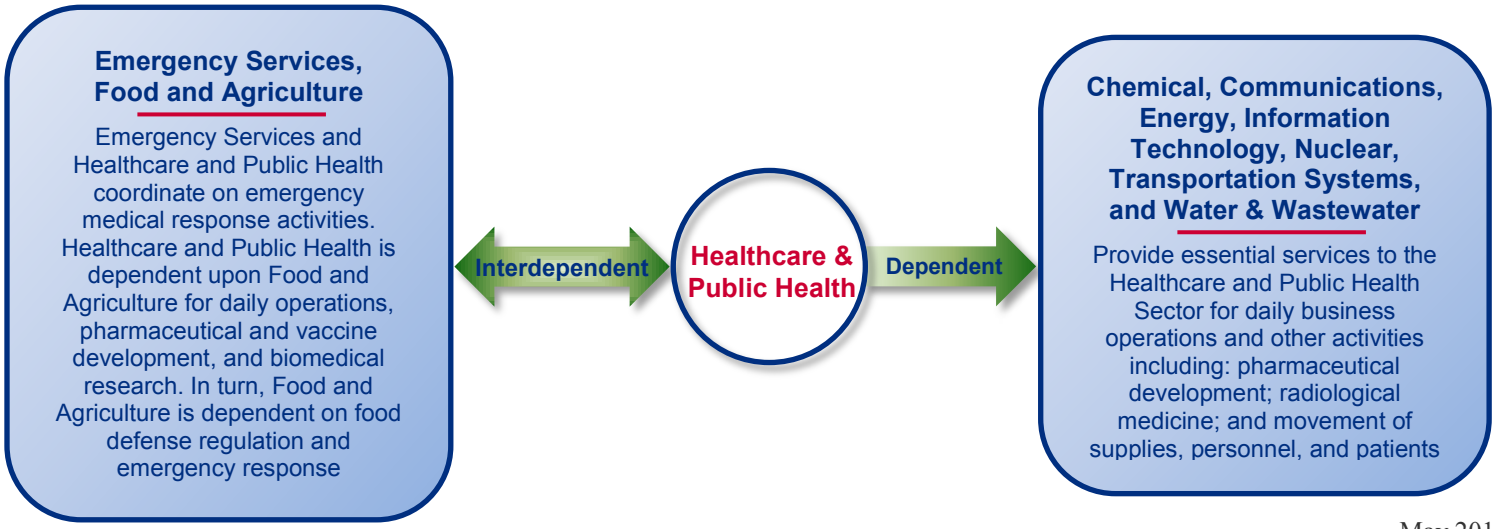
Threats and Hazards of Significant Concern

- **Global Supply Chain Disruptions**
  - A supply chain disruption refers to an event leading to a shortage of a pharmaceutical, device, or biologic. A natural disaster may make roads impassable and thereby prevent goods from arriving at an effected area, or a product may be contaminated at its place of origin and need to be recalled resulting in a limited amount of that product on the market.
  - Independent of the reason, supply chain disruptions can be catastrophic, as healthcare providers tend to rely on just-in-time resupplying and therefore do not always have sufficient stockpiles to weather a delay, especially during events that lead to an increased demand for healthcare or healthcare-related products.
- **Theft and Exploitation of Medical Goods and Confidential Medical Information**
  - Theft and exploitation result from the work of malicious actors.
  - Many medical facilities and laboratories contain radiological materials or biological select agents and toxins that are used for clinical treatment or medical research; and the open nature of these facilities presents a potential security vulnerability. These agents and materials may provide an attractive target to those wishing to construct a "dirty bomb," intentionally infect a population, or sell the material on the black market.
  - Medical systems and vital records are also at risk for compromise or theft by external hackers or malicious insiders, and cybertheft presents a trend in medical identity theft.
- **Pandemic**
  - Recent experience with influenza demonstrated how a rapidly-spreading infectious agent can significantly impact the HPH Sector and the country as a whole. A naturally occurring agent like influenza was able to cause death, hospitalizations, and absenteeism.
  - If a more dangerous agent, such as smallpox, were intentionally released, the effects could be even more catastrophic due to the increased lethality and our general immunological naiveté to the disease.

For More Information

- Sector-Specific Agency: Department of Health and Human Services (HHS), Public Health Preparedness and Emergency, www.phe.gov
- DHS, HHS, *2010 Healthcare and Public Health Sector-Specific Plan*, www.dhs.gov/files/programs/gc_1179866197607.shtm
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov

Figure 2: Common, First-order Dependencies and Interdependencies of the Healthcare and Public Health Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Information Technology Sector
Sector Risk Snapshot

Critical IT Sector Functions

- IT products and services
- Incident management capabilities
- Domain name resolution services
- Identity management and associated trust support services
- Internet-based content, information, and communications services
- Interrouting, access, and connection services

Information Technology Sector Overview

- Businesses, governments, academia, and private citizens are increasingly dependent upon IT Sector functions. The Information Technology (IT) Sector is central to the Nation's security, economy, public health, and safety.
- These virtual and distributed functions produce and provide hardware, software, IT systems and services, and—in collaboration with the Communications Sector—the Internet.
- The Sector's complex and dynamic environment makes identifying threats and assessing vulnerabilities difficult, and requires that these tasks be addressed in a collaborative and creative fashion.
- The IT Sector functions are operated by a collaboration of entities—often owners and operators and their respective associations—that maintain and reconstitute the network, including the Internet.
- Although the IT infrastructure has a certain level of inherent resilience, its interdependent and interconnected structure presents challenges as well as opportunities for coordinating public and private sector preparedness and protection activities.
- The IT Sector is at constant risk from cyberthreats, and identifying threat actors, intrusion methods, and network vulnerabilities are critical to mitigation and longer-term defensive strategies (Figure 1 and 2).

Figure 1: 2012 Confirmed Data Breach and Network Intrusion Threat Actors

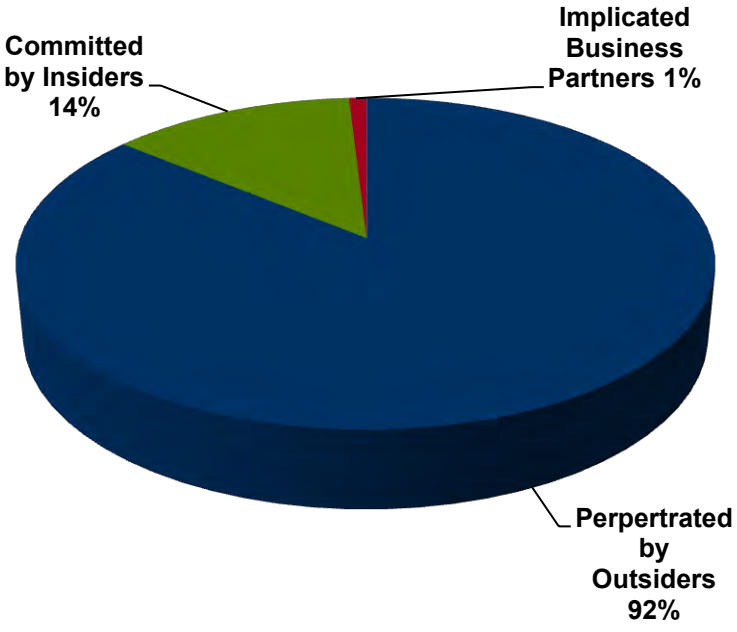
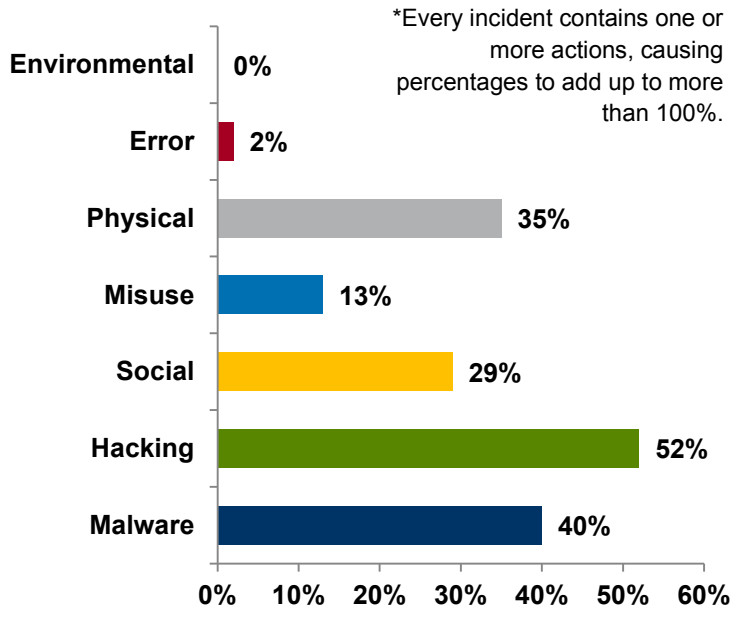


Figure 2: 2012 Confirmed Data Breach and Network Intrusion Threat Actions



Source: Verizon, *2013 Data Breach Investigations Report*, www.verizonenterprise.com/DBIR/2013/

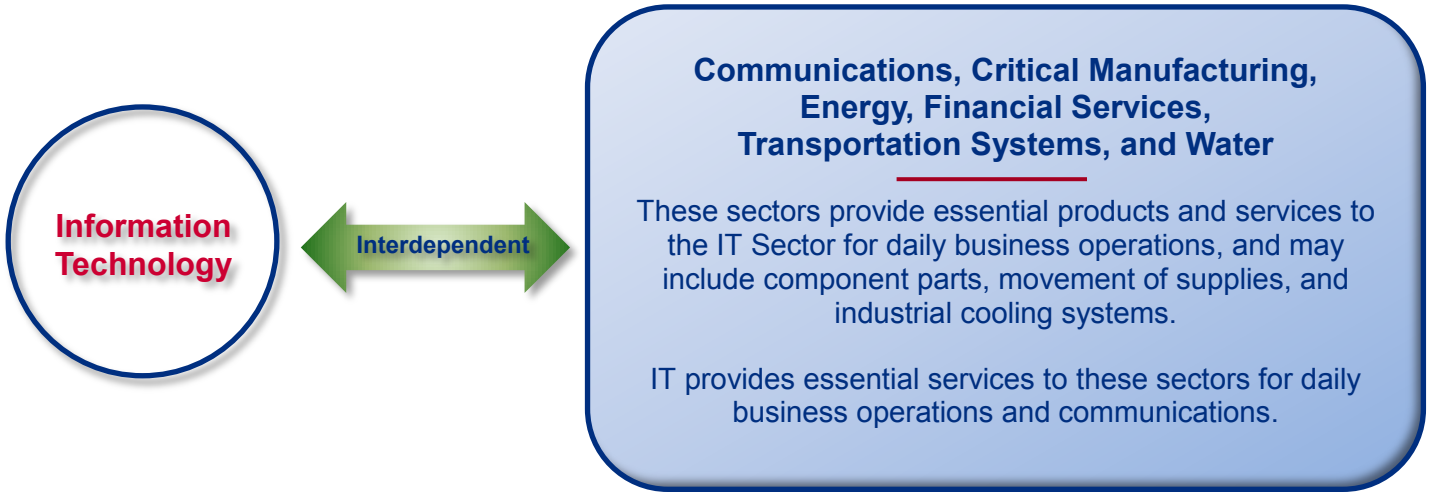
Threats and Hazards of Significant Concern

- **Cyberthreats**
  - The IT Sector is highly concerned about cyberthreats, particularly those that degrade the confidentiality, integrity, or availability of the Sector's critical functions.
  - Depending on its scale, a cyberattack could be debilitating to the IT Sector's highly interdependent critical infrastructures and ultimately to the Nation's economy, homeland security, and national security.
  - These cyberthreats include unintentional acts (e.g., the accidental disruption of Internet content services) and intentional acts (e.g., the exploitation of IT supply chain vulnerabilities or the loss of interoperability between systems as the result of an attack).
- **Attacks Targeting Internet-based Identity**
  - These include attacks targeting management, content, information, and communications. For example, malicious code increasingly proliferates through social networking and can degrade information technology system functionality.
  - Failures in identity management systems can lead to serious consequences like identity theft, criminal activity, unauthorized access to sensitive or classified information, systems, and facilities, which could jeopardize public safety and the operation of financial, government, or law enforcement systems.

For More Information

- Sector-Specific Agency: DHS, Office of Cybersecurity and Communications, www.dhs.gov/office-cybersecurity-and-communications
- DHS IT Sector, www.dhs.gov/information-technology-sector
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov
- U.S. Cyber Emergency Readiness Team, www.us-cert.gov
- U.S. Industrial Control Systems Cyber Emergency response Team (ICS-CERT), ics-cert.us-cert.gov
- National Vulnerability Database, http://nvd.nist.gov
- FBI Cyber Crime Investigations, www.fbi.gov/about-us/investigate/cyber

Figure 3: Common, First-order Interdependencies of the IT Sector



May 2014

Homeland Security

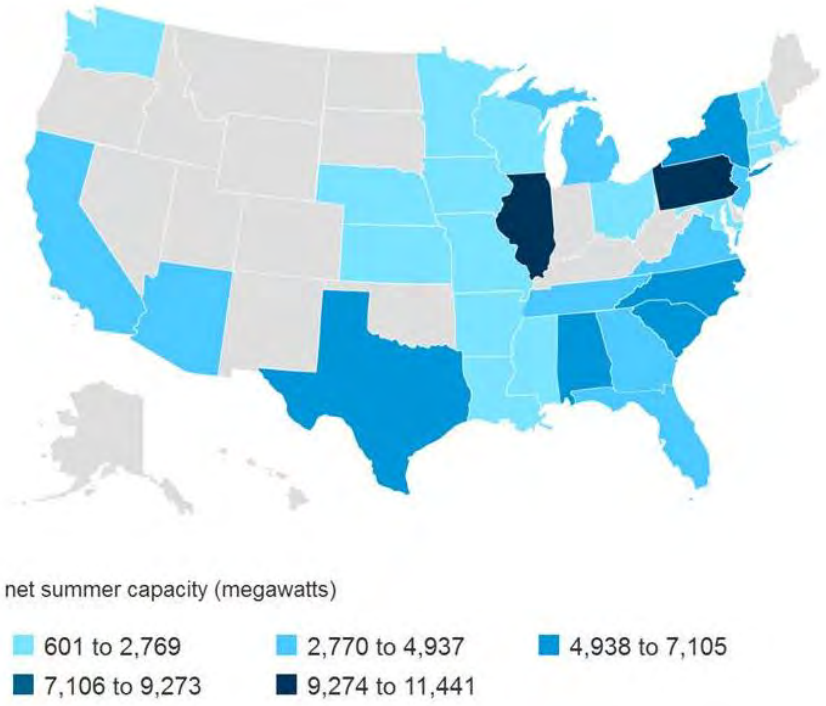
Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Nuclear Reactors, Materials, & Waste Sector

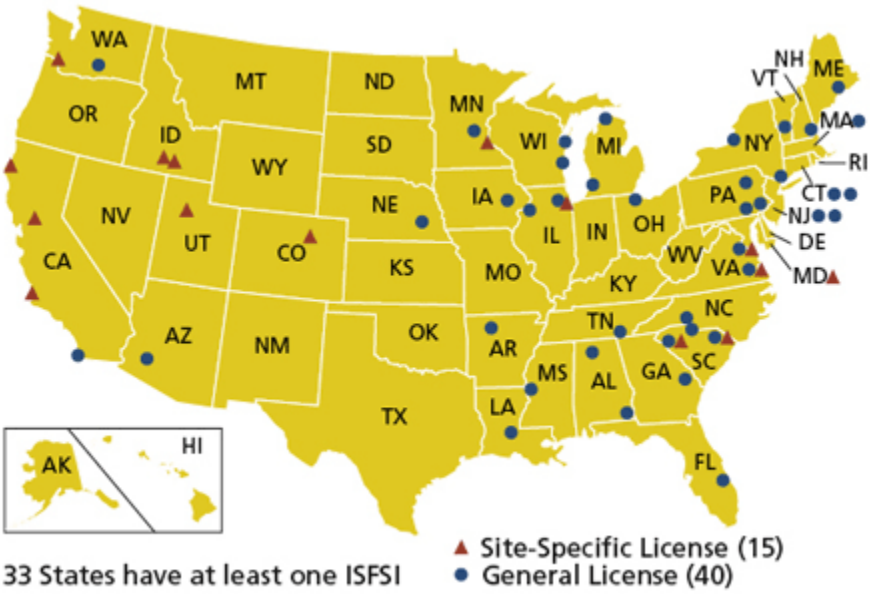
Sector Risk Snapshot

Figure 1: U.S. Nuclear Capacity and Generation



Source: U.S. Energy Information Administration (EIA), *Nuclear and Uranium*, 2014, www.eia.gov/nuclear/state.

Figure 2: Licensed/Operating Independent Spent Fuel Storage Installations



Source: U.S. Nuclear Regulatory Commission, *Locations of Independent Spent Fuel Storage Installations,* 2012, www.nrc.gov/waste/spent-fuel-storage/locations.html.

Nuclear Sector Overview

- Comprises nuclear power plants; research and test reactors; fuel cycle facilities; radioactive waste management; decommissioning reactors; nuclear and radioactive materials used in medical, industrial, and academic settings; and nuclear material transport.
- 104 nuclear power reactors at 65 nuclear power plants account for nearly 20 percent of annual U.S. electricity production (Figure 1). Increases in nuclear generation have roughly tracked the growth in total electricity output.
- There are 31 research and test reactors nationwide. Also known as non-power reactors, they are used primarily for education and research and development.
- Radioactive materials, including more than 75,000 high-activity sources, are used daily in a range of industrial, medical, and other commercial settings.
- The Sector faces current and ongoing risk for Sector facilities and materials due to physical incidents, cyber-disruptions, theft, diversion of materials, and disruptions in the supply chain.
- Theft or diversion of nuclear materials would pose a significant risk to populations through mishandling of the material or the use of a radiological dispersal device (RDD) or, in the worst case, the detonation of an improvised nuclear device.
- If successfully attacked or disrupted, some nuclear facilities have the potential to release radioactive material into the environment.

Radioactive Waste

- Most spent nuclear fuel is safely stored in specially designed pools at individual reactor sites around the country (Figure 2).
- Licensees may move spent fuel rods to above-ground dry storage casks after a minimum 5-year decay period, and if the licensee has an approved above-ground dry storage facility.

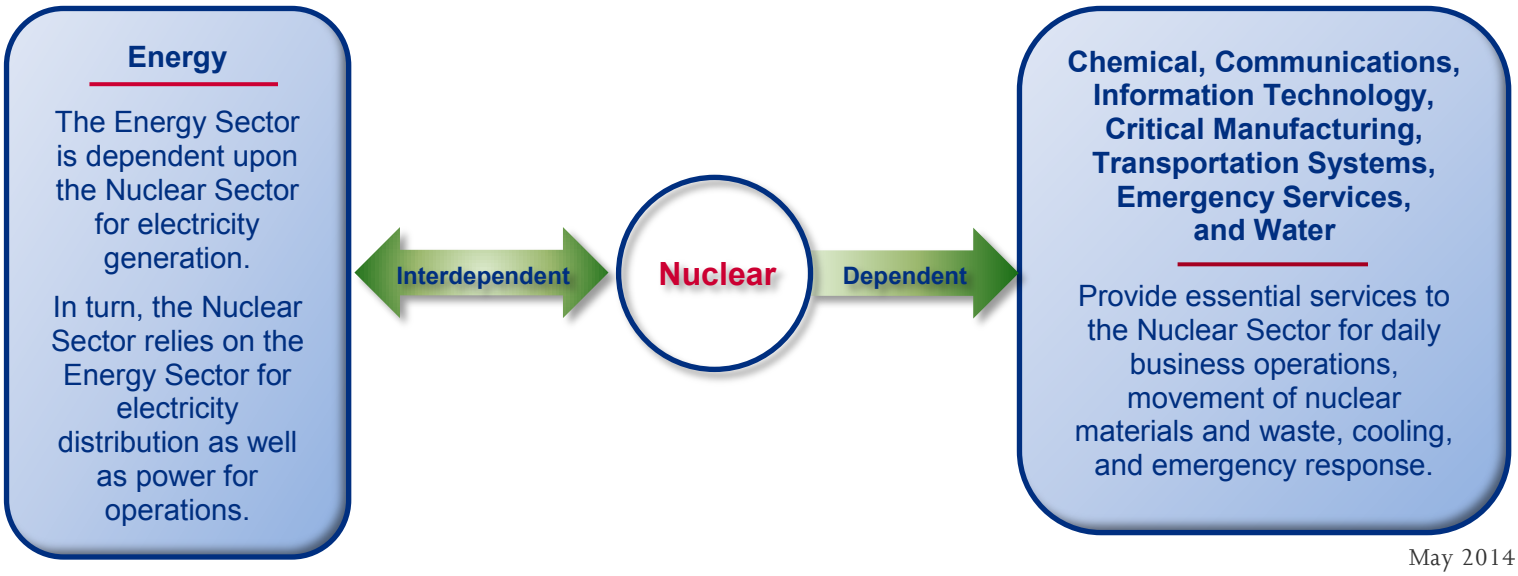
Threats and Hazards of Significant Concern

- **Theft and diversion of nuclear and radioactive materials:**
  - Determined and skilled adversaries could use stolen radioactive materials as elements of improvised nuclear devices (IND), radiological dispersion devices (RDD), or radiological exposure devices.
- **Natural hazards (e.g. hurricanes, tornados, floods, earthquakes, and drought):**
  - Pose a serious and continuing risk for the Sector.
  - The loss or disruption of a single nuclear power plant would have limited impact on the Nation's overall electrical capacity.
  - Sector infrastructure may be severely disrupted or destroyed by such hazards, which may further complicate an overall disaster emergency response due to multiple cross-sector interdependencies (Figure 3).
- **Physical and cyberattacks on Nuclear Sector infrastructure and assets by terrorists, homegrown extremists, or disgruntled insiders:**
  - Physical attacks using improvised explosive devices on nuclear power reactors, spent fuel and radioactive waste storage facilities, and fuel cycle facilities could result in a release of hazardous materials.
  - Cyberattacks and intrusions on industrial control systems may pose a significant threat to the Sector, allowing malicious actors to manipulate or exploit facility operations.

For More Information

- Sector-Specific Agency: DHS, Office of Infrastructure Protection, www.dhs.gov/about-office-infrastructure-protection
- Nuclear Regulatory Commission, www.NRC.gov
- Nuclear Energy Institute, www.NEI.org
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS, 2010 Nuclear Reactors, Materials, and Waste Sector-Specific Plan, www.dhs.gov/files/programs/gc_1179866197607.shtm

Figure 3: Common, First-order Dependencies and Interdependencies of the Nuclear Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Aviation Mode
Transportation Sector

Sector Risk Snapshot

Figure 1: Major Continental U.S. Airport Locations

Table 1: Schedules System (Domestic and International) Airline Travel on U.S. Airlines

	2012	2013	Change %
Passengers (in millions)	736.7	743.1	0.9
Flights (in thousands)	9,287.40	7,158.70	-1.4
Revenue Passenger Miles (in billions)	823.2	840.4	2.1
Available Seat-miles (in billions)	994.5	1.011.20	1.7
Load Factor*	82.8	83.1	0.3
Flight Stage Length**	755	770.3	2
Passenger Trip Length***	1,117.40	1,131.00	1.2

Source: Bureau of Transportation Statistics, *T-100 Market and Segment*, March 13, 2014, www.rita.dot.gov/bts/press_releases/bts012_14
* Measure of the amount of utilization of the total available capacity of an airline, i.e. percent of available seat-miles (ASM) occupied by passengers
** The average non-stop distance flown per departure in miles
*** The average distance flown per passenger in miles
Note: Percentage changes based on numbers prior to rounding.

Aviation Mode Overview

- **The Aviation Transportation System (ATS) is a vital mode within the Transportation Sector, integrally contributing to the free flow of people and commerce across the globe.**
- **The Aviation Mode consists of more than 19,700 airports in the United States. Of these, 5,170 are open to the general public with 503 offering commercial service.**
- **The ATS includes more than 690 air traffic control facilities, and over 11,000 air navigation facilities.**
- **More than 780,000 passenger flights take place over the United States each month carrying nearly 60 million passengers.**
- **This Mode transports more than 13 million ton-miles of freight domestically each year.**
- **The security and economic prosperity of the United States depend significantly upon the secure operation of its ATS and safe use of the world's airspace.**
- **Significant threats to the ATS include the potential for terrorist infiltrations and attacks, cyber attacks against ATS assets, and the hostile exploitation of air cargo.**
- **The U.S. Department of Homeland Security (DHS), Department of Transportation (DOT), and Department of Defense (DOD) continue to develop and enhance technological and procedural measures to detect, prevent, respond to, mitigate and recover from physical and cyber-based attacks on the ATS's critical infrastructure.**

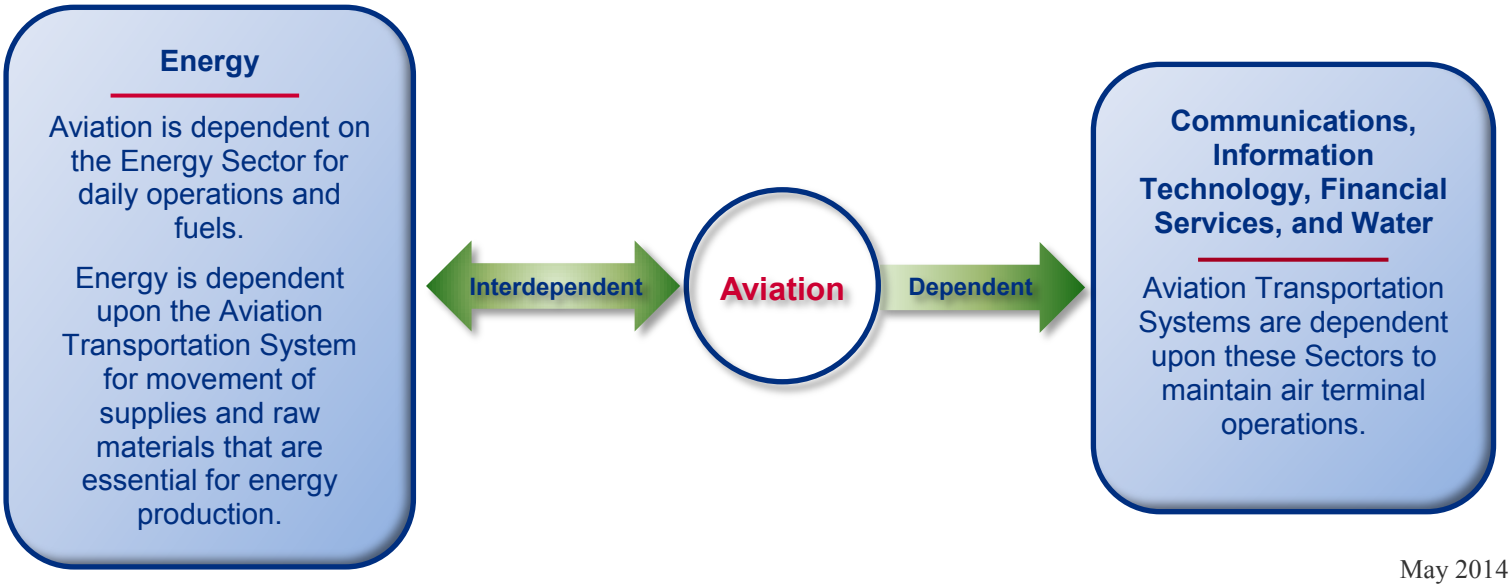
Threats and Hazards of Significant Concern

- **Terrorism**
  - Terrorism threats to the ATS persist. Aircraft have been the primary target of attacks in the past, and have been used as weapons. Despite security enhancements made after the attacks on September 11, 2001, intelligence continues to indicate that aviation remains a top target of terrorists. (DHS and TSA, 2011)
  - Terrorist groups are adapting to aviation countermeasures in multiple ways, including modality of planning, complexity of potential attacks, and methods of attack execution.
- **Cyberthreats**
  - The Sector focuses on developing countermeasures to address specific risks in the cyber-realm. A concerted, well-orchestrated attack on any Sector cybernetwork could cause considerable disruption Sector-wide.
  - The Federal Aviation Administration is collaborating with industry, academia, and other Federal agencies on aircraft cybersecurity research and development *(https://faaco.faa.gov/index.cfm/announcement/view/14453)*.
- **Cargo**
  - The air-cargo industry is highly dynamic and encompasses a wide range of users, characteristics which expose it to exploitation by terrorists.
  - Terrorists may use unsecured air transportation routes to transport arms, explosives, or operatives clandestinely to safe havens, training sites, or attack-staging locations. Ultimately, terrorists may use these access points and routes to transport more dangerous cargo, including weapons of mass destruction and their associated components.

For More Information

- Sector-Specific Agency: DHS, Transportation Security Administration (TSA), www.tsa.gov, Department of Transportation, www.dot.gov
- Federal Aviation Administration, www.faa.gov
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov
- DHS and TSA, *2010 Transportation Sector-Specific Plan*, www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf

Figure 2: Common, First-order Dependencies and Interdependencies of the Aviation Mode



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Freight Rail Mode
Transportation Sector

Sector Risk Snapshot

Figure 1: The rail network accounts for approximately 40 percent of U.S. freight moves by ton-miles (the length freight travels)
Source: Federal Railroad Administration, "National Rail Plan Progress Report," 2010

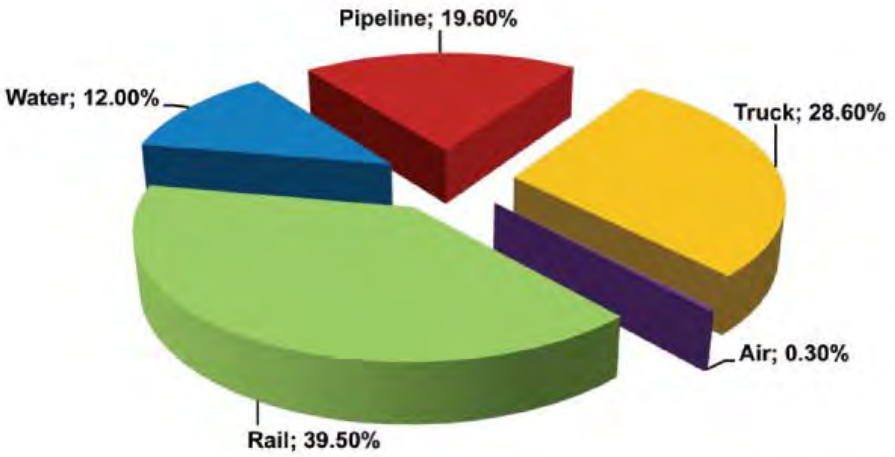
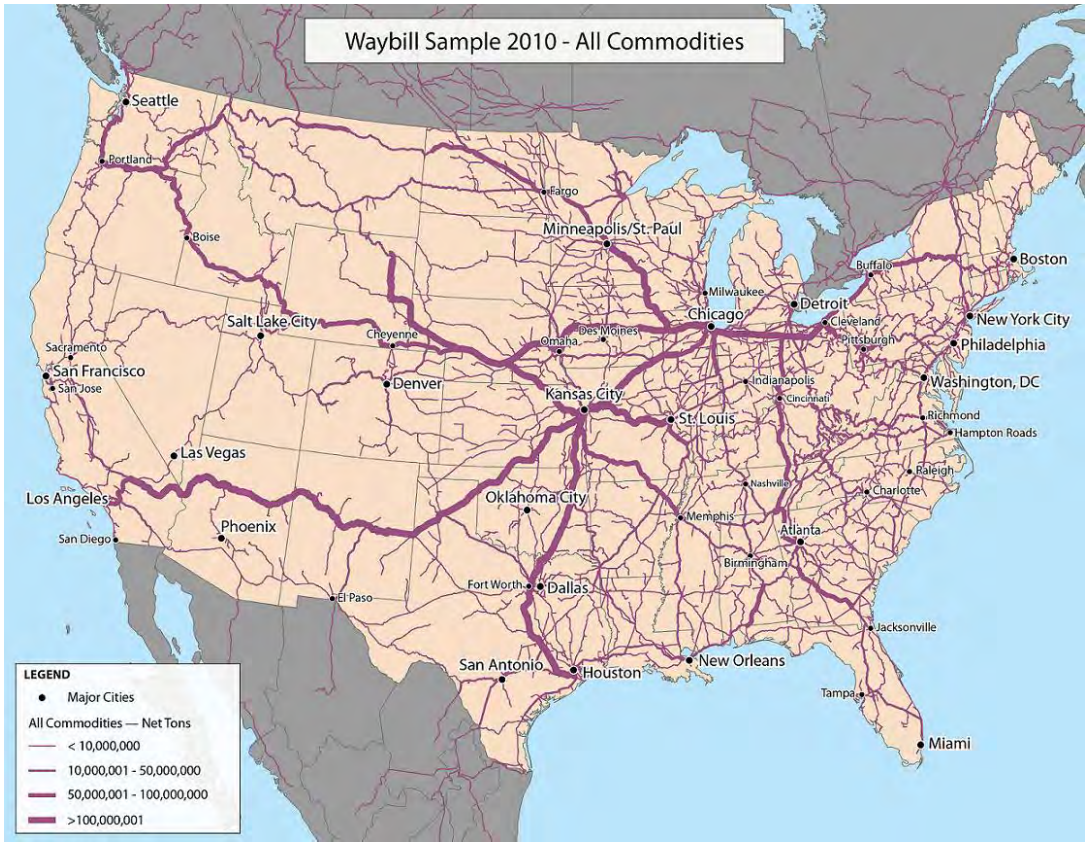


Figure 2: U.S. Freight Rail System Map
Source: Federal Railroad Administration, based on Surface Transportation Board's 2010 Carload Waybill Sample



Freight Rail Mode Overview

- **Freight Rail is one of seven modes that make up the Transportation Sector.**
- **The $60 billion industry consists of 140,000 miles of active rail track and provides 221,000 jobs across the country.**
- **Passenger and commuter rail systems throughout the country operate at least partially over tracks or rights-of-way owned by freight railroads. The National Railroad Passenger Corporation (Amtrak), for example, operates on more than 22,000 miles of track owned by freight railroads.**
- **Freight rail comprises 565 carriers divided among 3 Classes: Class I are the 7 major long haul carriers responsible for approximately 93 percent of total Sector revenue; the remaining 558 carriers (Class II and III) are local or short-haul carriers.**
- **Freight rail plays a critical role in support of the Energy Sector. Freight railroads are responsible for the transportation of more than 70 percent of all U.S. coal shipments (7.0 million carloads in 2010). Coal is the fuel that generates half of America's electricity.**

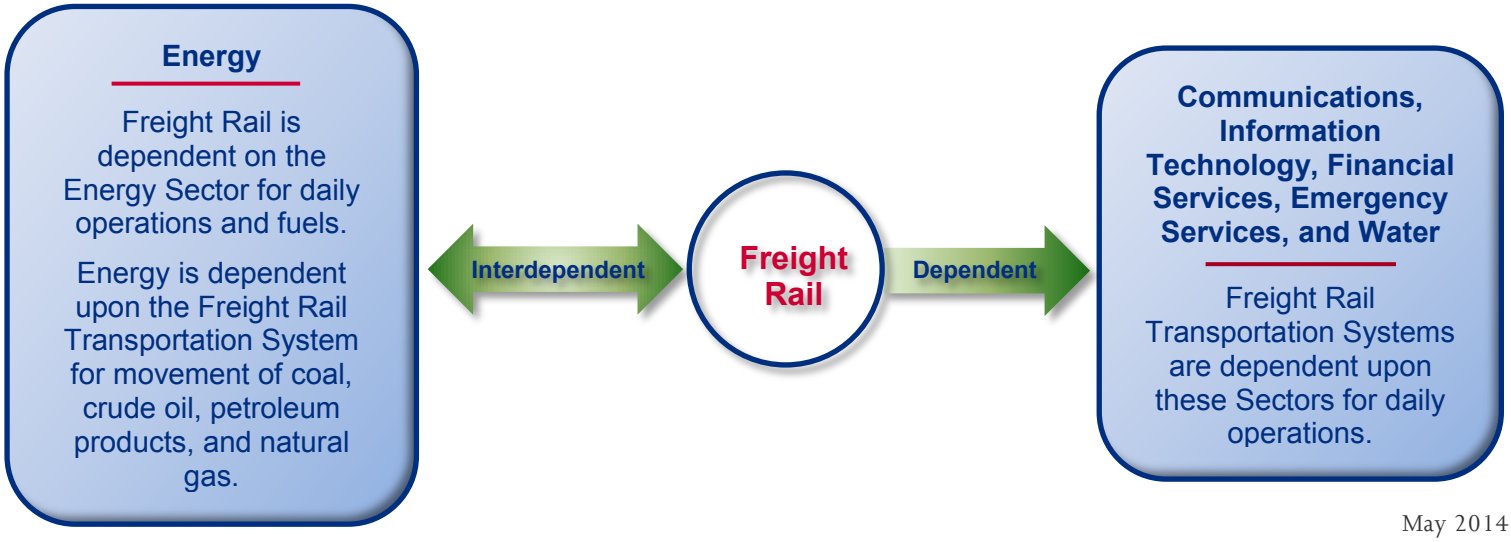
Threats and Hazards of Significant Concern

- **Sensitive Freight and Access Points**
  - Transportation Security Administration's (TSA's) risk assessment efforts examine the critical assets (e.g., bridges, tunnels, and yards) required for carrying out the freight railroad's basic mission of moving freight. Rail yards and terminals represent the fixed points in the network of railroad assets at which cars are transferred from one train to another, inspected, and repaired as necessary.
  - The movements of security-sensitive materials and toxic inhalation hazard materials through freight rail facilities, or over open tracks, leave railroad employees and public populations vulnerable if confronted with the threat of a terrorist attack.
- **Terrorist Attacks**
  - Intelligence reviews of various attacks worldwide, as well as analysis of seized documents, and the interrogation of captured and arrested suspects, reveal that there has been historic interest in carrying out attacks on railroad systems, particularly passenger rail systems due to the potential for large civilian casualties.
  - TSA concludes that long stretches of open, unattended track and numerous critical points (e.g., junctions, bridges, contiguous passenger rail sites) that are difficult to secure make the U.S. freight rail system an attractive target for terrorist attacks.
- **Insider Threat**
  - While the risk is considered low to moderate, documented evidence shows that disgruntled persons have tampered with tracks and other rail components.
  - Control systems are also vulnerable to tampering or external cyberattacks. However, the fail-safe nature of freight rail control systems may serve to mitigate the risk of a catastrophic incident.

For More Information

- Sector-Specific Agencies: DHS, Transportation Security Administration (TSA), www.tsa.gov, Department of Transportation, www.dot.gov
- Federal Rail Administration, www.fra.dot.gov
- American Association of Railroads, www.aar.org
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov
- DHS and TSA, 2010 Transportation Sector-Specific Plan, www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf

Figure 3: Common, First-order Dependencies and Interdependencies of the Freight Rail Mode



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

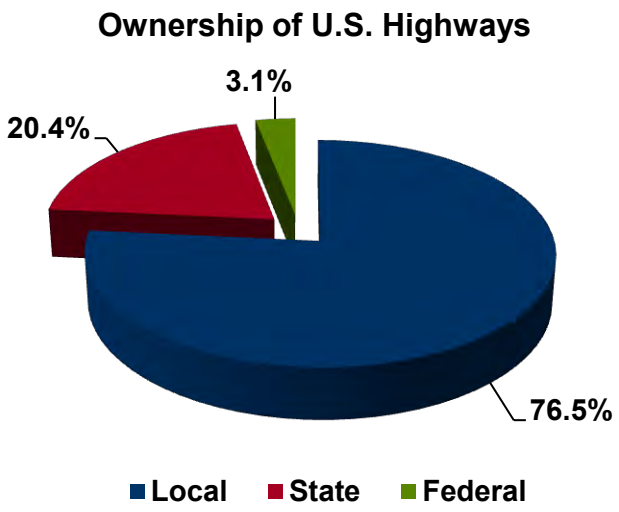
Highway and Motor Carrier Mode
Transportation Sector

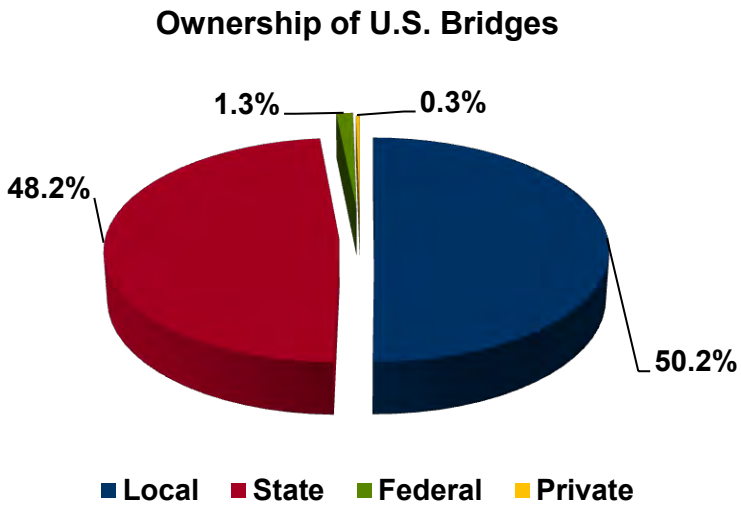
Sector Risk Snapshot

Highway and Motor Carrier Mode Overview

- **The Highway & Motor Carrier Mode assets include, but are not limited to, bridges, major tunnels, operations and management centers, trucks carrying hazardous materials, other commercial freight vehicles, motor coaches, school buses, and key intermodal facilities.**
- **The trucking industry is unique in that it is the only segment of the Highway Mode with complete intermodal supply chain relationships with aviation, maritime, mass transit, freight rail, and pipeline.**
- **The Nation's highway network includes nearly 4 million miles of roadway, almost 600,000 bridges, and some 400 tunnels.**
- **This Mode faces current and ongoing risk to facilities and materials due to terrorist attacks, natural hazards, and cyber-incidents.**
- **If successfully attacked or disrupted, impacts could result in regional shutdowns, diversions, or costly repairs with potentially severe results.**

Figure 1: Ownership of U.S. Highways and Bridges (2010)
Source: Department of Transportation, Federal Highway Administration, 2013 *Status of the Nation's Highways, Bridges, and Transit: Conditions & Performance*, January 31, 2014, www.fhwa.dot.gov/policy/2013cpr/overviews.htm





Hazardous Materials

- **The Transportation Security Administration (TSA) Hazardous Materials Endorsement Threat Assessment Program conducts a security threat assessment for any driver seeking to obtain, renew, or transfer a hazardous materials endorsement on a state-issued commercial driver's license.**
- **Hazardous materials include poisonous vapors, aerosols, liquids, and solids that have toxic effects on people, animals, or plants.**
- **They can have an immediate effect (a few seconds to a few minutes) or a delayed effect (2 to 48 hours).**
- **While potentially lethal, chemical agents are difficult to deliver in lethal concentrations. Outdoors, the agents often dissipate rapidly.**

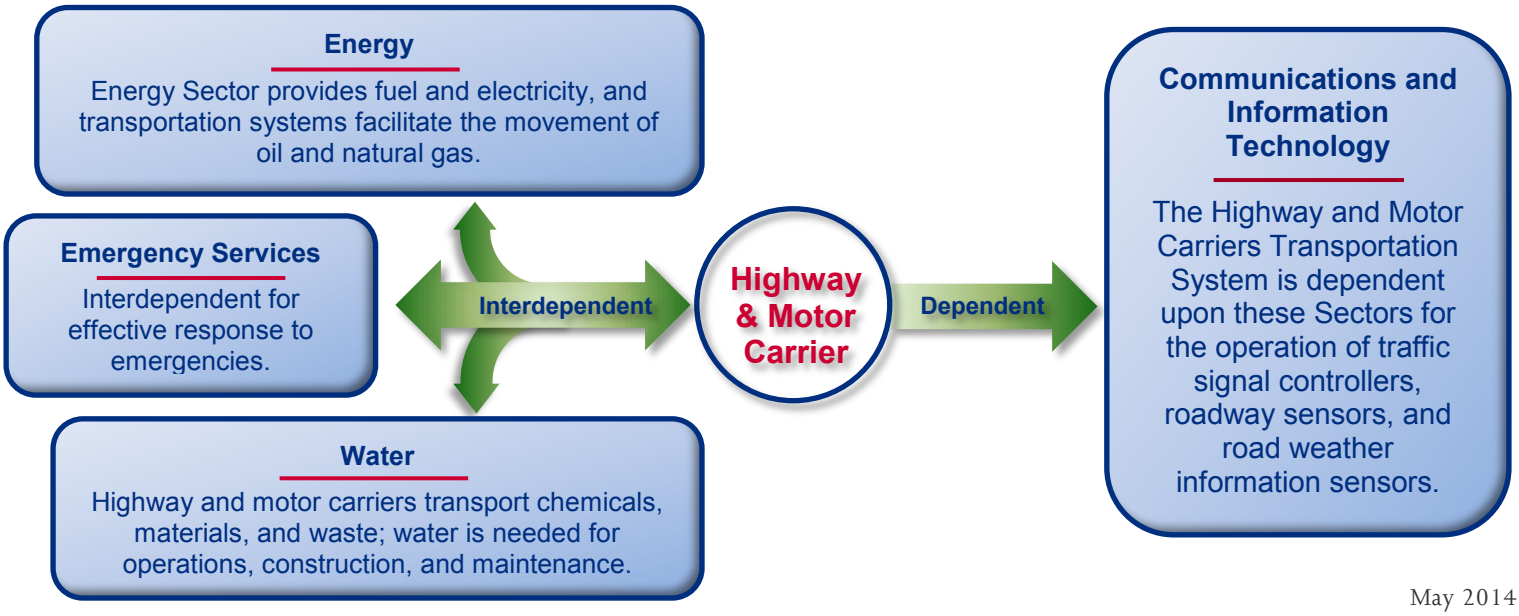
Threats and Hazards of Significant Concern

- **Terrorist attacks involving highway infrastructure and assets**
  - Highway infrastructure and assets may either be a target [e.g., improvised explosive devices (IEDs) against highway structures] or serves as a means to conduct an attack against other targets (e.g. use of a truck as a vehicle-borne IED against a building).
  - Use of HAZMAT materials as a terrorist attack is a serious and continuing risk to the Highway Mode.
- **Natural hazards, such as hurricanes, tornadoes, floods, and earthquakes**
  - Highway infrastructure may be severely disrupted or destroyed by such hazards, which may further complicate an overall disaster emergency response due to multiple cross-sector interdependencies.
- **Cyberattacks on highway infrastructure by terrorists, homegrown extremists, or disgruntled insiders**
  - Cyberattacks and intrusions on traffic control systems or other business systems pose a serious threat to highway infrastructure allowing malicious actors to manipulate or exploit control systems essential to operation of traffic control systems and highway messaging systems.

For More Information

- Sector-Specific Agency: DHS, Transportation Security Administration (TSA), www.tsa.gov, Department of Transportation, www.dot.gov
- American Association of State Highway and Transportation Officials, http://transportation.org/default.html
- American Bus Association, www.buses.org
- American Trucking Association, www.trucking.org/Pages/Home.aspx
- Federal Highway Administration, www.fhwa.dot.gov
- Pipeline and Hazardous Materials Safety Administration, http://phmsa.dot.gov/hazmat
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS and TSA, *2010 Transportation Sector-Specific Plan*, www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf

Figure 2: Common, First-order Dependencies and Interdependencies of the Highway and Motor Carrier Mode



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Maritime Mode Transportation Sector Sector Risk Snapshot

Figure 1: U.S. Import Value by Mode of Transportation, 2011, in Millions of U.S. Dollars

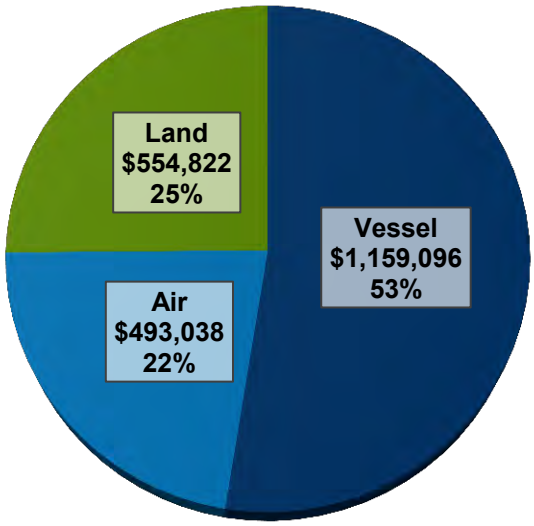
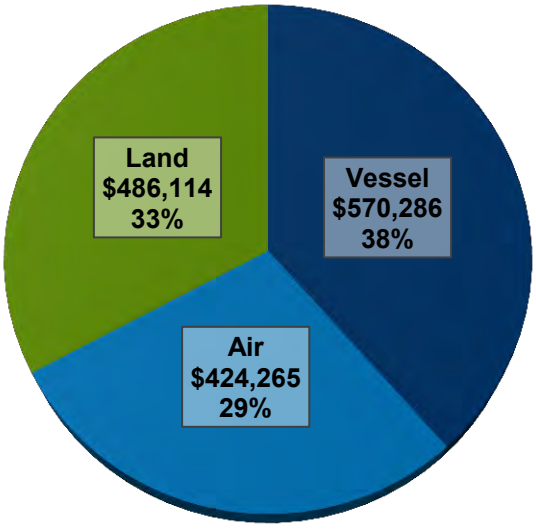


Figure 2: U.S. Export Value by Mode of Transportation, 2011, in Millions of U.S. Dollars



SOURCE Figures 1-2: U.S. Department of Transportation, Bureau of Transportation Statistics, "Maritime Trade and Transportation by the Numbers," accessed December 2013,www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/by_the_numbers/maritime_trade_and_transportation/index.html

Maritime Mode Overview

- **Maritime is one of seven modes that make up the Transportation Systems Sector.**
- **The Marine Transportation System (MTS) is a geographically and physically complex and diverse system consisting of waterways, ports, and intermodal landside connections that allow the various modes of transportation to move people and goods to, from, and on the water.**
- **The Mode consists of nearly 95,000 miles of coastline, 361 ports, over 25,000 miles of navigable waterways, over 29,000 miles of Marine Highway and 3.4 million square miles of Exclusive Economic Zone.**
- **The Exclusive Economic Zone is the area where the U.S. has jurisdiction over economic and resource management. U.S. Marine Highways are navigable waterways that have been designated by the Secretary of Transportation and have demonstrated the ability to provide additional capacity to relieve congested landside routes serving freight and passenger movement.**
- **Ships plying the maritime domain are the primary mode of transportation for global trade, carrying more than 80 percent of the world's trade by volume.**
- **In addition to the movement of freight, the marine transportation system serves as a critical component of the Nation's passenger transportation network. Over 200 ferry operators provide safe and reliable transportation for passengers and vehicles, while cruise ships and recreational boats contribute billions to the U.S. economy.**
- **The Mode faces current and ongoing risk for Sector facilities and materials due to potential cyberintrusion, port vulnerability, and insecure intermodal shoreside connections.**

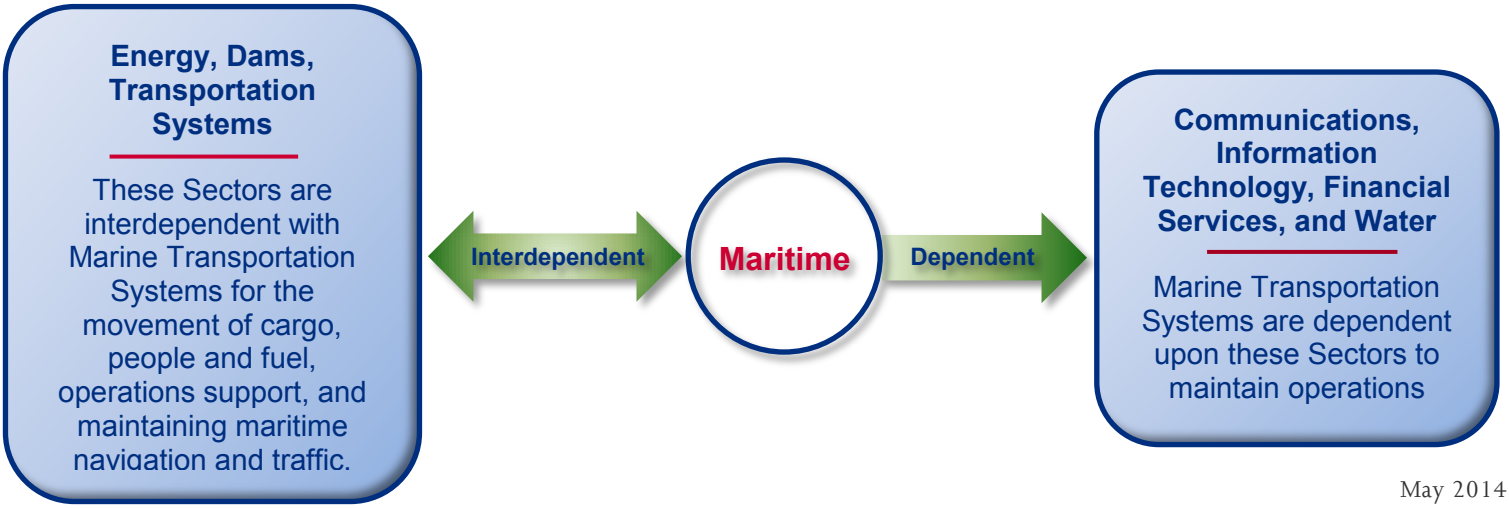
Threats and Hazards of Significant Concern

- **Natural Disasters**
  - From a risk-based perspective, the greatest risk facing the U.S. maritime domain, based on likelihood and consequence, is a major natural disaster, particularly hurricanes, flooding, drought, and tsunami.
  - These events are known to occur frequently and their consequences are often severe.
- **Cybersecurity**
  - Has become more important as the MTS has become increasingly dependent on cybersystems and faces a growing threat from cyberattacks.
  - These systems are used for a variety of purposes, including access control, navigation, traffic monitoring, and information transmission. Although the interconnectivity and utilization of cybersystems facilitate transport, they can also present opportunities for exploitation, contributing to risk for the MTS.
- **Malicious Actors**
  - Even though a robust security planning system (which includes ports, domestic facilities and vessels, as well as foreign vessels that call into the United States) has been implemented through the Maritime Transportation Security Act, a successful attack on critical infrastructure or nodes could cause transportation disruptions with cascading effects.
  - Port facilities and the ships and barges that transit port waterways are also somewhat vulnerable to tampering, theft, and unauthorized persons gaining entry to collect information and commit unlawful or hostile acts. Because of just-in-time method use, a successful attack against one node of maritime infrastructure could disrupt entire systems, cause congestion, limit capacity for product delivery, significantly damage the economy, or create an inability to project military force. Risks related to small vessel security also continue to be a focus of the U.S. Coast Guard (USCG).
- **"Dark Targets"**
  - Numerous maritime security assessments, most notably the DHS Small Vessel Security Strategy and the Current State Report of the Maritime Domain Awareness Interagency Solutions Analysis, have concluded that small "dark targets"—smaller vessels that are not required to carry electronic identification devices, make advance notices of arrival, or otherwise alert authorities to their whereabouts—constitute a major maritime awareness gap.
  - Although the majority of dark targets are legitimate, illicit operators can take advantage of their being difficult to detect and smuggle illegal cargo or people, or serve as waterborne platforms for terrorism.

For More Information

- Sector-Specific Agencies: DHS, Transportation Security Administration (TSA), http://www.tsa.gov, USCG, www.uscg.mil
- U.S. Department of Transportation, Maritime Administration, www.marad.dot.gov
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov
- DHS and TSA, 2010 Transportation Sector-Specific Plan, www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf

Figure 3: Common, First-order Dependencies and Interdependencies of the Maritime Mode



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Mass Transit Mode
Transportation Sector

Sector Risk Snapshot

Table 1: U.S. Unlinked Passenger Trips by Mode Report Year 2011		
Mode of Service	Passenger Trips	
	Millions	Percent
Bus	5,191	50.3
Bus Rapid Transit	6	0.1
Commuter Bus	37	0.4
Commuter Rail	466	4.5
Demand Response	191	1.9
Ferryboat	80	0.8
Heavy Rail	3,647	35.3
Hybrid Rail	6	0.1
Light Rail	436	4.2
Other Rail Modes*	44	0.4
Publico†	39	0.4
Streetcar	43	0.4
Transit Vanpool	34	0.3
Trolleybus	98	0.9
Total All Modes	10,319	100

*Aerial Tramway, automated guideway transit, cable car, inclined plane, and monorail.
†Publico is a mode of transit service provided by small vans or buses operated in San Juan, PR

Figure 1: Since 2004, Transit Use has Grown More Than Population or Highway Travel

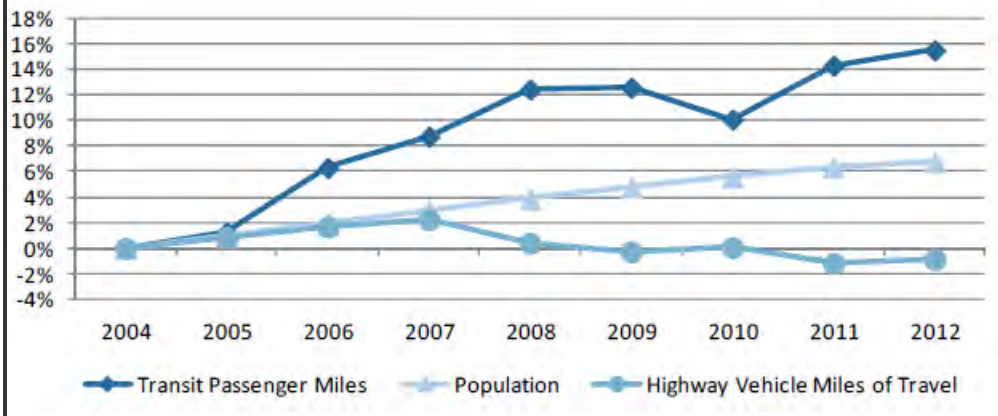


Table 1 and Figure 1 Source: American Public Transportation Association, "2013 Public Transportation Fact Book," Accessed December 2013, www.apta.com/resources/statistics/Pages/transitstats.aspx

Mass Transit Mode Overview

- **The Mass Transit and Passenger Rail Mode includes service by buses, rail transit (commuter rail, heavy rail, also known as subways, and light rail, including trolleys and streetcars), long-distance rail (namely Amtrak and Alaska Railroad), and other, less common types of service. It also includes demand response services for seniors and persons with disabilities, as well as vanpool/rideshare programs and taxi services operated under contract with a public transportation agency. The Mass Transit Mode does not include over-the-road motor coach operators, school bus systems, or private shuttle system operators.**
- **Passengers take 35 million trips each weekday in the United States. As part of an intermodal system of transportation, the Mass Transit Mode also connects to other modes of transportation through multimodal systems and within multimodal infrastructures.**
- **In 2011, U.S. public transportation was provided by 7,100 organizations, ranging from large multimodal systems to single-vehicle special demand response providers.**
- **In 2011, public transportation agencies spent $55 billion for operation of service and capital investment.**
- **The yearly totals for 2011 show that passengers took 10.3 billion trips and rode transit vehicles for 56.1 billion miles.**
- **The Mass Transit Mode includes thousands of employees, operational and maintenance facilities, construction sites, utilities, administrative facilities, and thousands of computerized networks, which facilitate operations and ensure efficient and reliable service.**

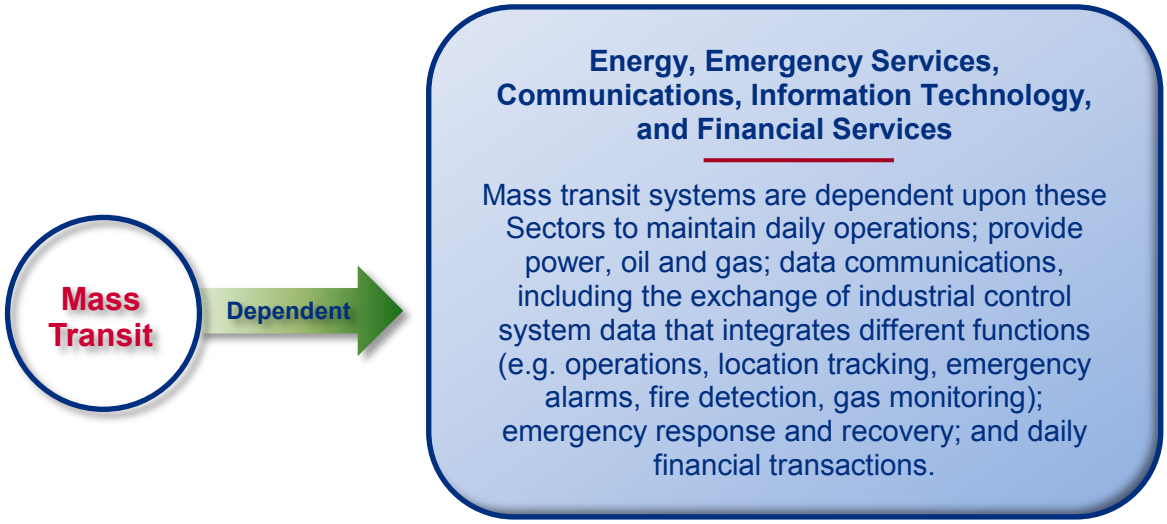
Threats and Hazards of Significant Concern

- **Access**
  - Unlike air transport, where strict access controls and universal security screening apply, public transportation operates more openly, in fast-paced operations with numerous entry, transfer, and exit points, to transport a high volume of passengers every day that greatly exceeds the number of air travelers. Multiple stops and interchanges lead to high passenger turnover, which is difficult to monitor effectively.
  - Broad geographical coverage of mass transit and passenger rail networks provide numerous options for access and getaway and afford the ability to use the system itself as the means to reach the location to conduct the attack.
- **Physical Attacks**
  - Physical attacks on the Mass Transit Mode represents a significant risk to the Sector, and may include a vehicle bomb near a station or track, explosives on a track, release of a caustic or biological agent in an enclosed station, tampering with rail switches, or an improvised explosive device or a lower-yield explosive in a station, train, or bus. Physical attacks on the Mass Transit Mode have to chance to result in scores of casualties. Consequences of such attacks can result in severe economic disruption and can impact the continuity of government operations.
- **Terrorism**
  - Attacks on mass transit systems are an attractive target for terrorists, and can result in a large number of victims, both killed and wounded, significant property damage, and loss of public confidence in public transit systems and Federal, State, local, and tribal governments. Coordinated attacks that simultaneously target multiple nodes in the system can potentially disrupt city-wide public transit operations, increasing public confusion and panic.
  - Examples of coordinated terrorist attacks on the Mass Transit Mode include the 1995 release of sarin gas in the Tokyo subway, which killed 13 people, severely injured 50, and caused temporary vision problems in over a 1000 others, and the 2005 bombings in London, in which IEDs were detonated in three London Underground trains across the city and a double-decker bus. The London bombings resulted in the deaths of 52 civilians and over 700 casualties.

For More Information

- Sector-Specific Agencies: DHS, Transportation Security Administration (TSA), www.tsa.gov and Department of Transportation, www.dot.gov
- American Public Transportation Association, www.apta.com
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS and TSA, *2010 Transportation Sector-Specific Plan*, www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf

Figure 2: Common, First-order Dependencies of the Mass Transit Mode



May 2014

Homeland Security

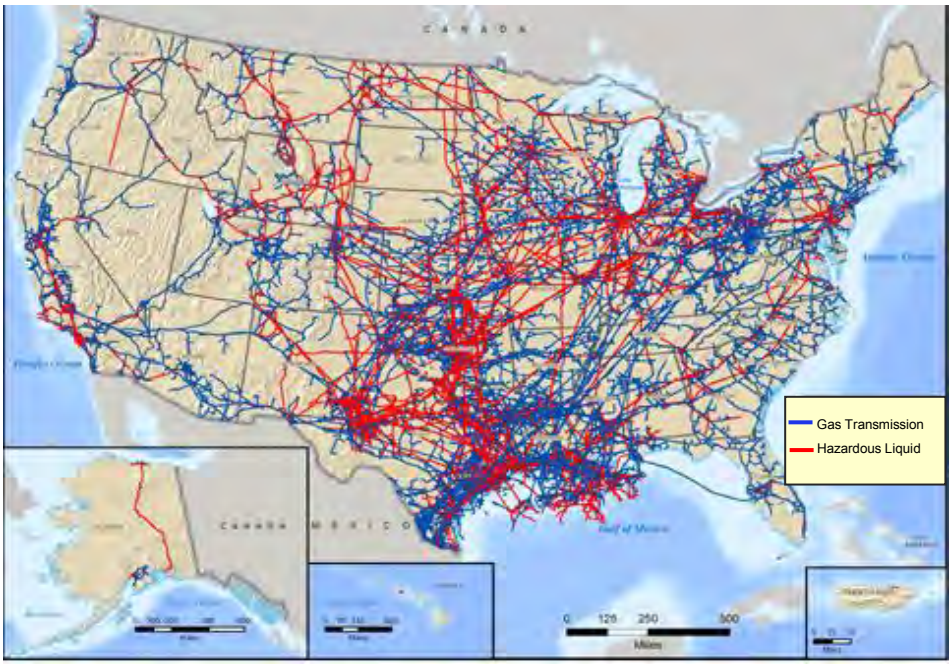
Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Pipeline Mode
Transportation Sector

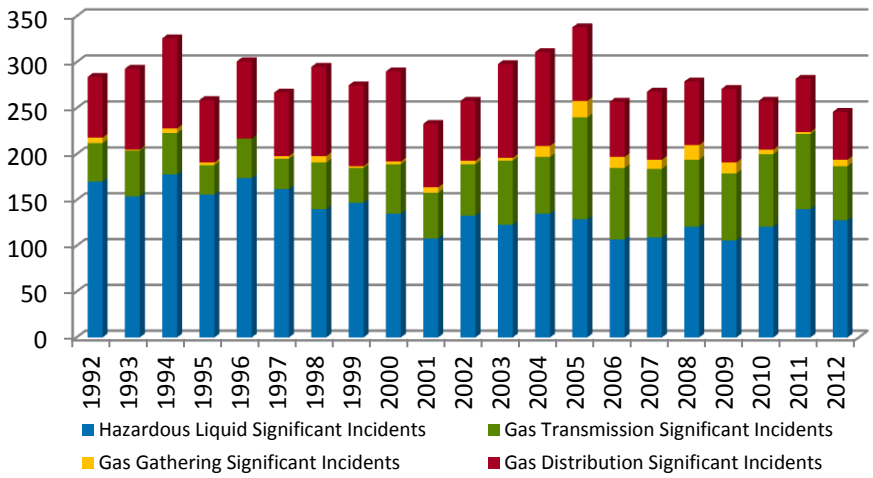
Sector Risk Snapshot

Figure 1: U.S. Gas Transmission and Hazardous Liquid Pipelines



Source: U.S. Department of Transportation, Pipeline and Hazardous Materials Safety Administration (PHMSA), National Pipeline Mapping System, March 2012.

Figure 2: Number of Significant Pipeline Systems Incidents 1992-2012*



*Significant Incidents are those incidents reported by pipeline operators when any of the following specifically defined consequences occur: 1) fatality or injury requiring in-patient hospitalization; (2) $50,000 or more in total costs; (3) highly volatile liquid releases of 5 barrels or more; or, (4) other liquid releases of 50 barrels or more resulting in an unintentional fire or explosion.

Source: PHMSA, *Significant Pipeline Incidents*, http://primis.phmsa.dot.gov/comm/reports/safety/sigpsi.html

Pipeline Mode Overview

- Pipelines are one of seven modes that make up the Transportation Sector.
- More than 2.5 million miles of pipelines network the United States to transport nearly all of the natural gas and about 65 percent of hazardous liquids, including crude and refined petroleum products, consumed within the United States.
- There are four main types of pipelines, most of which are buried underground: 1) Natural Gas Transmission and Storage; 2) Hazardous Liquid Pipelines and Tanks; 3) Natural Gas Distribution; and 4) Liquefied Natural Gas (LNG) Processing and Storage Facilities.
- Cross-border (international) pipelines are becoming increasingly important to the Nation's pipeline industry, which is prompting the U.S. and Canada to conduct joint assessments on trans-border infrastructure and identify necessary additional protective measures.
- While most pipelines are buried, the system has above-ground assets (e.g. wellheads, compressor stations, pumping stations, and processing facilities) that may be vulnerable to attack.
- The Mode faces current and ongoing risk to the movement of pipeline materials via direct attack upon critical pipeline system infrastructure and from cyberattacks against pipeline control systems and networks.

Toxic Inhalation Hazard

- A successful deliberate terrorist attack against toxic inhalation hazard (TIH) materials poses serious risks of fatalities and injuries, especially if the attack were to occur in a highly populated urban area.
- Pipelines are used to transport TIH chemicals such as anhydrous ammonia, a critical fertilizer for the American farming industry and feedstock for the chemical industry.

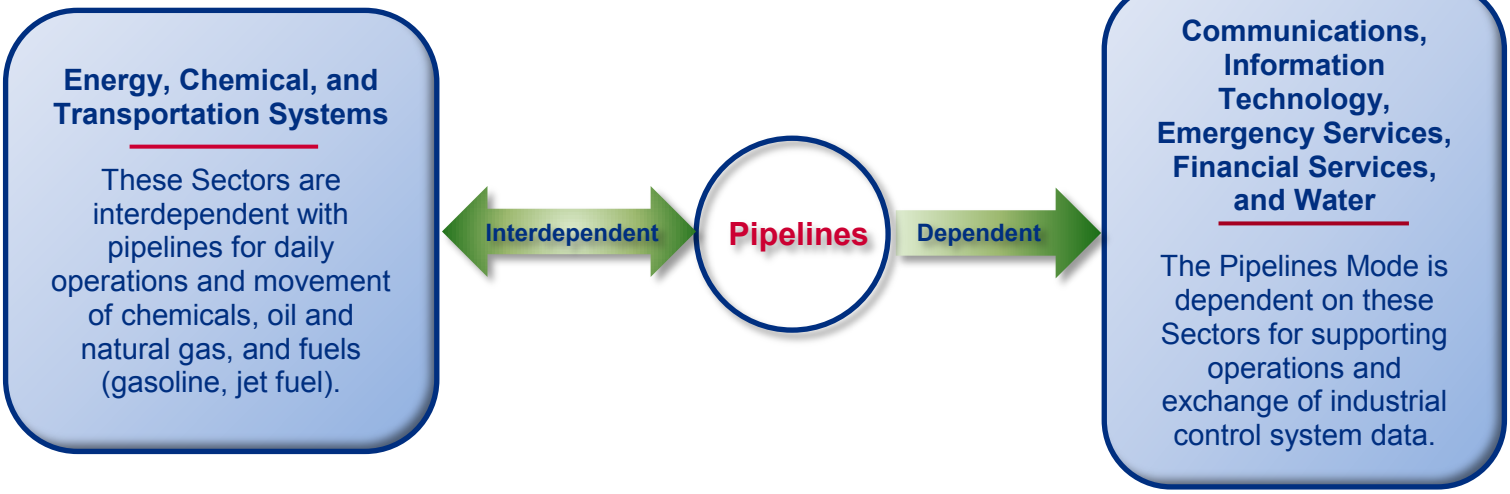
Threats and Hazards of Significant Concern

- **Release of Pipeline Materials**
  - The pipeline system is uniquely vulnerable to terrorist attacks because of the products transported and because pipeline networks are widely dispersed across both remote and urban portions of the country.
  - Many pipelines carry volatile and flammable materials that have the potential to cause serious injury to the public and the environment. A pipeline facility could be vandalized or attacked with explosive devices, resulting in flow disruption or the release of its contents.
- **Cyberthreats**
  - Pipelines are also susceptible to cyberattacks on their computer control systems. Cyberthreats could result from the acts of a terrorist-hacker or a rogue employee with computer access.
  - The latter threat requires that specific attention be given to personnel security credentials and access protocols, as well as general cybersecurity protocols.
- **Cascading Effects from Disruptions to Critical Dependencies**
  - In addition, attacks on other infrastructure, such as regional electricity grids and communication networks, could cause a serious disruption in pipeline operations, posing risks for all Sectors serviced by pipelines, including the military and major commercial installations (Figure 3).

For More Information

- Sector-Specific Agencies: DHS, Transportation Security Administration (TSA), www.tsa.gov, Department of Transportation, www.dot.gov
- Pipeline and Hazardous Materials Safety Administration (PHMSA), www.phmsa.dot.gov
- American Petroleum Institute, www.api.org
- American Gas Association, www.aga.org
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov
- DHS and TSA, *2010 Transportation Sector-Specific Plan*, www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf
- Interstate Natural Gas Association of America (INGAA) , www.ingaa.org
- Association of Oil Pipelines (AOPL), www.aopl.org

Figure 3: Common, First-order Dependencies and Interdependencies of the Pipeline Mode



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Postal and Shipping Mode
Transportation Sector

Sector Risk Snapshot

Table 1: Size of the U.S. Mailing Industry

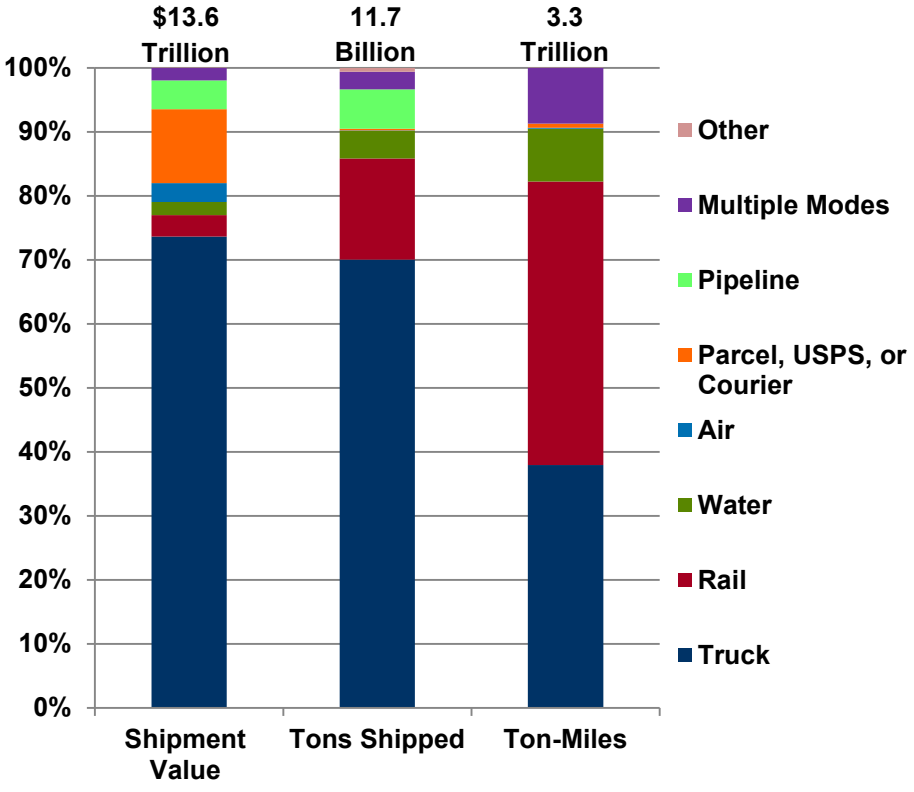
The size of the mailing industry compared to other key U.S. industries is significant. What happens in the mailing industry echoes throughout the economy as it supports over 8.6 percent of the U.S. Gross Domestic Product.

Industry	Number of Jobs Supported	Annual Revenue Supported
Mailing	8.4 million	$1.3 Trillion
Airline	10.0 Million	$1.0 Trillion
Oil and Natural Gas	9.6 million	$1.1 Trillion

SOURCE: U.S. Postal Service, *USPS FY2013 Annual Report to Congress*, 2013.

Figure 1: Value, Tonnage, and Ton-Miles of Shipments by Mode

In 2012, parcel delivery, USPS, and other courier services accounted for 11.6 percent of shipments by value, but less than half of one percent by tonnage, demonstrating that the Postal and Shipping industry typically ships higher value products.



SOURCE: U.S. Department of Transportation, Bureau of Transportation Statistics and U.S. Department of Commerce, U.S. Census Bureau, *2012 Economic Census: Transportation Commodity Flow Survey*, Preliminary Release, December 2013.

Postal and Shipping Mode Overview

- Postal and Shipping is one of seven modes that make up the Transportation Sector.
- Postal and Shipping was formerly recognized as a stand-alone Sector until the February 2013 release of Presidential Policy Directive-21 (PPD-21), when Postal and Shipping was incorporated into the Transportation Sector.
- Composed of large integrated carriers, regional and local courier service providers, mail services and mail management firms, and chartered air delivery services.
- Four large integrated carriers—the U.S. Postal Service (USPS), the United Parcel Service (UPS), FedEx, and DHL International—account for 94 percent of the Mode's assets systems, networks, and functions.
- Postal and Shipping moves more than 720 million messages, products, and financial transactions each day.
- The threat environment to the mode includes attacks on infrastructure, operations, and employees, and the use of the Mode to attack its customers, other Sectors, or the economy as a whole, using targeted or widespread techniques and tactics.
- Mode risk is a function of the vulnerability of an extremely large number of collection points, many of which are open and anonymous.
- The Mode is a highly trusted entity, and its employees and representatives have ready access to businesses and residences throughout the country.
- The Mode faces current and ongoing risk, due to terrorist attacks using hazardous materials, as well as chemical, biological, radiological, and nuclear explosives (CBRNE) for mail-based attacks.

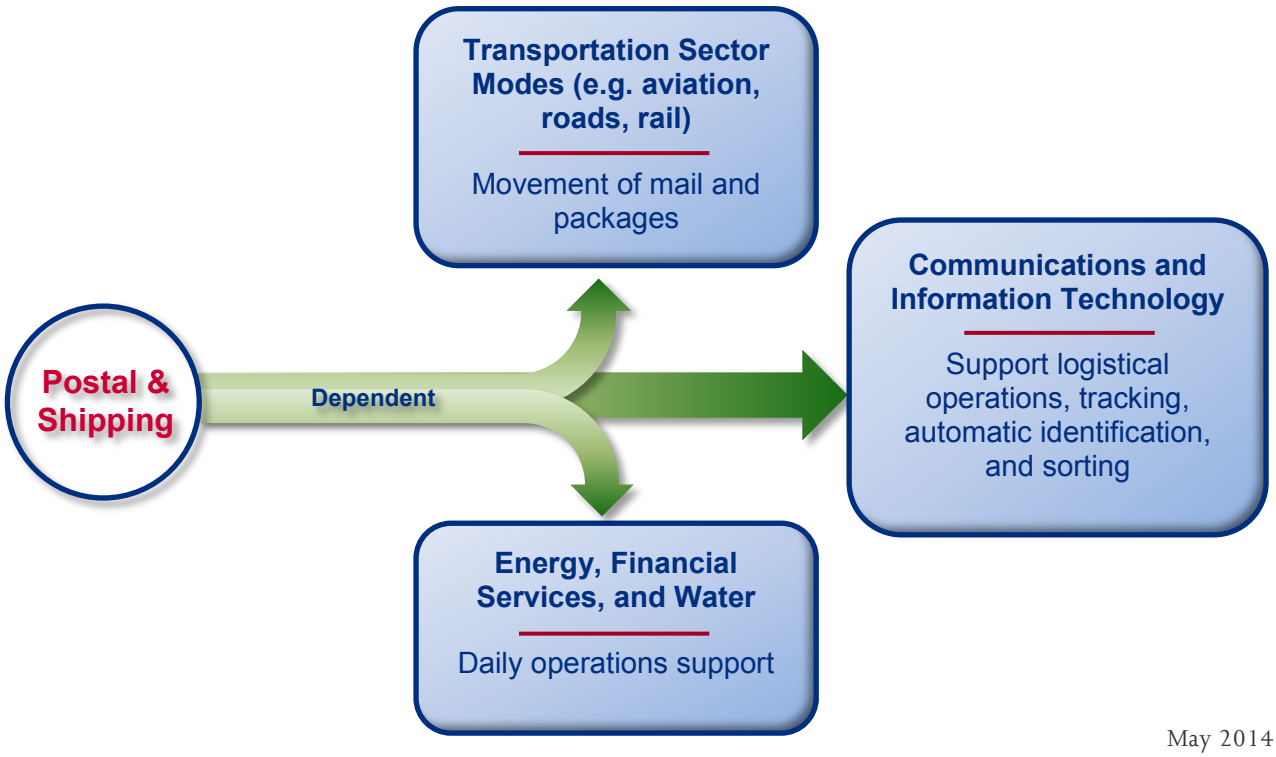
Threats and Hazards of Significant Concern

- **Open Access and Entry Points**
  - By design, the Postal and Shipping Mode is an open system with an extremely large number of entry and collection points, many of which are anonymous. These facilities present a vast number of entry points where dangerous materials could be inserted for delivery to intended targets.
- **Mail-based Threats**
  - Mail-based threats pose a significant and continuing risk for the Postal and Shipping Mode. For example, the Unabomber, Ted Kaczynski, hand-delivered or used the Postal Service over the course of 17 years to deliver parcel bombs that killed three Americans and injured 24 more (FBI, 2008).
  - Physical attacks using improvised explosive devices (letter bombs and parcel-based attacks) against postal and shipping facilities, or against other Sectors, could result in changes in the flow of ground and air mail and delays in mail service.
  - Postal and shipping infrastructure may be severely disrupted by such attacks, which may further complicate an overall disaster emergency response due to multiple cross-sector interdependencies (Figure 2).
- **Attacks Using Hazardous Materials or CBRNE**
  - The Postal and Shipping Mode is one of the few infrastructures that have been threatened by biological agents; in 2001, the USPS was used as a vehicle for delivering anthrax against multiple targets.
  - In 2010, the terrorist organization Al-Qaeda in the Arabian Peninsula (AQAP) planted bombs in two packages of printer cartridges found on separate cargo planes. Both U.S. and U.K. intelligence officials speculated that the bombs were probably designed to detonate mid-air, with the intention of destroying both planes over Chicago or another city in the U.S. (BBC, 2010, www.bbc.co.uk/news/world-us-canada-11671377)

For More Information

- Sector-Specific Agencies: DHS, Transportation Security Administration (TSA), www.tsa.gov, Department of Transportation, www.dot.gov
- USPS, www.usps.com and http://about.usps.com/securing-the-mail/mail-security-center.htm
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov

Figure 2: Common, First-order Dependencies of the Postal and Shipping Mode



May 2014

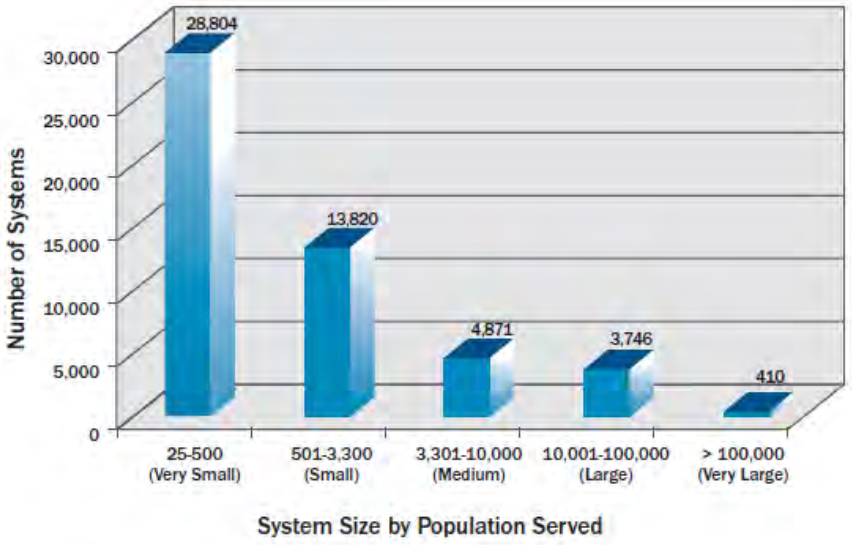
Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Water and Wastewater Systems Sector
Sector Risk Snapshot

Figure 1: Community Drinking Water Systems and System Size.
Source: EPA, Safe Drinking Water Information System (SDWIS)



Drinking Water

- A drinking water contamination incident or the denial of drinking water services would have far-reaching public health, economic, environmental, and psychological impacts across the Nation.
- Other critical services, such as fire protection, healthcare, and heating and cooling processes, would also be disrupted by the interruption or cessation of drinking water service, resulting in significant consequences to the national or regional economies.
- The majority of community water systems (CWS) are small systems that serve approximately 8 percent of the population who get their water from CWS (Figure 1).
- Only 17 percent of CWS are classified as medium or large systems, but these systems serve the majority of the U.S. population.
- The EPA reports that CWS served 300.2 million people, while non-community water systems (e.g. schools, factories, hospitals, campgrounds, and gas stations that have their own water systems) served 19.5 million people in 2010.

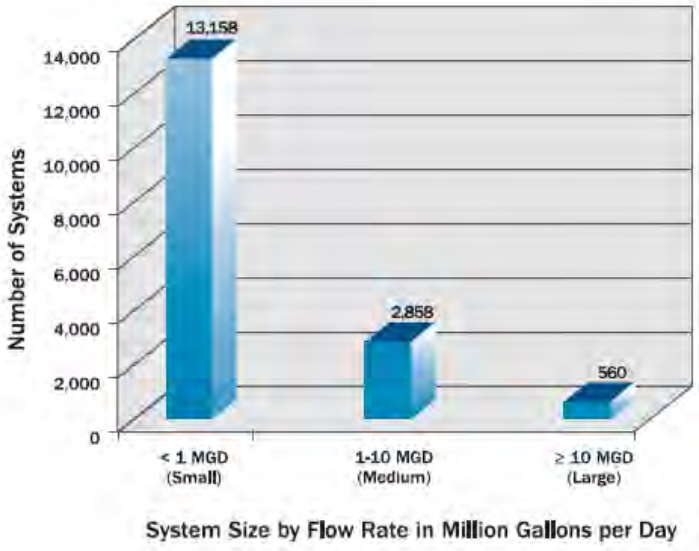
Wastewater

- Disruption of a wastewater treatment utility or service can cause loss of life, economic impacts, and severe public health and environmental impacts.
- If wastewater infrastructure were to be damaged, the lack of redundancy in the Sector might cause denial of service to domestic and industrial users.
- The majority of utilities are small in size, and provide wastewater treatment to approximately 23 million people (Figure 2).
- The medium or large size utilities systems serve the majority, at about 90 percent of the population.

Water Sector Overview

- **Comprises approximately 155,000 public drinking water systems (includes both community and non-community water systems, such as schools, factories and campgrounds) and approximately 16,500 publicly owned wastewater treatment utilities (EPA, 2012 and DHS, 2010).**
- **Water utilities consist of source waters, treatment facilities, pumping stations, storage sites, and extensive distribution, collection, and monitoring systems.**
- **The Water Sector is vulnerable to a variety of all-hazard threats including contamination with deadly agents; insider threats; physical attacks using improvised explosive devices (IEDs); cyberattacks; and natural hazards.**
- **Successful attacks on a drinking water or wastewater system could result in large numbers of illness, casualties, and denial of service, which could severely impact the Nation's public health and economic vitality.**

Figure 2: Publicly Owned Wastewater Treatment Works and System Size



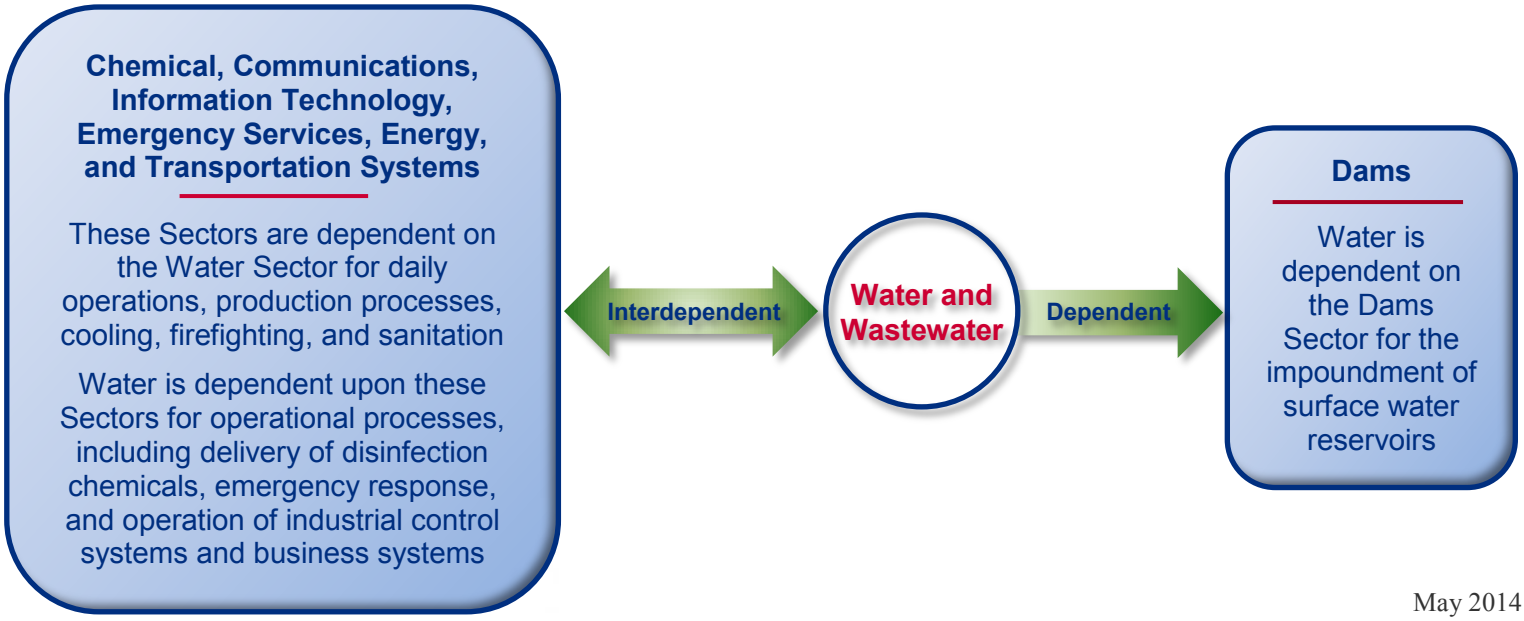
Threats and Hazards of Significant Concern

- **Chemical, Biological, or Radiological Contamination**
  - Most public water supplies are monitored and treated to prevent the distribution of contaminated drinking water.
  - The risk of CBR contamination stems from both the enduring terrorist threat to contaminate the U.S. water supply and the serious health impacts that could result from an undetected contaminant.
  - These impacts could vary depending on the type of substance, route of exposure (ingestion, absorption, inhalation), and amount of time before the contaminant is detected.
- **Natural Hazards**
  - Natural hazards, such as hurricanes, tornadoes, floods, earthquakes, and drought, pose a serious and continuing risk for the Sector.
  - Water infrastructure may be severely disrupted or destroyed by such hazards, which may further complicate an overall disaster emergency response due to multiple cross-sector interdependencies (Figure 3).
  - Critical water shortages may also result from drought conditions and climate change, leading to water use restrictions and rationing.
- **Physical and Cyberattacks by Terrorists, Homegrown Extremists, or Disgruntled Insiders**
  - Physical attacks using IEDs on chemical storage tanks or other critical nodes in a drinking water or wastewater system could result in a release of hazardous materials or in a long-term loss of service should a "single-point-of-failure" be destroyed.
  - Cyberattacks and intrusions on supervisory control and data acquisition (SCADA) systems or other business systems pose a serious threat to the Water Sector, allowing malicious actors to manipulate or exploit control systems essential to operation of drinking water and wastewater utilities.

For More Information

- Sector-Specific Agency: Environmental Protection Agency, www.epa.gov/
- Environmental Protection Agency (EPA), Water Security, http://water.epa.gov/infrastructure/
- DHS, *Infrastructure Protection Report Series: Community Water Systems (CVPIPM)*, version: 29 August 2011
- DHS and EPA, *2010 Water Sector-Specific Plan*, hwww.dhs.gov/files/programs/gc_1179866197607.shtm
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov

Figure 3: Common, First-order Dependencies and Interdependencies of the Water Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

The Office of Cyber and Infrastructure Analysis (OCIA) produces Sector Risk Snapshots in support of the Homeland Security Enterprise as part of the Department's efforts to carry out comprehensive assessments of the risks to critical infrastructure, and to facilitate a greater understanding of the emerging threats to and vulnerabilities of critical infrastructure in the United States. For more information, contact OCIA@hq.dhs.gov or visit our Website at www.dhs.gov/office-cyber-infrastructure-analysis.

Homeland
Security