GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 16, 2008

The Honorable James R. Langevin
Chairman
Subcommittee on Emerging Threats, Cybersecurity,
and Science and Technology
Committee on Homeland Security
House of Representatives

The Honorable Sheila Jackson-Lee
Chairwoman
Subcommittee on Transportation Security
and Infrastructure Protection
Committee on Homeland Security
House of Representatives

Subject: *Information Technology: Federal Laws, Regulations, and Mandatory Standards for Securing Private Sector Information Technology Systems and Data in Critical Infrastructure Sectors*

Federal policy identifies 18 infrastructure sectors—such as banking and finance, energy, public health and healthcare, and telecommunications—that are critical to the nation's security, economy, public health, and safety.[1] Because these sectors rely extensively on computerized information systems and electronic data, it is crucial that the security of these systems and data is maintained. Further, because most of these infrastructures are owned by the private sector, it is imperative that public and private entities work together to protect these assets. The federal government uses both voluntary partnerships with private industry and requirements in federal laws, regulations, and mandatory standards to assist in the security of privately owned information technology (IT) systems and data within critical infrastructure sectors.

As agreed, our objectives were to (1) identify, for each critical infrastructure sector, the federal laws, regulations, and mandatory standards that pertain to securing that sector's privately owned IT systems and data and (2) identify enforcement mechanisms for each of the above laws, regulations, and mandatory standards. To accomplish these objectives, we solicited information from the federal agencies responsible for overseeing each critical infrastructure sector to identify the applicable requirements, as well as the mechanisms and authorities available to the government to enforce compliance with these requirements.

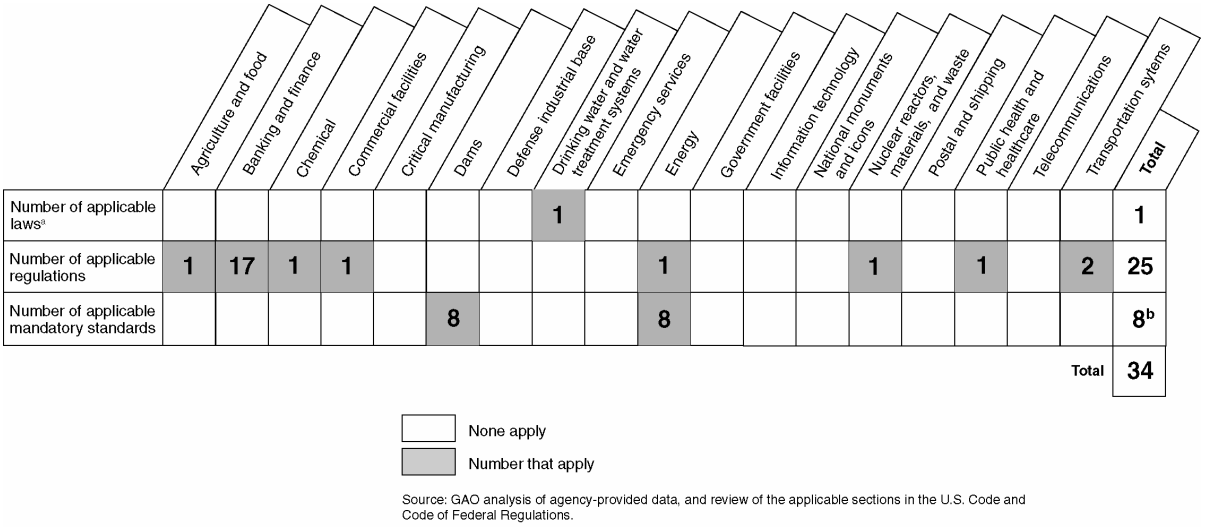
[1] See, for example, Homeland Security Presidential Directive 7.

On July 24, 2008, we presented a briefing to the staffs of the House Homeland Security Subcommittees on Transportation Security and Infrastructure Protection and Emerging Threats, Cybersecurity, and Science and Technology. This report briefly summarizes our findings and transmits the presentation slides we used to brief the staffs. The full briefing, including our scope and methodology, is reprinted in enclosure I.

At Least 34 Federal Legal Requirements Exist within Critical Infrastructure Sectors for Securing Privately Owned IT Systems and Data

There are at least 34 federal laws, regulations, and mandatory standards that pertain to securing privately owned IT systems and data in our nation's critical infrastructure sectors. Figure 1 summarizes the number of federal laws, regulations, and mandatory standards, by critical infrastructure sector.[2]

Figure 1: Summary of Federal Legal Requirements for Securing Privately Owned IT Systems and Data within Critical Infrastructure Sectors



Source: GAO analysis of agency-provided data, and review of the applicable sections in the U.S. Code and Code of Federal Regulations.

[a]The number of applicable laws does not include the authorizing laws for the regulations and mandatory standards.
[b]The dams and energy sectors share a common set of 8 mandatory standards that are applicable to both sectors, but these standards are counted only once in this total.

As shown in the figure, of the 34, 1 is a law, 25 are regulations, and 8 are mandatory standards.[3] These requirements pertain to 10 of the 18 critical infrastructure sectors, including the agriculture and food; energy; nuclear reactors, materials, and waste; and transportation systems sectors. For example, the drinking water and water

[2] These requirements do not necessarily pertain to just critical IT systems and data. Further, these requirements do not necessarily apply to all of a sector's entities, require all of an entity's IT systems and data to be secure, or provide for comprehensive coverage of the polices and procedures necessary to ensure adequate security. Lastly, in the absence of a law, regulation, or mandatory standard in a particular sector there may be other mechanisms or motives for protecting privately owned IT systems and data.
[3]We did not include the authorizing laws for the regulations and mandatory standards.

treatment systems sector has 1 applicable law. In addition, the energy sector has 1 applicable regulation and 8 applicable mandatory standards.

Eight sectors did not identify requirements that pertain to securing privately owned IT systems and data. They are: critical manufacturing, defense industrial base, emergency services, government facilities, information technology, national monuments and icons, postal and shipping, and telecommunications.

A more detailed description by sector, including authorizing laws, regulatory citations, regulatory agencies, regulated entities, and the statutory and regulatory requirements, is provided in enclosure I.

Federal Legal Requirements Contain Mechanisms for Enforcing Compliance

Each of the 34 federal legal requirements has at least one enforcement mechanism. These mechanisms include court injunctions, civil monetary penalties, criminal penalties, and administrative actions, such as license revocation and suspension. Typically, these mechanisms are what agencies use to enforce requirements in general, and are not necessarily specific to the requirements for securing privately owned IT systems and data. Examples of the sectors' enforcement mechanisms are as follows:

- For banking and finance, the sector's 17 applicable regulations may be enforced through
  - cease and desist orders;
  - civil monetary penalties;
  - criminal monetary penalties;
  - limitations on activities, functions, and operations;
  - registration revocations; and
  - termination of bank deposit insurance.

  In particular, the enforcement mechanisms for several of the sector regulations provide the potential for a civil monetary penalty against an enterprise of up to $1 million per day that the enterprise is in violation, if it is found that the violation or conduct was done knowingly and caused, or would be likely to cause, a substantial loss to the enterprise.

- For drinking water and water treatment, the sector's applicable law may be enforced through
  - administrative orders,
  - civil monetary penalties, and
  - court injunctions.

  Specifically, the law provides that a community water system in violation of the law could be fined up to $25,000 per violation.

- For nuclear reactors, materials, and waste, the sector's applicable regulation may be enforced through
  - court injunctions,

- civil monetary penalties,
- cease and desist orders,
- license modification orders,
- suspension orders, and
- revocation orders.

This regulation provides that an entity that violates the regulation could be fined up to $100,000 per day per violation.

A more detailed description by sector, including examples of enforcement mechanisms for each requirement, is provided in enclosure I. In commenting on a draft of the letter and the briefing, the sector-specific agencies agreed with our reporting of the information.

We are sending copies of this report to interested congressional committees and other interested parties. We also will make copies available to others upon request. In addition, this report will be available at no charge on GAO's Web site at http://www.gao.gov.

Should you or your staffs have any questions on matters discussed in this report, please contact Dave Powner at (202) 512-9286 or pownerd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this correspondence. In addition to the individual named above, Gary Mountjoy (Assistant Director), Scott Borre, Neil Doherty, Michael Gilmore, Franklin Jackson, Emily Longcore, Lee McCracken, and Adam Vodraska made key contributions to this report.

David A. Powner
Director, Information Technology
Management Issues

Enclosure

Enclosure I

Information Technology: Federal Laws, Regulations, and Mandatory Standards for Securing Private Sector Information Technology Systems and Data in Critical Infrastructure Sectors

Briefing for Staff Members of the

Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security

and the

Subcommittee on Transportation Security and Infrastructure Protection, Committee on Homeland Security.

July 24, 2008

Table of Contents

Introduction

Results in Brief

Background

Results

- Objective 1 – Federal Laws, Regulations, and Mandatory Standards
- Objective 2 – Enforcement Mechanisms

Agency Comments

Attachment 1: Objectives, Scope, and Methodology

Attachment 2: Detailed List and Description of Applicable Federal Laws, Regulations, and Mandatory Standards

Introduction

Federal policy identifies 18 infrastructure sectors as critical to the nation's security, economy, public health, and safety. Because these critical infrastructure sectors—such as banking and finance, telecommunications, energy, and public health and healthcare—rely extensively on computerized information systems and electronic data, it is crucial that the security of those systems and data is maintained. Further, because most of the infrastructures are owned by private companies, it is imperative that public and private entities work together to protect these assets.

The federal government uses both voluntary partnerships with private industry and requirements in federal laws, regulations, and mandatory standards to assist in the security of privately owned IT systems and data within critical infrastructure sectors.

Introduction

As agreed, our objectives were to

1. identify, for each critical infrastructure sector, the federal laws, regulations, and mandatory standards that pertain to securing that sector's privately owned information technology systems and data, and
2. identify enforcement mechanisms for each of the above laws, regulations, and mandatory standards.

For the purposes of this review, federal laws are defined as statutes enacted by the Congress of the United States that pertain to matters which are within the legislative authority delegated to the national government by the United States Constitution. Federal regulations are defined as the general and permanent rules published in the *Federal Register* by a federal department or agency. Federal mandatory standards are defined as requirements adopted by a federal department or agency with the legal authority to regulate the entities and/or activities that are the subject of the standards.

To accomplish the first objective, we solicited information from the federal agencies responsible for overseeing each sector to identify the applicable requirements. We reviewed, among other things, sections of the United States Code, the Code of Federal Regulations, and federal mandatory standards identified by the agencies to confirm the requirements that were applicable in each sector. After reviewing each sector's specific laws, regulations, and mandatory standards, we requested further clarification from the regulating agencies when we were unable to validate the applicability of the requirements. Where we could not reconcile our analysis with the agencies' interpretations, we reported the characterizations of the federal agencies since they implement and enforce the requirements. There is a possibility that the agencies did not identify all applicable requirements and we did not conduct an independent search for applicable requirements. We did not include privately owned IT systems and data that are operated on behalf of a federal agency. In particular, our review did not include systems owned by contractors that are operated on behalf of federal agencies subject to governmentwide computer security and privacy requirements, such as the Federal Information Security Management Act of 2002, that require agencies (e.g. the Department of Defense) to ensure that contractors running agency IT systems meet federal information security requirements.

To accomplish the second objective, federal agency officials responsible for enforcing the requirements identified in the first objective identified the mechanisms and authorities available to the agencies and others to enforce compliance with these requirements. The mechanisms and authorities identified are examples of the enforcement mechanisms available to the agencies, and do not necessarily constitute a complete list. We verified the information provided by the agencies by analyzing the applicable sections of the United States Code, Code of Federal Regulations, and other appropriate sources. Attachment I provides further details on our objectives, scope, and methodology.

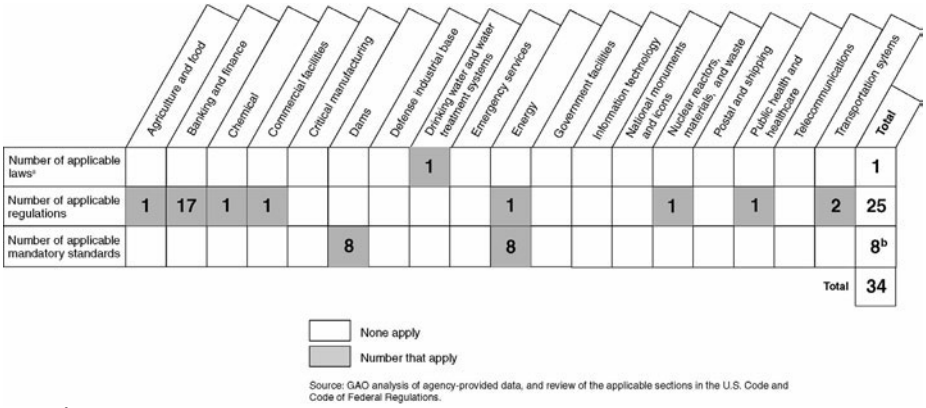
We performed our work at federal agencies in the Washington, D.C., metropolitan area from November 2007 to July 2008. We conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings based on our audit objectives.

Results in Brief

We identified 34 federal laws, regulations, and mandatory standards that pertain to securing privately owned IT systems and data in our nation's critical infrastructure sectors.[1] (Figure 1 summarizes, by critical infrastructure sector, the number of federal laws, regulations, and mandatory standards that have been identified by the federal agency officials responsible for overseeing each sector.)

[1] These requirements do not necessarily pertain [specifically? solely?] to critical infrastructure IT systems and data.

Figure 1: Summary of Federal Legal Requirements for Securing Privately Owned IT Systems and Data within Critical Infrastructure Sectors



[a]The number of applicable laws does not include the authorizing laws for the regulations and mandatory standards.
[b]The dams and energy sectors share a common set of 8 mandatory standards that are applicable to both sectors, but these standards are counted only once in this total.

Results in Brief

As shown in the figure, of the 34, 1 is a law, 25 are regulations, and 8 are mandatory standards. These requirements pertain to 10 of the 18 critical infrastructure sectors, including the nuclear reactors, materials, and waste and transportation systems sectors. For example, the drinking water and water treatment systems sector has one applicable law, and the energy sector has one applicable regulation and eight applicable mandatory standards.

Eight sectors did not identify requirements that pertain to securing privately owned IT systems and data. These are critical manufacturing, defense industrial base, emergency services, government facilities, information technology, national monuments and icons, postal and shipping, and telecommunications.

With regard to enforcement, each of the 34 requirements has at least one enforcement mechanism. These mechanisms include court injunctions, civil monetary penalties, criminal penalties, and administrative measures. Typically, these mechanisms are what agencies use to enforce requirements in general, and are not necessarily specific to the requirements for securing privately owned IT systems and data.

In commenting on a draft of the briefing, the sector-specific agencies agreed with the information and provided technical comments, which we have incorporated into the briefing, as appropriate.

Background

Critical infrastructure protection involves activities that enhance the cyber and physical security of the public and private infrastructures that are critical to national security, economic security, and public health and safety.

Because a large percentage of the nation's critical infrastructures is owned and operated by the private sector, public/private partnerships are crucial for successful critical infrastructure protection.

Federal law and policies establish critical infrastructure protection as a national goal and describe a strategy for cooperative efforts by government and private entities to protect the physical and cyber-based systems that are essential to the minimum operations of the economy and the government. These include Homeland Security Presidential Directive 7 and the *National Infrastructure Protection Plan*.

Homeland Security Presidential Directive 7

- established the Department of Homeland Security (DHS) as the principal federal agency to lead, integrate, and coordinate the implementation of efforts to protect critical infrastructures and key resources; and
- identified lead federal agencies, referred to as sector-specific agencies (including, but not limited to, DHS, the Department of the Treasury, and the Department of Health and Human Services), that are responsible for coordinating critical infrastructure protection efforts with the public and private stakeholders in their respective sectors. (See table 1 below for a list of each sector-specific agency and a brief description of each sector.)

Table 1: Critical Infrastructure Sectors and Designated Sector-Specific Agencies

Sector	Description	Sector-specific agency
Agriculture and food	Ensures the safety and security of food, animal feed, and food-producing animals; coordinates animal and plant disease and pest response; and provides nutritional assistance.	Dept. of Agriculture, Dept. of Health and Human Services, Food and Drug Administration
Banking and finance	Provides the financial infrastructure of the nation. This sector consists of commercial banks, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out transactions.	Department of the Treasury
Chemical	Transforms natural raw materials into commonly used products benefiting society's health, safety, and productivity. The chemical sector produces products that are essential to automobiles, pharmaceuticals, food supply, electronics, water treatment, health, construction, and other necessities.	Department of Homeland Security
Commercial facilities	Includes prominent commercial centers, office buildings, sports stadiums, theme parks, and other sites where large numbers of people congregate to pursue business activities, conduct personal commercial transactions, or enjoy recreational pastimes.	Department of Homeland Security
Critical manufacturing	Transforms materials into finished goods. The sector includes the manufacture of primary metals, machinery, electrical equipment, appliances, and components, and transportation equipment.	Department of Homeland Security
Dams	Manages water retention structures, including levees, dams, navigation locks, canals (excluding channels), and similar structures, including larger and nationally symbolic dams that are major components of other critical infrastructures that provide electricity and water.	Department of Homeland Security
Defense industrial base	Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.	Department of Defense
Drinking water and water treatment systems	Provides sources of safe drinking water from community water systems and properly treated wastewater from publicly owned treatment works.	Environmental Protection Agency

Table 1: Critical Infrastructure Sectors and Designated Sector-Specific Agencies, cont.

Sector	Description	Sector-Specific Agency
Emergency services	Saves lives and property from accidents and disaster. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.	Department of Homeland Security
Energy	Provides the electric power used by all sectors and the refining, storage, and distribution of oil and gas. The sector is divided into electricity and oil and natural gas.	Department of Energy
Government facilities	Ensures continuity of functions for facilities owned and leased by the government, including all federal, state, territorial, local, and tribal government facilities located in the U.S. and abroad.	Department of Homeland Security
Information technology	Produces information technology and includes hardware manufacturers, software developers, and service providers, as well as the Internet as a key resource.	Department of Homeland Security
National monuments and icons	Maintains monuments, physical structures, objects, or geographical sites that are widely recognized to represent the nation's heritage, traditions, or values, or widely recognized to represent important national cultural, religious, historical, or political significance.	Department of the Interior
Nuclear reactors, materials, and waste	Provides nuclear power. The sector includes commercial nuclear reactors and non-power nuclear reactors used for research, testing, and training; nuclear materials used in medical, industrial, and academic settings; nuclear fuel fabrication facilities; the decommissioning of reactors; and the transportation, storage, and disposal of nuclear materials and waste.	Department of Homeland Security
Postal and shipping	Delivers private and commercial letters, packages, and bulk assets. The U.S. Postal Service and other carriers provide the services of this sector.	Department of Homeland Security
Public health and healthcare	Mitigates the risk of disasters and attacks and also provides recovery assistance if an attack occurs. The sector consists of health departments, clinics, and hospitals.	Department of Health and Human Services
Telecommunications	Provides wired, wireless, and satellite communications to meet the needs of businesses and governments.	Department of Homeland Security
Transportation systems	Enables movement of people and assets that are vital to our economy, mobility, and security with the use of aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.	Department of Homeland Security

Source: GAO, *Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics,* GAO-07-39 (Washington, D.C.: Oct. 16, 2006).

The *National Infrastructure Protection Plan*

- is a base plan that serves as a road map for how DHS and other relevant stakeholders should use risk management principles to prioritize protection activities within and across the sectors in an integrated, coordinated fashion; and
- requires each of the lead federal agencies associated with the 18 critical infrastructure sectors to develop plans to address how the sectors' stakeholders would implement the national plan and how they would improve the security of their assets and functions. These plans are to, among other things, describe how the sector will identify and prioritize its critical assets, including cyber assets, and define approaches the sector will take to assess risks and develop programs to protect these assets.

In October 2007, we reported that each critical infrastructure sector, to a varying degree, addressed key aspects of cyber security in its respective sector-specific plan.[2] As a whole, the plans addressed certain key aspects more comprehensively than they did others. To assist the sectors in securing their cyber infrastructure, we recommended that the Secretary of Homeland Security request that, by September 2008, the sector-specific agencies develop plans that address all of the key aspects.

[2] GAO, *Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies*, GAO-08-111 (Washington, D.C.: Oct. 31, 2007).

We identified at least 34 applicable federal requirements for securing privately owned IT systems and data, consisting of 1 law, 25 regulations, and 8 mandatory standards that pertain to 10 critical infrastructure sectors.[3,4] Specifically, these requirements and the sectors they apply in are as follows:

- The one law applies in the drinking water and water treatment systems sector.
- The 25 regulations apply in 8 sectors:
  - agriculture and food;
  - banking and finance;
  - chemical;
  - commercial;
  - energy;

[3] We did not include the authorizing laws for the regulations and mandatory standards unless the law specifically references cyber security.

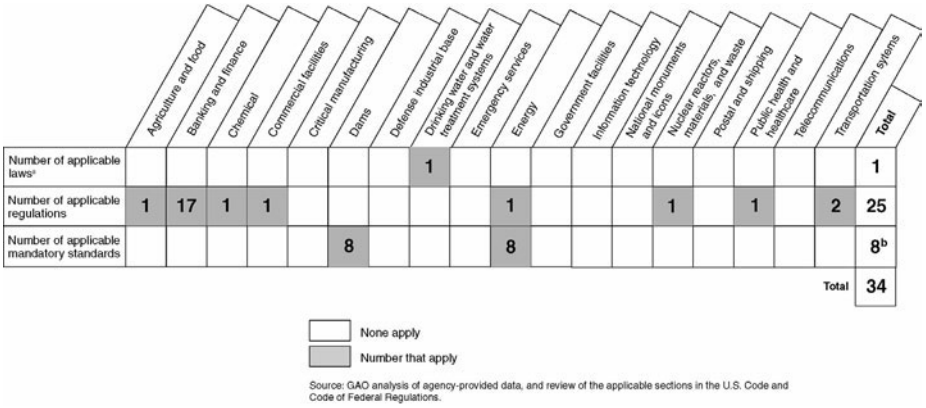
[4] These requirements do not necessarily pertain to critical infrastructure IT systems and data. Further, these requirements do not necessarily apply to all of a sector's entities, require all of an entity's IT systems and data to be secure, or provide for comprehensive coverage of the polices and procedures necessary to ensure adequate security. Lastly, in the absence of a law, regulation, or mandatory standard in a particular sector there may be other mechanisms or motives for protecting privately owned IT systems and data

- nuclear reactors, materials, and waste;
- public health and healthcare; and
- transportation systems.

- The mandatory standards apply in the dams and energy sectors.

Figure 2 summarizes, by critical infrastructure sector, the federal law, regulations, and mandatory standards that have been identified by the agency officials responsible for overseeing each sector as including requirements for private entities to secure their IT systems and data.

Figure 2: Summary of Federal Legal Requirements for Securing Privately Owned IT Systems and Data within Critical Infrastructure Sectors



[a]The number of applicable laws does not include the authorizing laws for the regulations and mandatory standards.
[b]The dams and energy sectors share a common set of 8 mandatory standards that are applicable to both sectors, but these standards are counted only once in this total.

Consequently, while 10 sectors have these requirements, 8 do not; those sectors are

- critical manufacturing,
- defense industrial base,
- emergency services,
- government facilities,
- information technology,
- national monuments and icons,
- postal and shipping, and
- telecommunications.

Results: Objective 1

Federal Legal Requirements within Critical Infrastructure Sectors for Securing IT Systems and Data

The following slides briefly summarize the applicable law, regulations, and mandatory standards, and the sectors in which they apply. (A more detailed description by sector, including authorizing laws, regulatory citations, regulatory agencies, regulated entities, and the statutory and regulatory requirements, is provided in attachment 2.)

Applicable law and corresponding sector

There is one law applicable to the drinking water and water treatment systems sector that pertains to securing the sector's privately owned IT systems and data. The law is the Public Health Security and Bioterrorism Preparedness and Response Act of 2002,[5] which required each community water system serving more than 3,300 people to conduct an assessment of its vulnerability to an intentional act meant to substantially disrupt its ability to provide a safe and reliable supply of drinking water.[6] The vulnerability assessments were to include, but were not limited to, a review of electronic, computer, or other automated systems that are utilized by the public water system. The act also requires each community to prepare and/or revise and maintain an emergency response plan.

[5] Section 401 of Title IV of the Public Health Security and Bioterrorism Preparedness and Response Act amends The Safe Drinking Water Act, which is title XIV of the Public Health Service Act.

[6] These assessments were to be completed and certified to the Environmental Protection Agency administrator prior to March 31, 2003, in the case of systems serving a population of 100,000 or more; December 31, 2003, in the case of systems serving a population of 50,000 or more but less than 100,000; or June 30, 2004, in the case of systems serving a population greater than 3,300 but less than 50,000.

Applicable regulations and corresponding eight sectors

There are 25 regulations, and they apply in 8 sectors as follows:

- 1 in agriculture and food;
- 17 in banking and finance;
- 1 in chemical;
- 1 in commercial facilities;
- 1 in energy;
- 1 in nuclear reactors, materials, and waste;
- 1 in public health and healthcare; and
- 2 in transportation systems.

One regulation applies in the agriculture and food sector:

- It specifies the security requirements that electronic records and signatures must meet to qualify as equivalent to paper records and signatures, and requires implementation of controls to ensure the authenticity, integrity, confidentiality, and nonrepudiation of electronic records.

Seventeen regulations apply in the banking and finance sector. Examples of requirements in these regulations include the following:

- Eight regulations establish standards for developing and implementing administrative, technical, and physical safeguards to protect customer information. They require regulated financial institutions to, among other things, have a written information security program designed to (1) ensure the security and confidentiality of customer records and information, (2) protect against any anticipated threats or hazards to the security or integrity of such information, and (3) protect against unauthorized access to or use of the information that would result in substantial harm or inconvenience to any customer. These regulations differ in which entities they apply to, and which agency has regulatory authority.
- One regulation requires the identification, assessment, and mitigation of IT security risks.

Results: Objective 1
Regulations

One regulation applies in the chemical sector:

- It defines risk-based performance standards that chemical facilities must comply with if they have been determined to present a high risk. Each covered facility must select, develop in their site security plan, and implement risk-based measures designed to deter cyber sabotage, including preventing unauthorized onsite or remote access to critical process controls.

One regulation applies in the commercial sector:

- It establishes IT internal control standards for gaming operations on Indian land, including ensuring that physical and logical security measures are implemented and adhered to by personnel.

One regulation applies in the energy sector:

- This regulation requires any organization that has an outstanding loan made or guaranteed by the Department of Agriculture's Rural Utilities Service for the purpose of rural electrification, or that is seeking such financing, to perform a system security vulnerability and risk assessment, establish and maintain an Emergency Restoration Plan, and maintain records of the physical, cyber, and electrical condition and security of its electric system.

One regulation applies in the nuclear reactors, materials, and waste sector:

- It requires Nuclear Regulatory Commission licensees to design safeguards to defend against cyber attacks that could cause radiological sabotage. In addition, the commission issued orders that established requirements to meet this regulation, including requiring the development of a cyber security program at each nuclear plant.[7]

[7] Commission officials stated that another regulation is being developed that they anticipate will include requirements for establishing a cyber security program, performing cyber security assessments, establishing incident response and recovery operations, and implementing a cyber security and awareness training program.

Results: Objective 1
Regulations

One regulation applies in the public health and healthcare sector:

- It requires the implementation of physical and technical safeguards to help protect and control access to electronic protected health information.

Two regulations apply in the transportation systems sector:

- The first requires covered persons[8] to protect information designated by the Department of Homeland Security's Transportation Security Administration as "Sensitive Security Information" from unauthorized disclosure.
- The second requires control systems, including computer-based control systems, of liquefied natural gas facilities to be surrounded by protective enclosures.

[8] Covered persons include, for example, those employed by, contracted to, or acting for DHS or the Department of Transportation, owners and operators of maritime facilities, and airport and aircraft operators.

Applicable mandatory standards and corresponding two sectors

Dams and energy sector entities are affected by the same eight mandatory standards that establish requirements intended to ensure the security of the electronic exchange of information used to support the reliability of the bulk power system. The requirements include

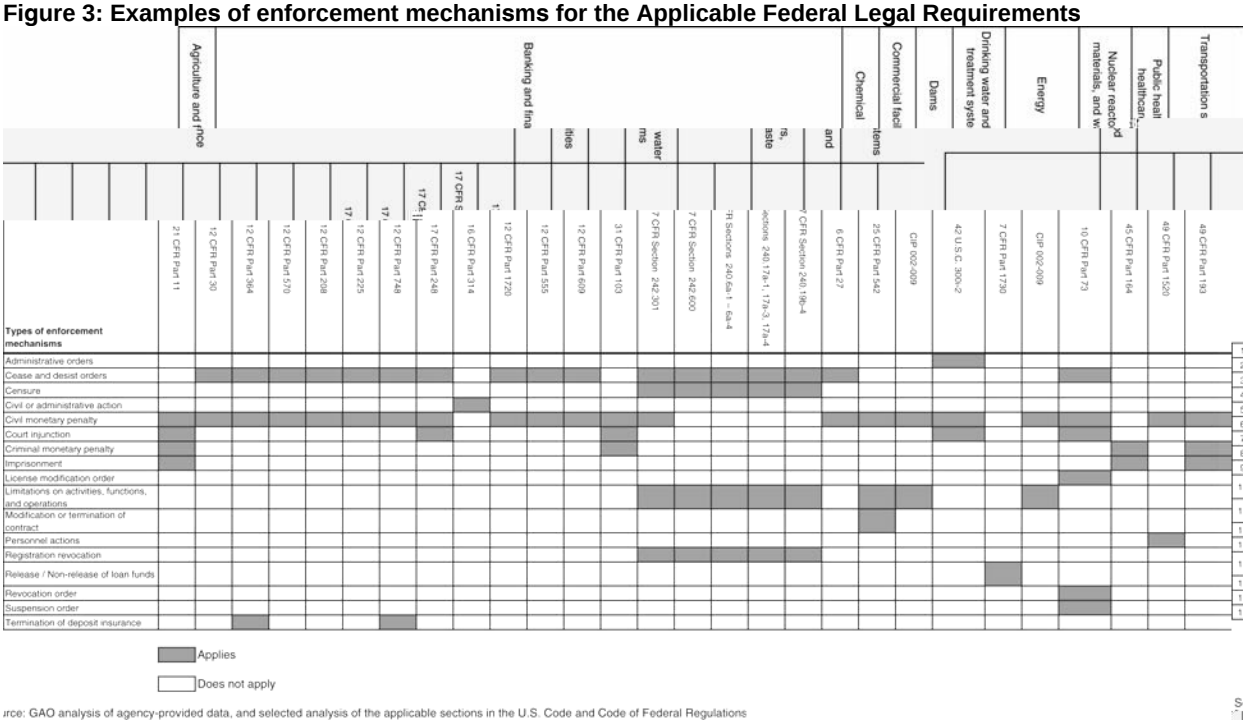
- establishing policies, plans, and procedures to safeguard physical and electronic access to control systems;
- training personnel on security matters;
- reporting security incidents; and
- preparing to recover from cyber incidents.

Results: Objective 2

Federal Legal Requirements' Enforcement Mechanisms

As shown in figure 3 below, there are multiple types of enforcement mechanisms for the 34 federal requirements applying in the corresponding 10 sectors. These types include court injunctions, civil monetary penalties, criminal penalties, and administrative measures. These mechanisms are typically those that an agency uses to enforce regulations in general, and are not necessarily specific to the requirements for securing privately owned IT systems and data.

Figure 3: Examples of enforcement mechanisms for the Applicable Federal Legal Requirements



ırce: GAO analysis of agency-provided data, and selected analysis of the applicable sections in the U.S. Code and Code of Federal Regulations

Results: Objective 2

Federal Legal Requirements' Enforcement Mechanisms

The following slides briefly describe, by the pertinent 10 critical infrastructure sectors, examples of enforcement mechanisms that federal agency officials responsible for overseeing each sector have identified as the means for enforcing the 34 applicable federal requirements.

Agriculture and food: The enforcement mechanisms for the sector's one applicable regulation are the Food and Drug Administration's general statutory enforcement mechanisms, including

- court injunction,
- civil monetary penalty,
- criminal monetary penalty, and
- imprisonment.

For example, the statutory Enforcement authority that would be used in enforcing the agriculture and food sector's regulation provides for a penalty of imprisonment for up to one year, a fine of up to $1,000, or both.

Results: Objective 2
Enforcement Mechanisms

Banking and finance: The enforcement mechanisms for the sector's 17 applicable regulations include

- cease and desist orders;
- civil monetary penalty;
- criminal monetary penalty;
- limitations on activities, functions, and operations;
- registration revocation; and
- termination of deposit insurance.

For example, the enforcement mechanisms for several of the sector regulations provide the potential for a civil monetary penalty against an enterprise of up to $1 million per day that the enterprise is in violation, if it is found that the violation or conduct was done knowingly and caused, or would be likely to cause, a substantial loss to the enterprise.

Results: Objective 2
Enforcement Mechanisms

Chemical: The enforcement mechanisms for the sector's one applicable regulation include

- civil monetary penalty and
- cease and desist order.

For example, a chemical facility can be fined up to $25,000 per day that it is in violation of the regulatory requirements.

Commercial facilities: The enforcement mechanisms for the sector's one applicable regulation include

- civil monetary penalty;
- limitations on activities, functions, and operations; and
- modification or termination of contract.

For example, for any violation, the tribal operator of an Indian game or a management contractor engaged in gaming can be fined up to $25,000 per violation.

Results: Objective 2
Enforcement Mechanisms

Dams: The enforcement mechanisms for the sector's eight applicable mandatory standards include

- civil monetary penalty and
- limitations on activities, functions, and operations.

For example, each mandatory standard authorizes the North American Electric Reliability Corporation to place limitations on the activities, functions, and operations of a regulated entity that violates the standards by, for example, failing to perform a cyber vulnerability assessment at least annually.

Results: Objective 2
Enforcement Mechanisms

Drinking water and water treatment systems: The enforcement mechanisms for the sector's law include

- administrative orders,
- civil monetary penalty, and
- court injunction.

For example, a community water system that did not conduct a system vulnerability assessment could be fined up to $25,000 per violation.

Results: Objective 2
Enforcement Mechanisms

Energy: The enforcement mechanisms for the sector's one applicable regulation include the release/non-release of loan funds, and for the eight applicable mandatory standards include

- civil monetary penalty and
- limitations on activities, functions, and operations.

For example, a borrower of loans from the Department of Energy's Rural Utility Service may not receive loans if found in violation of the regulation.

Results: Objective 2
Enforcement Mechanisms

Nuclear reactors, materials, and waste: The enforcement mechanisms for the sector's one applicable regulation include

- court injunction,
- civil monetary penalty,
- cease and desist order,
- license modification order,
- suspension order, and
- revocation order.

For example, an entity that violates the regulation could be fined up to $100,000 per day per violation.

Results: Objective 2
Enforcement Mechanisms

Public health and healthcare: The enforcement mechanisms for the sector's one applicable regulation include

- criminal monetary penalty and
- imprisonment.

For example, a person who knowingly discloses individually identifiable health information, which is a violation of the underlying statute, may be fined up to $50,000, imprisoned for up to 1 year, or both.

Results: Objective 2
Enforcement Mechanisms

Transportation systems: The enforcement mechanisms for the sector's two applicable regulations include

- civil monetary penalty,
- criminal monetary penalty,
- imprisonment, and
- personnel actions.

For example, if person violates one of the regulations, the person can be fined up to $100,000 for each violation.

Agency Comments

In commenting on a draft of the briefing, the sector-specific agencies agreed with the information and provided technical comments, which we have incorporated into the briefing, as appropriate.

Our objectives were to

1. identify, for each critical infrastructure sector, the federal laws, regulations, and mandatory standards that pertain to securing that sector's privately owned information technology systems and data, and
2. identify enforcement mechanisms for each of the above laws, regulations, and mandatory standards.

To accomplish the first objective, we solicited information from the federal agencies responsible for overseeing each sector to identify the applicable requirements.

A law, regulation, or mandatory standard pertains to securing a private entity's information technology systems and data if it imposes a physical, administrative, or technical safeguard whose implementation would protect the security, confidentiality, or integrity of data or an IT system, or requires private entities to take certain security measures, such as conducting vulnerability or risk assessments, to identify security weaknesses in their IT systems. We did not include privately owned IT systems and data that are operated on behalf of an agency. In particular, our review did not include systems owned by contractors that are operated on behalf of federal agencies subject to governmentwide computer security and privacy requirements, such as the Federal Information Security Management Act of 2002, that require agencies (e.g. the Department of Defense) to ensure that contractors running agency IT systems meet federal information security requirements.

We reviewed, among other things, sections of the United States Code, the Code of Federal Regulations, and federal mandatory standards to confirm the requirements that were applicable for each sector. After reviewing each sector's specific laws, regulations, and mandatory standards, we requested clarification from the regulating agencies when we were unable to validate the applicability of the requirements. Where we could not reconcile our analysis with the agencies' interpretations, we reported the characterizations of the federal agencies since they implement and enforce the requirements.

To accomplish the second objective, federal agency officials responsible for enforcing the requirements identified in the first objective identified mechanisms and authorities available to the agencies and others to enforce compliance with these requirements. The mechanisms and authorities identified are examples of the enforcement mechanisms available to the agencies, and do not necessarily constitute a complete list. We verified the information provided by the agencies by analyzing the applicable sections of the United States Code, Code of Federal Regulations, and other appropriate sources.

We performed our work at federal agencies in the Washington, D.C., metropolitan area from November 2007 to July 2008. We conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings based on our audit objectives.

The following slides describe, by critical infrastructure sector, the federal laws, regulations, and mandatory standards that pertain to securing privately owned IT systems and data in each sector, as identified by the federal agencies responsible for overseeing each sector.

Table 2: Applicable Regulation in the Agriculture and Food Sector

Regulations	Regulator	Regulated entity	Requirements
21 CFR Sections 11.10, 11.30, 11.200, 11.300 (Authorizing laws: 21 U.S.C. 321-393)	Food and Drug Administration (FDA)	FDA-regulated industries, including certain foods, drugs, biologics, medical devices, veterinary products, cosmetics, and radiation-emitting electronic products.	Specifies security requirements that must be implemented in order for electronic records and electronic signatures to qualify as equivalent to paper records and handwritten signatures. The regulated organizations must implement controls to ensure the authenticity, integrity, confidentiality, and non-repudiation of electronic records. Examples of enforcement mechanisms: Civil monetary penalty, court injunction, criminal monetary penalty, imprisonment Enforcement authority: 21 U.S.C. 331, 21 U.S.C. 332, 21 U.S.C. 333

Source: Data provided by the FDA and GAO review of the applicable sections in the U.S. Code and Code of Federal Regulations.

Table 3: Applicable regulations in the Banking and Finance Sector

Regulations	Regulator	Regulated entity	Requirements
12 CFR Part 30 App. B (Authorizing laws: 15 U.S.C. 6801 and 6805(b) 15 U.S.C. 1681m(e) and 1681w 12 U.S.C. 1831p-1)	Office of the Comptroller of Currency	National banks and federal branches of foreign banks and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisors).	Establish standards for developing and implementing administrative, technical, and physical safeguards to protect customer information. Require financial institutions to have a written information security program designed to (1) ensure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such information; (3) protect against unauthorized access to or use of such information that would result in substantial harm or inconvenience to any customer; and (4) ensure the proper disposal of customer and consumer information.[a] Examples of enforcement mechanisms: Civil monetary penalty, cease and desist orders. Administrative actions enforceable via judicial proceedings Enforcement authority: 12 U.S.C. 1818(b), 1818(c), 1818(i); 12 U.S.C. 1831p-1

Table 3: Applicable Regulations in the Banking and Finance Sector, cont.

Regulations	Regulator	Regulated entity	Requirements
12 CFR Part 570 App. B (Authorizing laws: 15 U.S.C. 6801 and 6805(b) 15 U.S.C. 1681m(e) and 1681w 12 U.S.C. 1831p-1)	Office of Thrift Supervision	Savings associations whose deposits are FDIC-insured, their subsidiaries and other entities under OTS supervision (except brokers, dealers, persons providing insurance, investment companies, and investment advisors)	See requirements on slide 47. Examples of enforcement mechanisms: Civil monetary penalty, cease and desist orders Enforcement authority: 12 CFR Sections 570.4 and 570.5, 12 U.S.C. 1464(d), 12 U.S.C.1818(a)(2), 1818(a)(8), 1818(b), 1818(c), 1818(i), 1831p-1

Table 3: Applicable Regulations in the Banking and Finance Sector, cont.

Regulations	Regulator	Regulated entity	Requirements
12 CFR Part 364 App. B (Authorizing laws: 15 U.S.C. 6801 and 6805(b))	Federal Deposit Insurance Corporation	Insured state nonmember banks, insured state licensed branches of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).	See requirements on slide 47. Examples of enforcement mechanisms: Civil monetary penalty, cease and desist orders, termination of deposit insurance Enforcement authority: 12 CFR Section 364 App. A, I, iv; 12 CFR Section 308.305; 12 U.S.C.1818(a)(2), 1818(a)(8), 1818(b), 1818(c), 1818(i), 1831p-1
17 CFR Section 248.30 (Authorizing laws: 15 U.S.C. 6801 and 6805(b) 15 U.S.C. 1681m(e) and 1681w 12 U.S.C. 1831p-1)	Securities and Exchange Commission	Every broker, dealer, and investment company, and every investment adviser registered with the Securities and Exchange Commission.	See requirements on slide 47. Examples of enforcement mechanisms: Civil monetary penalty, cease and desist orders, civil injunctive orders Enforcement authority: 15 U.S.C. 6805; 15 U.S.C. 78o, 78u, 78u-2, and 78u-3; 15 U.S.C. 80a-9 and 80a-41; 15 U.S.C. 80b-3 and 80b-9.

Table 3: Applicable Regulations in the Banking and Finance Sector, cont.

Regulations	Regulator	Regulated entity	Requirements
12 CFR Part 225, App. F (Authorizing laws: 15 U.S.C. 6801 and 6805(b) 15 U.S.C. 1681m(e) and 1681w 12 U.S.C. 1831p-1)	Federal Reserve Board	Bank holding companies, including financial holding companies, and the U.S. operations of foreign banking organizations.	See requirements on slide 47. Examples of enforcement mechanisms: Civil monetary penalty, cease and desist orders Enforcement authority: 12 U.S.C. 1818(b), 1818(c), 1818(i), and 1831p-1

Table 3: Applicable Regulations in the Banking and Finance Sector, cont.

Regulations	Regulator	Regulated entity	Requirements
12 CFR Section 208, App. D-2 (Authorizing laws: 15 U.S.C. 6801 and 6805(b) 15 U.S.C. 1681m(e) and 1681w 12 U.S.C. 1831p-1)	Federal Reserve Board	State chartered banks that are members of the Federal Reserve System. 12 CFR Section 211.24: Offices of foreign banks 12 CFR Section 211.5: Edge Act corporations and agreement corporations. 12 CFR Section 222.83: State member banks, branches and agencies of foreign banks, commercial lending companies owned or controlled by foreign banks, and Edge Act corporations and agreement corporations.	See requirements on slide 47. Examples of enforcement mechanisms: Civil monetary penalty, cease and desist orders Enforcement authority: 12 U.S.C. 1818(b), 1818(c), 1818(i), and 1831p-1

Table 3: Applicable Regulations in the Banking and Finance Sector, cont.

Regulations	Regulator	Regulated entity	Requirements
12 CFR Section 748.0 (Authorizing laws: 15 U.S.C. 6801 and 6805(b) 15 U.S.C. 1681m(e) and 1681w 12 U.S.C. 1751)	National Credit Union Administration	Federally insured credit unions.	See requirements on slide 47. Examples of enforcement mechanisms: Civil monetary penalty, cease and desist orders, termination of deposit insurance Enforcement authority: 12 CFR Section 747.0, 12 U.S.C. 1786
16 CFR Section 314.3, 314.4 (Authorizing laws: 15 U.S.C. 6801 and 6805(b))	Federal Trade Commission	All financial institutions over which the Federal Trade Commission has jurisdiction under the Gramm-Leach-Bliley Act.	Require financial institutions to develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards that are appropriate to the size and complexity of the entity, the nature and scope of its activities, and the sensitivity of any customer information these institutions handle. In addition, financial institutions are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information that they handle. Examples of enforcement mechanisms: Civil and administrative action. A wide range of remedies is available in either form; for example, courts may order restitution and disgorgement. Enforcement authority: 15 U.S.C. 45, 53(b), 6805(b)

Table 3: Applicable Regulations in the Banking and Finance Sector, cont.

Regulations	Regulator	Regulated entity	Requirements
12 CFR Section 555.210 (Authorizing laws: 12 U.S.C. 1462a, 1463(a)(c) 1464(d), 1467(g))	Office of Thrift Supervision	Federal savings associations providing products and services through electronic means.	Sets forth requirements for Federal savings associations that provide products and services through electronic means. Requires these financial institutions to identify, assess, and mitigate risks, and prevent unauthorized access to information. Examples of enforcement mechanisms: Civil monetary penalty, cease and desist order Enforcement authority: 12 U.S.C. 1818(b), 1818(j), 12 U.S.C. 1464(d), 12 U.S.C. 1831p-1
12 CFR Section 1720, App. C (Authorizing law: 12 U.S.C. 4501 et seq)	Office of Federal Housing Enterprise Oversight	Federal National Mortgage Association and the Federal Home Loan Mortgage Corporation, otherwise respectively known as Fannie Mae and Freddie Mac.	Contain policy guidance that establishes standards for Fannie Mae and Freddie Mac concerning administrative, technical, and physical safeguards to ensure the security, confidentiality, and integrity of information. Examples of enforcement mechanisms: Civil monetary penalty, cease and desist proceedings Enforcement authority: 12 U.S.C. 4631(c) and (d), 12 U.S.C. 4636

Table 3: Applicable Regulations in the Banking and Finance Sector, cont.

Regulations	Regulator	Regulated entity	Requirements
31 CFR Sections 103.100, 103.110 (Authorizing law: 31 U.S.C. 5311 Note)	Department of the Treasury	31 CFR Section 103.100: Financial institutions described in 31 U.S.C. 5312(a)(2). 31 CFR Section 103.110: Financial institutions described in 31 U.S.C. 5312(a)(2) that are required to establish and maintain an anti-money-laundering program, or are treated as having satisfied the requirements of 31 U.S.C. 5318(h)(1).	Require each financial institution to maintain adequate procedures, as established in 15 U.S.C. 6801 and applicable regulations issued thereunder, to protect the security and confidentiality of requests from the Financial Crimes Enforcement Network for information under this section regarding terrorist activity or money laundering. Examples of enforcement mechanisms: Civil monetary penalty, criminal monetary penalty, court injunction Enforcement authority: 31 U.S.C. 5320, 5321, 5322
17 CFR Section 242.301(b)(6) (Authorizing laws: 15 U.S.C. 78c, 78e, 78f, 78k-1, 78o, 78q(a), 78q(b), 78s(b), 78w(a), and 78mm.)	Securities and Exchange Commission	Alternative trading systems that meet or exceed 20 percent of nationwide securities trading volume under Section 301(b)(6) of 17 CFR Section 242.300 et seq.	Requires alternative trading systems that meet or exceed 20 percent of nationwide securities trading volume to meet standards regarding capacity, security, and resiliency under the Automation Review Program. Examples of enforcement mechanisms: Civil monetary penalty, revocation of registration, censure, suspension or limitation of activities, cease-and-desist orders Enforcement authority: 15 U.S.C. 78s(h), 15 U.S.C. 78u-3.

Table 3: Applicable Regulations in the Banking and Finance Sector, cont.

Regulations	Regulator	Regulated entity	Requirements
17 CFR Sections 242.600 et seq. (Authorizing law: 15 U.S.C 78k-1)	Securities and Exchange Commission	Exchanges, clearing agencies, and broker-dealers.	Authorizes the Commission to maintain fair and orderly markets and adopt rules to establish a national market system. Pursuant to Section 11A, the Commission adopted the Automation Review Policies, which establish a voluntary framework for the national securities exchanges and national securities associations to establish comprehensive planning and assessment programs to determine systems capacity and vulnerability. (For additional information see table note 'b' on slide 58.) Examples of enforcement mechanisms: Revocation or suspension of registration; censure; limitation of activities, functions, and operations; cease and desist orders Enforcement authority: 15 U.S.C 78s(h), 17 CFR Section 240.19h-1, 15 U.S.C. 78u(C).

Table 3: Applicable Regulations in the Banking and Finance Sector, cont.

Regulations	Regulator	Regulated entity	Requirements
17 CFR Sections 240.6a-1–6a-4 (Authorizing law: 15 U.S.C 78f)	Securities and Exchange Commission	National securities exchanges	Require exchanges to be so organized, and have the capacity to be able to carry out the purposes of the Exchange Act, and require exchanges to file reports with the Commission. Securities Exchange Commission officials stated that this includes requiring exchanges to maintain adequately secure IT systems to meet the Exchange Act requirements, and to maintain security of IT systems to ensure the accuracy of the reports filed with the Commission. Examples of enforcement mechanisms: Revocation or suspension of registration; censure; limitation of activities, functions, and operations; cease and desist orders Enforcement authority: 15 U.S.C 78s(h), 17 CFR 240.19h-1, 15 U.S.C. 78u(c)

Table 3: Applicable Regulations in the Banking and Finance Sector, cont.

Regulations	Regulator	Regulated entity	Requirements
17 CFR Section 240.19b-4 (Authorizing law: 15 U.S.C 78s(b))	Securities and Exchange Commission	Exchanges and clearing agencies.	Requires the national securities exchange and national securities associations to file proposed rule changes with the commission. According to Securities and Exchange Commission officials, proposed rule changes filed under Section 19(b) of the Exchange Act and rules thereunder often contain information that relates directly to IT security, such as a description of a new trading system or trading algorithm. This information helps the Commission staff prevent disruptions to the nation's securities markets by identifying potential system vulnerabilities. Examples of enforcement mechanisms: Revocation or suspension of registration; censure; limitation of activities, functions, and operations; cease and desist orders Enforcement authority: 15 U.S.C 78s(h); 17 CFR Section 240.19h-1; 15 U.S.C. 78u(c)

Table 3: Applicable Regulations in the Banking and Finance Sector, cont.

Regulations	Regulator	Regulated entity	Requirements
17 CFR Sections 240.17a-1, 17a-3, 17a-4 (Authorizing law: 15 U.S.C 78q-1)	Securities and Exchange Commission	Every national securities exchange, national securities association, registered clearing agency, and the Municipal Securities Rulemaking Board, and every member of a national securities exchange who transacts a business in securities directly with others than members of a national securities exchange, and every broker or dealer who transacts a business in securities through the medium of any such member.	Establish requirements for all exchanges, clearing agencies, and broker-dealers to make and keep records of all documents, and provide these records to the Securities Exchange Commission during inspections and otherwise. Examples of enforcement mechanisms: Revocation or suspension of registration; censure; limitation of activities, functions, and operations; cease and desist orders Enforcement authority: 15 U.S.C 78s(h); 17 CFR Section 240.19h-1; 15 U.S.C. 78u(c)

Table 3: Applicable Regulations in the Banking and Finance Sector, cont.

Regulations	Regulator	Regulated entity	Requirements
12 CFR Sections 609.930, 609.940, 609.945 (Authorizing law: 12 U.S.C. 2001 et seq.)	Farm Credit Administration	Farm Credit System Institutions, which include a network of cooperatively organized banks and associations that are owned and controlled by their borrowers.	Requires Farm Credit System institutions to adopt e-commerce policies and procedures to ensure the institution's safety and soundness. These policies and procedures must address, when applicable, the security and integrity of System Institution and borrower data, and intrusion detection and management. Requires institutions' internal systems and controls to provide reasonable assurances that System institutions will prevent and detect material deficiencies on a timely basis. Examples of enforcement mechanisms: Civil monetary penalty; cease and desist proceedings, including suspension or removal of directors or officers; and administrative actions enforceable via judicial proceedings Enforcement authority: 12 U.S.C. 2261–2269; 12 CFR Part 622

Source: Data provided by the Board of Governors of the Federal Reserve System, the Department of the Treasury, the Federal Deposit Insurance Corporation, the Federal Trade Commission, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Office of Federal Housing Enterprise Oversight, the Office of Thrift Supervision, the U.S. Securities and Exchange Commission, and the Farm Credit Administration; and GAO review of the applicable sections in the U.S. Code and Code of Federal Regulations.

[a] According to agency officials, the Office of the Comptroller of Currency, the Office of Thrift Supervision, the Federal Deposit Insurance Corporation, and Board of Governors of the Federal Reserve System also may enforce standards set forth in supervisory guidance, such as the Information Security Handbooks issued under the auspices of the Federal Financial Institutions Examination Council, if the failure to comply with the guidance is an unsafe and unsound banking practice.

[b] According to Security Exchange Commission officials, in addition to the previous two regulations, Sections 6(b)(1) and 11A(a)(1) of the Securities Exchange Act of 1934 authorize the Commission to maintain fair and orderly markets and ensure that exchanges are able to carry out the purposes of the Exchange Act. Pursuant to that authority, the Commission's Division of Trading and Markets conducts an inspection program, the Automation Review Program, which focuses on, among other items, the IT security of the organized markets and clearing organizations. Under the Automation Review Program, the Division conducts inspections of the markets and clearing organizations to determine whether those organizations meet ever-evolving industry standards regarding IT security.

Table 4: Applicable Regulation in the Chemical Sector

Regulations	Regulator	Regulated entity	Requirements
6 CFR Sections 27.215, 27.225, 27.230, 27.235, 27.240, 27.245 (Authorizing law: Pub. L. No. 109-295, sec. 550)	Department of Homeland Security (DHS)	Chemical facilities determined by the Assistant Secretary for Infrastructure Protection, DHS, or his designee, to present high levels of security risk, or a facility that the Assistant Secretary has determined is presumptively high risk.	Require every covered facility to satisfy the risk-based performance standards identified in the regulation.[a] Each covered facility must select, develop in its site security plan, and implement, risk-based measures designed to deter cyber sabotage, including preventing unauthorized onsite or remote access to critical process controls, such as supervisory control and data acquisition systems, critical business systems, and other sensitive computerized systems. Examples of enforcement mechanisms: Order assessing civil monetary penalty, order to cease operation[b] Enforcement authority: 6 CFR Section 27.300

Source: Data provided by DHS and GAO review of the applicable sections in the U.S. Code and Code of Federal Regulations.

[a] According to DHS officials, these risk-based performance standards have not been finalized by DHS or submitted to the Office of Management and Budget for approval, and therefore are not yet enforceable.

[b] To ensure compliance, the regulation also allows DHS to review and approve security vulnerability assessments and site security plans. DHS is also authorized to conduct inspections and audits.

Table 5: Applicable Regulation in the Commercial Facilities Sector

Regulations	Regulator	Regulated entity	Requirements
25 CFR Section 542.16 (Authorizing laws: 25 U.S.C. 2702, 2706)	National Indian Gaming Commission, Department of the Interior	Gaming operations on Indian land.	Establishes information technology internal control standards for gaming operations on Indian land. It requires management to take an active role in ensuring that physical and logical security measures are implemented, maintained, and adhered to by personnel, and requires incompatible duties to be adequately segregated and monitored. Examples of enforcement mechanisms: Civil monetary penalty, temporary closure of game, permanent closure, modification or termination of any management contract Enforcement authority: 25 U.S.C. 2713, 25 CFR Section 542.3 [a]

Source: Data provided by DHS and the Federal Deposit Insurance Corporation, and GAO review of the applicable sections in the U.S. Code and Code of Federal Regulations.

[a] The regulation also provides for Certified Public Accountant testing as well as Commission enforcement action (after notice to Tribe and Tribal gaming regulatory authority, and opportunity for corrective action).

Table 6: Applicable Mandatory Standards in the Dams Sector

Mandatory Standards	Regulator	Regulated entity	Requirements
Reliability Standards CIP 002–009 (Authorizing law: 16 U.S.C. 824o)	Federal Energy Regulatory Commission	Reliability coordinators; balancing and interchange authorities; transmission service providers, owners, and operators; generator owners and operators; load serving entities; the North American Electric Reliability Corporation; and regional reliability organizations.	Establishes requirements to help ensure the security of the electronic exchange of information that is needed to support the reliability of the bulk power system, and to help prevent unauthorized physical or electronic access to critical cyber assets, The eight standards require certain users, owners, and operators of the bulk power system to establish policies, plans, and procedures to safeguard physical and electronic access to control systems; identify and protect critical cyber assets; train personnel on security matters; report security incidents; and be prepared to recover from a cyber incident. Examples of enforcement mechanisms: Civil monetary penalty, sanctions, and remedial actions, including limitations on activities, functions, and operations Enforcement authority: 16 U.S.C. 824o and the North American Electric Reliability Corporation Rules of Procedure, Appendix 4B Sanction Guidelines as approved by the Federal Energy Regulatory Commission.

Source: Data provided by DHS and GAO review of the applicable sections in the U.S. Code and Code of Federal Regulations.

Table 7: Applicable Law in the Drinking Water and Water Treatment Systems Sector

Laws	Regulated entity	Requirements
42 U.S.C. 300i-2	Community water systems serving more than 3,300 people.	Required each community water system to conduct an assessment of the vulnerability of its system to a terrorist attack or other intentional acts intended to substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water. The law required these assessments to be submitted to the U.S. Environmental Protection Agency. The vulnerability assessments were to include, but were not limited to, a review of electronic, computer, or other automated systems which are utilized by the public water system. Required each regulated system to prepare or revise an emergency response plan based on the results of their vulnerability assessments. Each regulated system had to certify in writing to the Environmental Protection Agency that its emergency response plan was completed.[a] Examples of enforcement mechanisms: Civil monetary penalty, administrative orders, court injunction Enforcement authority: 42 U.S.C. 300g-3

Source: Data provided by the Environmental Protection Agency and GAO review of the applicable sections in the U.S. Code and Code of Federal Regulations.

[a] These assessments were to be completed by March 31, 2003, in the case of systems serving a population of 100,000 or more; December 31, 2003, in the case of systems serving a population of 50,000 or more but less than 100,000; or June 30, 2004, in the case of systems serving a population greater than 3,300 but less than 50,000.

Table 8: Applicable Regulations in the Energy Sector

Regulations	Regulator	Regulated entity	Requirements
7 CFR Sections 1730.20, 1730.21, 1730.22, 1730.27, 1730.28 (Authorizing laws: 42 U.S.C. 5195c(e) 7 U.S.C. 901 et seq., 1921 et seq., 6941 et seq.)	U.S. Department of Agriculture's Rural Utilities Service	All electric borrowers,[a] including both distribution borrowers and power supply borrowers.	Requires each electric borrower to perform a system security vulnerability and risk assessment; establish and maintain an Emergency Restoration Plan; and maintain records of the physical, cyber, and electrical condition and security of its electric system. Examples of enforcement mechanisms: Release/non-release of loan funds pending verification of an Emergency Restoration Plan Enforcement authority: 7 CFR Sections 1730.2, 1730.20, 1730.21, 1730.22, 1730.25, 1730.26

Source: Data provided by the Department of Agriculture; and GAO review of the applicable sections in the U.S. Code and Code of Federal Regulations.

[a] A borrower is any organization that has an outstanding loan made or guaranteed by the Rural Utilities Service for rural electrification, or that is seeking such financing.

Table 9: Applicable Mandatory Standards in the Energy Sector

Mandatory Standards	Regulator	Regulated entity	Requirements
Reliability Standards CIP 002–009 (Authorizing law: 16 U.S.C. 824o)	Federal Energy Regulatory Commission	Reliability coordinators; balancing and interchange authorities; transmission service providers, owners, and operators; generator owners and operators; load serving entities; the North American Electric Reliability Corporation; and regional reliability organizations.	These requirements are the same for the standards detailed in the dams sector, which is on slide 62. Examples of enforcement mechanisms: Civil monetary penalty, sanctions, and remedial actions, including limitations on activities, functions, and operations Enforcement authority: 16 U.S.C. 824o and the North American Electric Reliability Corporation Rules of Procedure, Appendix 4B Sanction Guidelines as approved by the Federal Energy Regulatory Commission.

Source: Data provided by the Department of Energy, DHS, and the Department of Agriculture; and GAO review of the applicable sections in the U.S. Code and Code of Federal Regulations.

Table 10: Applicable Regulation in the Nuclear Reactors, Materials, and Waste Sector

Regulations	Regulator	Regulated entity	Requirements
10 CFR Section 73.1 (Authorizing laws: 42 U.S.C 10155, 10161)	Nuclear Regulatory Commission	Entities authorized to conduct activities under a license issued by the Nuclear Regulatory Commission.	Requires licensees to design safeguards to defend against specified threats, including cyber attacks, that could cause radiological sabotage, and to prevent the theft or diversion of formula quantities of special nuclear material. Subsequent Nuclear Regulatory Commission orders revised the specified threats; added additional requirements, including requiring nuclear power plants to identify digital systems that are critical to the operation of the facility and to identify potential consequences to the facility if these systems are affected; and established requirements for the development of a cyber security program at each nuclear plant.[a] Examples of enforcement mechanisms: Civil monetary penalty, injunction or other court order, license modification order, suspension order, revocation order, cease and desist orders Enforcement authority: 10 CFR Section 73.80, 73.81, Atomic Energy Act of 1954, as amended.

Source: Data provided by DHS and GAO review of the applicable sections in the U.S. Code and Code of Federal Regulations.

[a]According to Nuclear Regulatory Commission officials, new regulations that pertain to securing privately owned IT systems and data are in the rulemaking process. If promulgated, they are meant to revise 10 CFR 73.1. The regulations are intended to establish requirements for establishing a cyber security program, including performing a cyber-security assessment, incident response and recovery operations, implementing protective strategies, and implementing a cyber security and awareness training program. The Nuclear Regulatory Commission expects to present the proposed regulations to their Executive Board in September 2008, and the final rulemaking to occur in early 2009.

Table 11: Applicable Regulation in the Public Health and Healthcare Sector

Regulations	Regulator	Regulated entity	Requirements
45 CFR Sections 164.306, 164.310, 164.312, 164.314 (Authorizing Law: 42 U.S.C. 1320d-2)	Department of Health and Human Services	Health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form.	This regulation requires the implementation of physical and technical safeguards to help protect electronic protected health information and control access to it. Examples of enforcement mechanisms: Criminal monetary penalty, imprisonment Enforcement authority: 42 U.S.C. 1320d-5, 1320d-6

Source: Data provided by the Department of Health and Human Services and GAO review of the applicable sections in the U.S. Code and Code of Federal Regulations.

Table 12: Applicable Regulations in the Transportation Systems Sector

Regulations	Regulator	Regulated entity	Requirements
49 CFR Section 1520.9 (Authorizing law: 49 U.S.C. 114(s))	Department of Homeland Security, Transportation Security Administration	All covered persons[a] whom have access to Sensitive Security Information.[b]	Requires covered persons to take reasonable steps to safeguard Sensitive Security Information from unauthorized disclosure. Examples of enforcement mechanisms: Civil monetary penalty, personnel actions Enforcement authority: 49 CFR Section 1520.17
49 CFR Section 193.2905 (Authorizing laws: 49 U.S.C. 60102, 60103)	Department of Transportation	Liquefied natural gas facilities used in the transportation of gas by pipeline.	Requires control systems, including IT control systems, of liquefied natural gas facilities to be surrounded by a protective enclosure. Examples of enforcement mechanisms: Civil monetary penalty, criminal monetary penalty, imprisonment Enforcement authority: 49 U.S.C. 60122, 60123

Source: Data provided by DHS and GAO review of the applicable sections in the U.S. Code and Code of Federal Regulations.

[a]Covered persons include public and private sector employees including those employed by, contracted to, or acting for DHS or the Department of Transportation, owners and operators of maritime facilities, and airport and aircraft operators.

[b]The regulation defines Sensitive Security Information as information obtained or developed in the conduct of security activities, and the disclosure of which the Transportation Security Administration has determined would (1) constitute an unwarranted invasion of privacy, (2) reveal trade secrets or privileged or confidential information, or (3) be detrimental to the security of transportation.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548