United States Government Accountability Office

GAO

Report to Congressional Requesters

September 2007

CRITICAL INFRASTRUCTURE PROTECTION

Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain

This Report is Temporarily Restricted Pending Official Public Release

GAO-07-1036

September 2007

CRITICAL INFRASTRUCTURE PROTECTION

Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-1036, a report to congressional requesters

Why GAO Did This Study

Control systems—computer-based systems that monitor and control sensitive processes and physical functions—perform vital functions in many of our nation's critical infrastructures, including electric power, oil and gas, water treatment, and chemical production. The disruption of control systems could have a significant impact on public health and safety, which makes securing them a national priority. GAO was asked to (1) determine cyber threats, vulnerabilities, and the potential impact of attacks on critical infrastructure control systems; (2) determine the challenges to securing these systems; (3) identify private sector initiatives to strengthen the cybersecurity of control systems; and (4) assess the adequacy of public sector initiatives to strengthen the cybersecurity of control systems. To address these objectives, we met with federal and private sector officials to identify risks, initiatives, and challenges. We also compared agency plans to best practices for securing critical infrastructures.

What GAO Recommends

GAO is making recommendations to the Department of Homeland Security (DHS) to develop a strategy for coordinating control systems security efforts and to enhance information sharing with relevant stakeholders. DHS officials did not agree or disagree with GAO's recommendations, but stated that they would take them under advisement.

www.gao.gov/cgi-bin/getrpt?GAO-07-1036.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Dave Powner at (202) 512-9286 or at pownerd@gao.gov.

What GAO Found

Critical infrastructure control systems face increasing risks due to cyber threats, system vulnerabilities, and the serious potential impact of attacks as demonstrated by reported incidents. Threats can be intentional or unintentional, targeted or nontargeted, and can come from a variety of sources. Control systems are more vulnerable to cyber attacks than in the past for several reasons, including their increased connectivity to other systems and the Internet. Further, as demonstrated by past attacks and incidents involving control systems, the impact on a critical infrastructure could be substantial. For example, in 2003, a computer virus was blamed for shutting down train signaling systems throughout the East Coast and in 2006, a foreign hacker was reported to have planted malicious software capable of affecting a water filtering plant's treatment operations.

Critical infrastructure owners face both technical and organizational challenges to securing control systems. Technical challenges—including control systems' limited processing capabilities, real-time operations, and design constraints—hinder an infrastructure owner's ability to implement traditional information technology security processes, such as strong user authentication and patch management. Organizational challenges include difficulty in developing a compelling business case for investing in control systems security and differing priorities of information security personnel and control systems engineers.

Multiple private sector entities such as trade associations and standards setting organizations are working to help secure control systems. Their efforts include developing standards, providing guidance to members, and hosting workshops on control systems security. For example, the electricity industry has recently developed standards for cybersecurity of control systems and a gas trade association is developing guidance for members to use encryption to secure control systems.

Federal agencies also have multiple initiatives under way to help secure critical infrastructure control systems, but more remains to be done to coordinate these efforts and to address specific shortfalls. Over the past few years, federal agencies—including the Department of Homeland Security, the Department of Energy, and the Federal Energy Regulatory Commission (FERC)—have initiated efforts to improve the security of critical infrastructure control systems. However, there is as yet no overall strategy to coordinate the various activities across federal agencies and the private sector. Further, DHS lacks processes needed to address specific weaknesses in sharing information on control system vulnerabilities. Until public and private sector security efforts are coordinated by an overarching strategy and specific information sharing shortfalls are addressed, there is an increased risk that multiple organizations will conduct duplicative work and miss opportunities to fulfill their critical missions.

Contents

Figures

Abbreviations

CIP	critical infrastructure protection
DHS	Department of Homeland Security
DOE	Department of Energy
FERC	Federal Energy Regulatory Commission
IT	information technology
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
SCADA	supervisory control and data acquisition
US-CERT	United States Computer Emergency Readiness Team

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 10, 2007

Congressional Requesters

Control systems are computer-based systems that are used in many industries to monitor and control sensitive processes and physical functions. Control systems perform vital functions in many of our nation's critical infrastructures, including electric power generation, transmission, and distribution; oil and gas refining and pipelines; water treatment and distribution; chemical production and processing; railroads and mass transit; and manufacturing. Ten years ago, the President's Commission on Critical Infrastructure Protection highlighted the risk of cyber attacks on critical infrastructures, stating that "the widespread and increasing use of supervisory control and data acquisition systems for control of energy systems provides increasing ability to cause serious damage and disruption by cyber means."

In 2003, the *National Strategy to Secure Cyberspace*[1] (often called the cyberspace strategy) stated that the disruption of control systems could have significant consequences for public health and safety, and made securing these systems a national priority. The cyberspace strategy further states that both the private and public sectors have roles in securing control systems. The strategy directs the Department of Homeland Security (DHS), in coordination with the Department of Energy (DOE) and other agencies, to work in partnership with private industry in increasing awareness of the importance of efforts to secure control systems, developing standards, and improving policies with respect to control systems security.

Given the importance of this issue, you asked us to (1) determine cyber threats, vulnerabilities, and the potential impact of attacks on critical infrastructure control systems; (2) determine the challenges to securing critical infrastructure control systems; (3) identify private sector initiatives to strengthen the cybersecurity of control systems; and (4) assess the adequacy of public sector initiatives to strengthen the cybersecurity of control systems.

[1]The White House, *The National Strategy to Secure Cyberspace* (Washington, D.C.: February 2003).

To accomplish these objectives, we assessed documentation of control system security incidents and analyzed research studies and reports, as well as our prior reports and testimonies on control systems, critical infrastructure protection (CIP), and national preparedness, among others. We analyzed reports by, and met with, private sector and federal officials who had expertise in control systems and their security. Our work was performed from March 2007 to July 2007 in accordance with generally accepted government auditing standards. Appendix I contains further details on our objectives, scope, and methodology.

Results in Brief

Critical infrastructure control systems face increasing risks due to cyber threats, system vulnerabilities, and the serious potential impact of attacks as demonstrated by reported incidents. Threats can be intentional or unintentional, targeted or nontargeted, and can come from a variety of sources including foreign governments, criminal groups, and disgruntled organization insiders. Control systems are more vulnerable to cyber attacks than in the past for several reasons, including their increased connectivity to other systems and the Internet. Further, as demonstrated by past attacks and incidents involving control systems, the impact on a critical infrastructure could be substantial. For example, in 2003, a computer virus was blamed for shutting down train signaling systems throughout the East Coast; in 2006, a foreign hacker was reported to have planted malicious software capable of affecting a water filtering plant's water treatment operations; and, also in 2006, excessive traffic on a nuclear power plant's control system network—possibly caused by the failure of another control system device—caused two circulation pumps to fail, forcing the unit to be shut down manually.

Critical infrastructure owners face both technical and organizational challenges to securing control systems. Technical challenges—including control systems' limited processing capabilities, real-time operations, and design constraints—hinder an infrastructure owner's ability to implement traditional information technology (IT) security processes, such as strong user authentication and patch management. Organizational challenges include difficulty in developing a compelling business case for investing in control systems security and differing priorities of information security personnel and control systems engineers.

Multiple private sector entities such as trade associations and standards setting organizations are working to help secure control systems. These organizations include those specific to the electric, chemical, oil and gas, and water sectors. Their efforts include developing standards, providing

guidance to members, and hosting workshops on control systems security. For example, the electricity industry has recently developed standards for cybersecurity of control systems, and a gas trade association is developing guidance for members to use encryption to secure control systems.

Over the past few years, federal agencies—including DHS, DOE, the National Institute of Standards and Technology (NIST), the Federal Energy Regulatory Commission (FERC), and others—have initiated efforts to improve the security of critical infrastructure control systems. However, there is as yet no overall strategy to coordinate the various control systems activities across federal agencies and the private sector. Further, DHS lacks processes needed to address specific weaknesses in sharing information on control system vulnerabilities. Until public and private sector security efforts are coordinated by an overarching strategy, there is an increased risk that multiple organizations will conduct duplicative work and miss opportunities to learn from other organizations' activities. In addition, until information-sharing weaknesses are addressed, DHS risks not being able to effectively carry out its responsibility for sharing information on vulnerabilities with the private and public sectors.

We are making recommendations to the Secretary of the Department of Homeland Security to develop a strategy for coordinating control systems security efforts and to enhance information sharing with control systems stakeholders.

DHS officials, including the Deputy Director of the National Cyber Security Division, provided comments via e-mail on a draft of this report, but did not agree or disagree with our recommendations. Instead, agency officials stated that the agency would take the recommendations under advisement. DHS officials also discussed the agency's plans to develop a comprehensive strategy for control systems security and efforts to develop a process for sharing sensitive information on control system vulnerabilities. In addition, DHS officials and others who contributed information to this report provided technical comments, which we have incorporated in this report as appropriate.

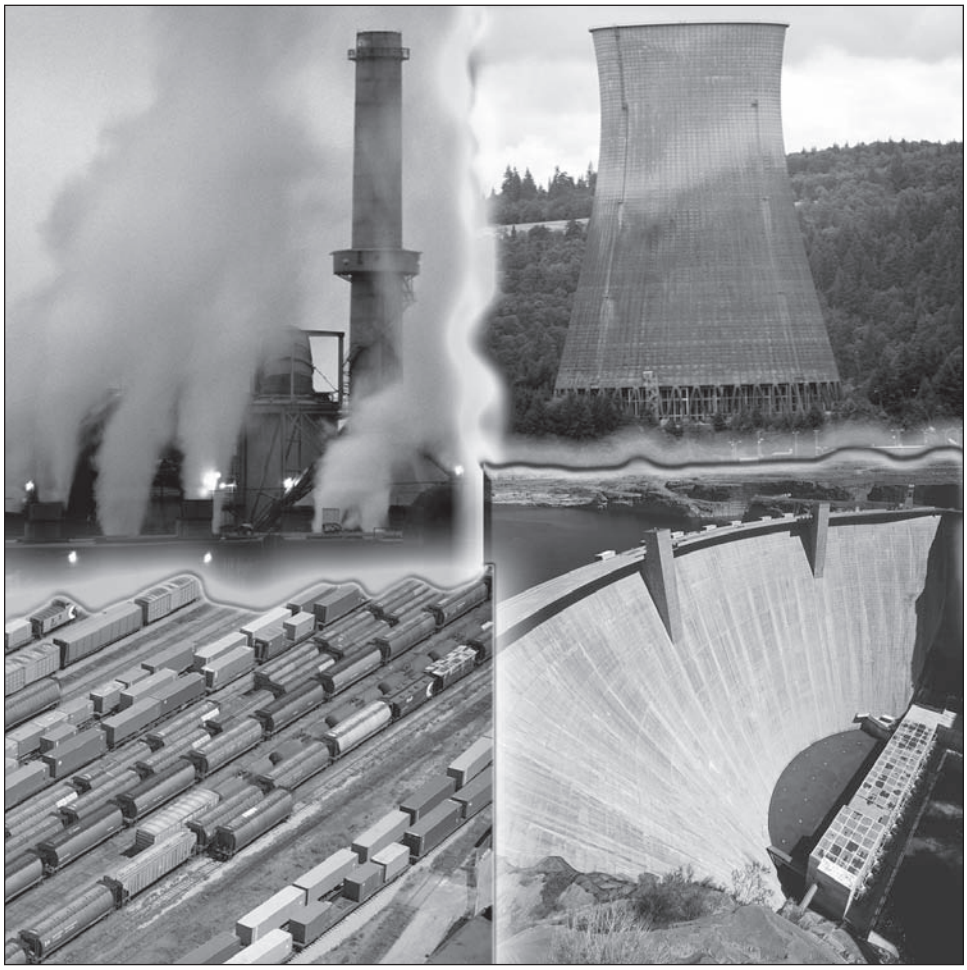
Background

Critical infrastructures are physical or virtual systems and assets so vital to the nation that their incapacitation or destruction would have a debilitating impact on national and economic security, public health, and safety. These systems and assets—such as the electric power grid, chemical plants, and water treatment facilities—are essential to the operations of the economy and the government. Recent terrorist attacks

and threats have underscored the need to protect our nation's critical infrastructures. If vulnerabilities in these infrastructures are exploited, our nation's critical infrastructures could be disrupted or disabled, possibly causing loss of life, physical damage, and economic losses.

Although the vast majority of our nation's critical infrastructures are owned by the private sector, the federal government owns and operates key facilities that use control systems, including oil, gas, water, energy, and nuclear facilities (see fig. 1).

Figure 1: Examples of Critical Infrastructures (clockwise from upper left: chemical plants, nuclear power plants, hydroelectric dams, and railroads)



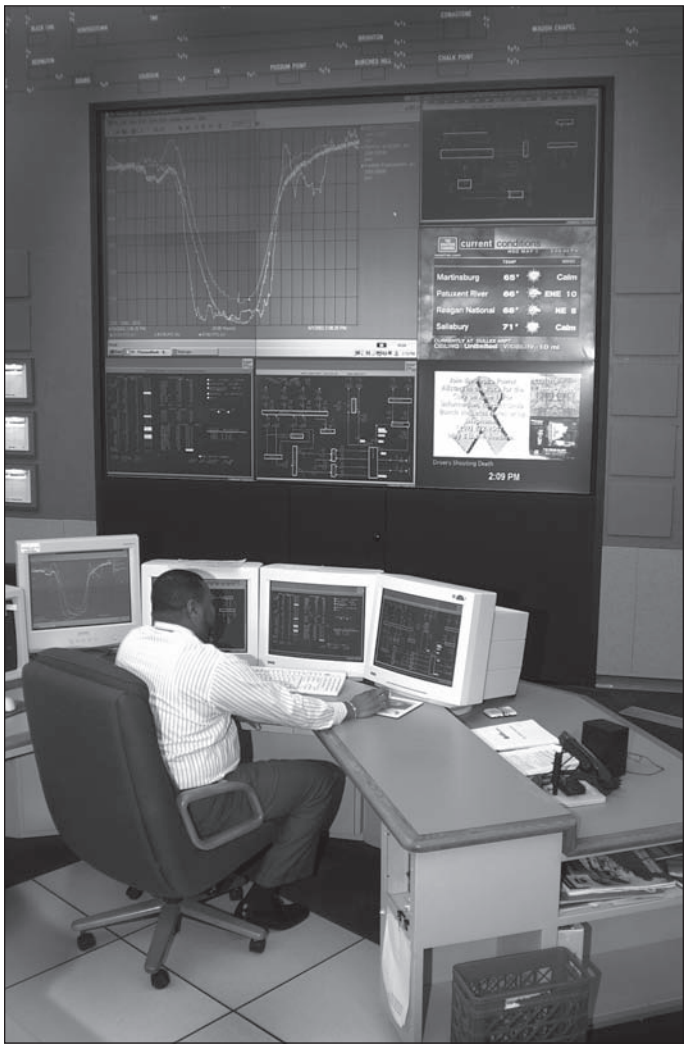
Sources (clockwise from upper left): © Corbis, PhotoDisc, © Corbis, Digital Vision.

Control Systems Are Used in Many Critical Infrastructures

Control systems are computer-based systems that are used within many infrastructures and industries to monitor and control sensitive processes and physical functions. Typically, control systems collect sensor measurements and operational data from the field, process and display this information, and relay control commands to local or remote equipment. Control systems perform functions that range from simple to complex. They can be used to simply monitor processes—for example, the environmental conditions in a small office building—or to manage the complex activities of a municipal water system or a nuclear power plant.

In the electric power industry, control systems can be used to manage and control the generation, transmission, and distribution of electric power (see fig. 2). For example, control systems can open and close circuit breakers and set thresholds for preventive shutdowns. The oil and gas industry uses integrated control systems to manage refining operations at plant sites, remotely monitor the pressure and flow of gas pipelines, and control the flow and pathways of gas transmission. Water utilities can remotely monitor well levels and control the wells' pumps; monitor flows, tank levels, or pressure in storage tanks; monitor water quality characteristics such as pH, turbidity, and chlorine residual; and control the addition of chemicals to the water. Control systems are also used in manufacturing and chemical processing. Chemical reactors may use control systems to produce chemicals or regulate temperatures within the production process.

Figure 2: Control Room of an Electric Power Company



Source: Major electric utility.

Installing and maintaining control systems requires a substantial financial investment. DOE cites research estimating the value of the control systems used to monitor and control the electric grid and the oil and

natural gas infrastructure at $3 billion to $4 billion.[2] The thousands of remote field devices represent an additional investment of $1.5 billion to $2.5 billion. Each year, the energy sector alone spends over $200 million for control systems, networks, equipment, and related components and at least that amount in personnel costs.

Control Systems: Types and Components

There are two primary types of control systems: distributed control systems and supervisory control and data acquisition (SCADA) systems. Distributed control systems typically are used within a single processing or generating plant or over a small geographic area, while SCADA systems typically are used for large, geographically dispersed operations. For example, a utility company may use a distributed control system to manage power generation and a SCADA system to manage its distribution.

A SCADA system is generally composed of six components: instruments, operating equipment, local processors, short-range communication, host computers, and long-range communications.

- **Instruments** sense conditions such as pH, temperature, pressure, power level, and flow rate.
- **Operating equipment** includes pumps, valves, conveyors, and substation breakers that can be controlled by energizing actuators or relays.
- **Local processors** communicate with the site's instruments and operating equipment. Local processors go by several different names, including programmable logic controller, remote terminal unit, intelligent electronic device, and process automation controller. A single local processor may be responsible for dozens of inputs from instruments and outputs to operating equipment. Local processors can collect instrument data; turn on and off operating equipment; translate protocols so different controllers, instruments, and equipment can communicate; and identify alarm conditions.

[2]Newton-Evans Research Company, Inc., *World Market Study of SCADA, Energy Management Systems and Distribution Management Systems in Electrical Utilities: 2005-2007*, (Ellicott City, Maryland: June 2005) as cited in U.S. Department of Energy, *Roadmap to Secure Control Systems in the Energy Sector* (Washington, D.C.: January 2006).

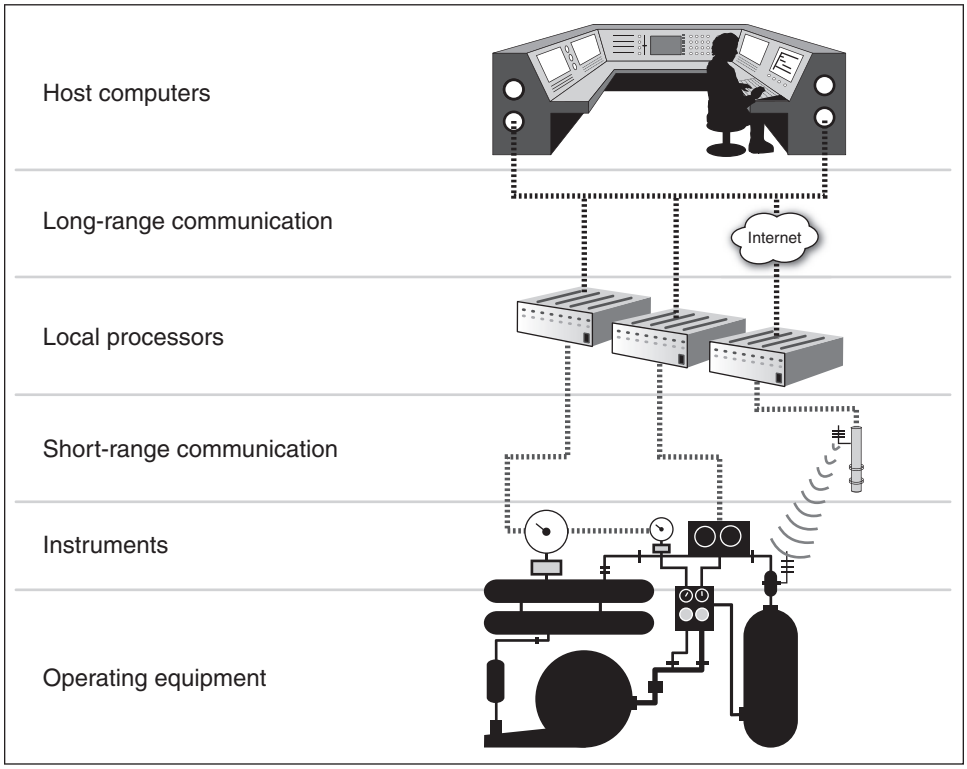
- **Short-range communication** consists of the relatively short cables or wireless connections that carry analog and discrete signals between the local processors and the instruments and operating equipment. The communication uses electrical characteristics such as voltage and current or other established industrial communications protocols.

- **Host computers** are the central point of monitoring and control. The host computer is where a human operator can supervise the process, receive alarms, review data, and exercise control. In some cases the host computer has logic programmed into it to provide control over the local processors. The host computer may be called the master terminal unit, the SCADA server, or a personal computer.

- **Long-range communication** consists of the communication between the local processors and host computers. This communication typically covers miles using methods such as leased phone lines, satellite, microwave, and cellular packet data.

Figure 3 illustrates the major components of a SCADA system and Figure 4 illustrates how these components would be distributed in a typical water utility.

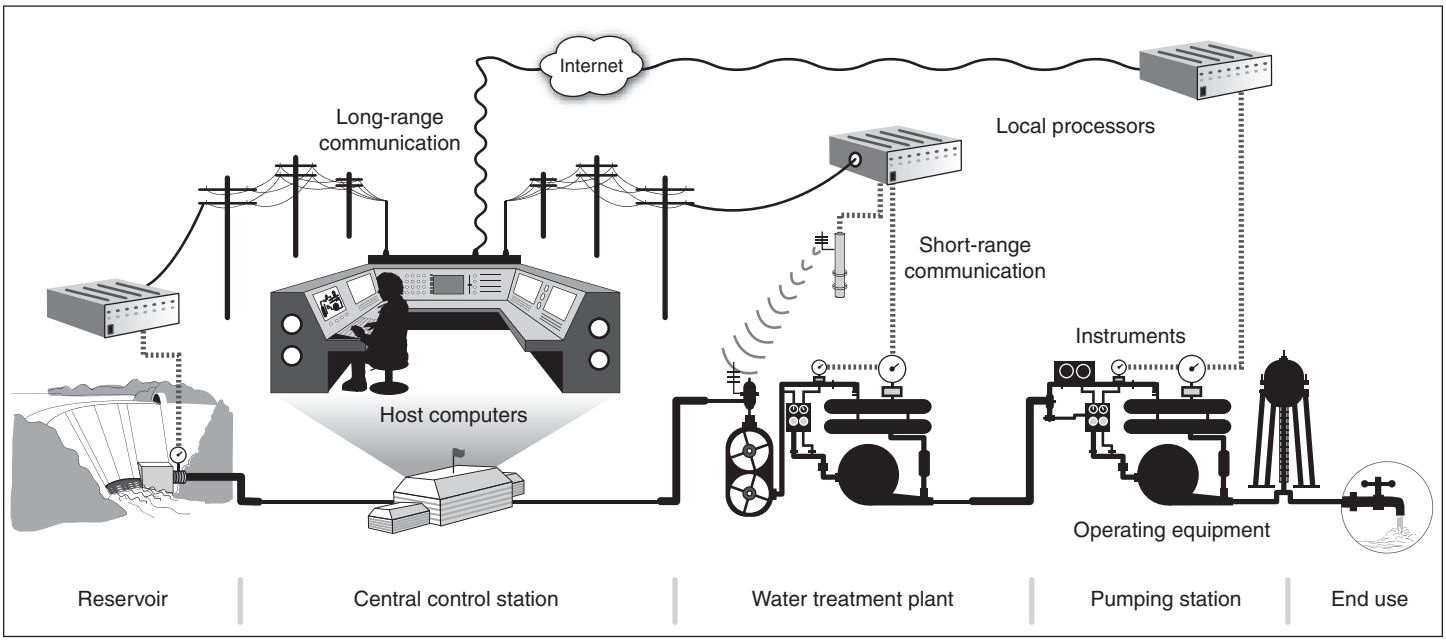
Figure 3: Major Components of a SCADA System



Source: GAO.

These components can be adapted to perform specific functions in many industrial sectors. For example, the following graphic shows the application of these components in a water treatment and distribution system.

Figure 4: Components of a Control System in a Water Treatment and Distribution Facility



Source: GAO.

The Federal Government Plays a Critical Role in Helping Secure Critical Infrastructures and Their Control Systems

Federal law and policies call for critical infrastructure protection activities to enhance the cyber and physical security of both public and private infrastructures that are essential to national security, national economic security, and national public health and safety.[3] Federal policy designates certain federal agencies as lead points of contact for each key critical infrastructure sector (see table 1). Further, it assigns agencies responsibility for infrastructure protection activities in their assigned sectors and for coordination with other relevant federal agencies, state and local governments, and the private sector. In addition, federal policy establishes DHS as the focal point for the security of cyberspace—including analysis, warning, information sharing, vulnerability reduction, mitigation, and recovery efforts for public and private critical

[3]These laws and policies include, for example, the Homeland Security Act of 2002 (Pub. L. No. 107-296, sec. 214 (Nov. 25, 2002)); Homeland Security Presidential Directive 7, the Energy Policy Act of 2005 (Pub. L. No. 109-58, sec. 1211 (Aug. 8, 2005)); and *The National Strategy to Secure Cyberspace*.

infrastructure information systems. To accomplish this mission, DHS is to work with other federal agencies, state and local governments, and the private sector.

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

Sector	Sector-specific agency
Agriculture and food	Department of Agriculture, Department of Health and Human Services, Food and Drug Administration[a]
Banking and finance	Department of the Treasury
Chemical	Department of Homeland Security
Commercial facilities	Department of Homeland Security
Commercial nuclear reactors, materials, and waste	Department of Homeland Security
Dams	Department of Homeland Security
Defense industrial base	Department of Defense
Drinking water and water treatment systems	Environmental Protection Agency
Emergency services	Department of Homeland Security
Energy	Department of Energy
Government facilities	Department of Homeland Security
Information technology	Department of Homeland Security
National monuments and icons	Department of the Interior
Postal and shipping	Department of Homeland Security
Public health and health care	Department of Health and Human Services
Telecommunications	Department of Homeland Security
Transportation systems	Department of Homeland Security

Source: *The National Infrastructure Protection Plan,* Homeland Security Presidential Directive 7, and the *National Strategy for Homeland Security.*

[a]The Department of Agriculture is responsible for food (including meat, poultry, and eggs) and agriculture; and the Department of Health and Human Services, Food and Drug Administration, is responsible for food other than meat, poultry, and egg products.

Several key federal plans focus on securing critical infrastructure control systems. The cyberspace strategy [4] calls for DHS and DOE to work in partnership with industry to develop best practices and new technology to

[4]The White House, *The National Strategy to Secure Cyberspace* (Washington, D.C.: February 2003).

increase the security of critical infrastructure control systems, to determine the most critical control systems-related sites, and to develop a prioritized plan for short-term cybersecurity improvements for those sites. In addition, DHS's *National Infrastructure Protection Plan*[5] specifically identifies control systems as part of the cyber infrastructure, establishes an objective of reducing vulnerabilities and minimizing severity of attacks on these systems, and identifies programs directed at protecting control systems. Further, in May 2007, the critical infrastructure sectors issued sector-specific plans to supplement the *National Infrastructure Protection Plan*. Twelve sectors, including the chemical, energy, water, information technology, postal, emergency services, and telecommunications sectors, identified control systems within their respective sectors. Of these, most identified control systems as critical to their sector and listed efforts under way to help secure them.

Critical Infrastructure Control Systems Face Increasing Risks Due to Cyber Threats, Vulnerabilities, and the Potentially Serious Impact of an Attack

Critical infrastructure control systems face increasing risks due to cyber threats, system vulnerabilities, and the potentially serious impact of an attack as demonstrated by reported incidents. Cyber threats can be unintentional or intentional, targeted or nontargeted, and can come from a foreign, domestic, or inside source. Control systems can have vulnerabilities that make them susceptible to cyber attacks, including the increased connectivity of control systems to other systems and the Internet. Further, based on past events, the impact of a control systems incident on a critical infrastructure could be substantial.

Critical Infrastructures Face Multiple Cyber Threats

Cyber threats can be unintentional and intentional, targeted or nontargeted, and can come from a variety of sources. Unintentional threats can be caused by software upgrades or maintenance procedures that inadvertently disrupt systems. Intentional threats include both targeted and nontargeted attacks. A targeted attack is when a group or individual specifically attacks a critical infrastructure system. A nontargeted attack occurs when the intended target of the attack is

[5]Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, D.C.: June 2006).

uncertain, such as when a virus, worm, or malware[6] is released on the Internet with no specific target.

There is increasing concern among both government officials and industry experts regarding the potential for a cyber attack on a national critical infrastructure, including the infrastructure's control systems. The Federal Bureau of Investigation has identified multiple sources of threats to our nation's critical infrastructures, including foreign nation states engaged in information warfare, domestic criminals and hackers, and disgruntled employees working within an organization. Table 2 summarizes those groups or individuals that are considered to be key sources of threats to our nation's infrastructures.

Table 2: Sources of Cyber Threats to Critical Infrastructures

Threat source	Description
Criminal groups	There is an increased use of cyber intrusions by criminal groups that attack systems for monetary gain.
Foreign nation states	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities. Also, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that, according to the Director of the Central Intelligence Agency, can affect the daily lives of Americans across the country.[a]
Hackers	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, attack tools have become more sophisticated and easier to use.
Hacktivists	Hacktivism refers to politically motivated attacks on publicly accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into Web sites to send a political message.
Disgruntled insiders	The disgruntled insider, working from within an organization, is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes contractor personnel.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. However, traditional terrorist adversaries of the United States are less developed in their computer network capabilities than other adversaries. Terrorists likely pose a limited cyber threat. The Central Intelligence Agency believes terrorists will stay focused on traditional attack methods, but it anticipates growing cyber threats as a more technically competent generation enters the ranks.

[6]"Malware" (malicious software) is defined as programs that are designed to carry out annoying or harmful actions. They often masquerade as useful programs or are embedded into useful programs so that users are induced into activating them.

Threat source	Description
Virus writers	Virus writers are posing an increasingly serious threat. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa macro virus, the Explore.Zip worm, the CIH (Chernobyl) virus, Nimda, and Code Red.

Source: Federal Bureau of Investigation, unless otherwise indicated.

[a]Prepared statement of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence, February 2, 2000.

Control Systems Are Vulnerable to Cyber Attacks

Control systems are vulnerable to flaws or weaknesses in system security procedures, design, implementation, and internal controls. When these weaknesses are accidentally triggered or intentionally exploited, they could result in a security breach. Vulnerabilities could occur in control systems' policies, platform (including hardware, operating systems, and control system applications), or networks.

Federal and industry experts believe that critical infrastructure control systems are more vulnerable today than in the past. Reasons include the increased standardization of technologies, the increased connectivity of control systems to other computer networks and the Internet, insecure connections, and the widespread availability of technical information about control systems. Further, it is not uncommon for control systems to be configured with remote access through either a dial-up modem or over the Internet to allow remote maintenance or around-the-clock monitoring. If control systems are not properly secured, individuals and organizations may eavesdrop on or interfere with these operations from remote locations.

Reported Control Systems Incidents Reveal the Potential for Substantial Impact

Reported attacks and unintentional incidents involving critical infrastructure control systems demonstrate that a serious attack could be devastating. Although there is not a comprehensive source for incident reporting, the following attacks, reported in government and media sources,[7] demonstrate the potential impact of an attack.

- **Worcester air traffic communications**. In March 1997, a teenager in Worcester, Massachusetts, disabled part of the telephone network using a dial-up modem connected to the system. This disabled phone service to the airport control tower, airport security, the airport fire department, the weather service, and the carriers that use the airport. Also, the tower's main radio transmitter and another transmitter that activates runway lights were shut down, as well as a printer that controllers use to monitor flight progress. The attack also disrupted phone service to 600 homes in a nearby town.
- **Maroochy Shire sewage spill**. In the spring of 2000, a former employee of an Australian organization that develops manufacturing software applied for a job with the local government, but was rejected. Over a 2-month period, this individual reportedly used a radio transmitter on as many as 46 occasions to remotely break into the controls of a sewage treatment system. He altered electronic data for particular sewerage pumping stations and caused malfunctions in their operations, ultimately releasing about 264,000 gallons of raw sewage into nearby rivers and parks.
- **Los Angeles traffic lights**. According to several published reports, in August 2006, two Los Angeles city employees hacked into computers controlling the city's traffic lights and disrupted signal lights at four intersections, causing substantial backups and delays. The attacks were launched prior to an anticipated labor protest by the employees.

In addition, the following incidents illustrate the consequences of nontargeted attacks and unintentional incidents on critical infrastructure control systems. According to experts, incidents such as these could also be triggered by a targeted attack.

[7]See National Institute of Standards and Technology, *Special Publication 800-82 Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security: Recommendations of the National Institute of Standards and Technology*, (Gaithersburg, Maryland. September 2006); Los Angeles County District Attorneys Office (da.co.la.ca.us/mr/010507a.htm), *Two City Engineers Charged with Allegedly Hacking Into City's Traffic Computer* (Los Angeles, California: Jan. 5, 2007); and ISA (www.isa.org/content/contentgroups/news/2006/november29/hackers_hit_pennsylvania_water_system.htm), *Hackers Hit Pennsylvania Water System*, (Research Triangle Park, North Carolina: November 2,, 2006).

- **CSX train signaling system**. In August 2003, the Sobig computer virus was blamed for shutting down train signaling systems throughout the East Coast of the United States. The virus infected the computer system at CSX Corporation's Jacksonville, Florida, headquarters, shutting down signaling, dispatching, and other systems. According to an Amtrak spokesman, 10 Amtrak trains were affected. Train service was either shut down or delayed up to 6 hours.
- **Davis-Besse power plant**. The Nuclear Regulatory Commission confirmed that in January 2003, the Microsoft SQL Server worm known as Slammer infected a private computer network at the idled Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly 5 hours. In addition, the plant's process computer failed, and it took about 6 hours for it to become available again.
- **Northeast power blackout**. In August 2003, failure of the alarm processor in the control system of FirstEnergy, an Ohio-based electric utility, prevented control room operators from having adequate situational awareness of critical operational changes to the electrical grid. This problem was compounded when the state estimating program at the Midwest Independent System Operator failed due to incomplete information on the electric grid. When several key transmission lines in northern Ohio tripped due to contact with trees, they initiated a cascading failure of 508 generating units at 265 power plants across eight states and a Canadian province.
- **Zotob worm**. In August 2005, a round of Internet worm infections knocked 13 of DaimlerChrysler's U.S. automobile manufacturing plants offline for almost an hour, leaving workers idle as infected Microsoft Windows systems were patched. Zotob and its variations also caused computer outages at heavy-equipment maker Caterpillar Inc., aircraft maker Boeing, and several large U.S. news organizations.
- **Taum Sauk Water Storage Dam failure**. In December 2005, the Taum Sauk Water Storage Dam, approximately 100 miles south of St. Louis, Missouri, suffered a catastrophic failure, releasing a billion gallons of water. According to the dam's operator, the incident may have occurred because the gauges at the dam read differently than the gauges at the dam's remote monitoring station.
- **Bellingham, Washington, gasoline pipeline failure**. In June 1999, 237,000 gallons of gasoline leaked from a 16-inch pipeline and ignited an hour and a half later, causing three deaths, eight injuries, and extensive property damage. The pipeline failure was exacerbated by poorly performing control systems that limited the ability of the pipeline controllers to see and react to the situation.
- **Harrisburg, Pennsylvania, water system**. In October 2006, a foreign hacker penetrated security at a water filtering plant. The intruder planted malicious software that was capable of affecting the plant's water

treatment operations. The infection occurred through the Internet and did not seem to be an attack that directly targeted the control system.

- **Browns Ferry power plant**. In August 2006, two circulation pumps at Unit 3 of the Browns Ferry, Alabama, nuclear power plant failed, forcing the unit to be shut down manually. The failure of the pumps was traced to excessive traffic on the control system network, possibly caused by the failure of another control system device.

As control systems become increasingly interconnected with other networks and the Internet, and as the system capabilities continue to increase, so do the threats, potential vulnerabilities, types of attacks, and consequences of compromising these critical systems.

Critical Infrastructure Owners Face Technical and Organizational Challenges to Securing Control Systems

Critical infrastructure owners face both technical and organizational challenges in securing their control systems. Technical challenges—including control systems' limited processing capabilities and their real-time operations—hinder infrastructure owners' ability to implement traditional information security technologies and practices. Organizational challenges include the lack of a compelling business case to improve security and a reluctance to share information regarding incidents.

Technical Challenges Hinder Use of Traditional Information Security Measures for Control Systems

According to industry experts, existing information security technologies and practices—such as strong user authentication and patch management—are generally not implemented in control systems due to several technical issues, including limited computational processing capabilities, the need for real-time operation, and the lack of consideration of cybersecurity in the original design of the system. These challenges are described here in more detail.

Limited computational capabilities. Existing security technologies—such as authorization, authentication, encryption, intrusion detection, and filtering of network traffic and communications—require more bandwidth, processing power, and memory than control system components typically have. Controller stations are generally designed to do specific tasks, and they often use low-cost, resource-constrained microprocessors. In addition, passwords and other data from control systems are often

transmitted in a plain, unencrypted format. Encrypting this data could overload the processing abilities of the control system.

Need for real-time operations. Complex passwords and other strong password practices are not always used to prevent unauthorized access to control systems, in part because they could hinder the operator's ability to respond rapidly during an emergency. As a result, according to security experts, weak passwords that are easy to guess, and shared and infrequently changed, are common in control systems. Some even use default passwords or no password at all.

Design limitations. Historically, control systems vendors did not design their products with security in mind, although recently vendors have begun including more security-related features in their products. In addition, although modern control systems are based on standard operating systems, they are typically customized to support control system applications. Consequently, software patches may either be incompatible with the customized version of the operating system or difficult to implement without compromising service by shutting down "always-on" systems or affecting interdependent operations.

Table 3 illustrates the technical challenges in securing control systems by contrasting them with conventional information technology (IT) systems.

Table 3: Comparing IT Systems to Control Systems Illustrates Security Challenges

System characteristic	Information technology system	Control system	Security challenge for control systems
Performance requirements	• Generally not real time. • Response must be consistent. • High throughput is demanded. • Delay may be acceptable.	• Real time. • Response is time critical. • Modest throughput is acceptable. • Delay is a serious concern.	Real-time operations: The security solution should not delay system response time.
Availability requirements	• Responses such as rebooting are acceptable. • Availability deficiencies can often be tolerated, depending on the system's operational requirements.	• Responses such as rebooting may not be acceptable because of process availability requirements. • Outages must be planned and scheduled days/weeks in advance. • High availability requires exhaustive predeployment testing.	Design limitations: The security solution should not require rebooting or cause unplanned outages.

System characteristic	Information technology system	Control system	Security challenge for control systems
Risk management requirements	• Data confidentiality and integrity are paramount. • Fault tolerance is less important –momentary downtime is not a major risk. • Major risk impact is delay of business operations.	• Human safety is paramount, followed by protection of the process. • Fault tolerance is essential: even momentary downtime is not acceptable. • Major risk impact is regulatory noncompliance or loss of life, equipment, or production.	Design limitations: The security solution should not impose unacceptable risk by endangering lives or affecting the process being controlled; the security solution should not cause downtime.
Time-critical interaction	• Less critical emergency interaction. • Tightly restricted access control can be implemented to the degree necessary.	• Response to human and other emergency interaction is critical. • Access to control system should be strictly controlled, yet not hamper human-machine interaction.	Real-time operations: Increased security of stringent access controls must be balanced against the need for fast response times in emergencies.
System operation	• Systems are designed for use with typical operating systems. • Upgrades are straightforward with the availability of automated deployment tools.	• Differing and custom operating systems often do not have security capabilities. • Software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and perhaps modified hardware and software involved.	Design limitation: Additional testing and modification of off-the-shelf products may be required; additional time may be required for vendors to implement upgrades.
Resource constraints	• Systems are specified with enough resources to support the addition of third party applications such as security solutions.	• Systems are designed to support the intended industrial process, with minimal memory and computing resources to support the addition of security technology.	Processing capabilities: It is more difficult to add additional security technology or processes to control systems.
Communications	• Standard communications protocols. • Primarily wired networks with some localized wireless capabilities. • Typical IT networking practices.	• Many proprietary and standard communication protocols. • Several types of communications media used including dedicated wire and wireless (radio and satellite). • Networks are complex and sometimes require the expertise of control engineers.	Design limitation: Standard IT solutions may not operate on control system networks.
Change management	• Software changes are applied in a timely fashion in the presence of good security policies and procedures. The procedures are often automated.	• Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the control system is maintained. • Control system outages often must be planned and scheduled days/weeks in advance.	Real-time operations: Additional planning, testing, and slower deployment are required when implementing security solutions.

System characteristic	Information technology system	Control system	Security challenge for control systems
Managed support	• Allow for diversified support methods.	• Service support is usually via a single vendor.	Design limitations: Solutions may be limited to those provided or supported by vendor.
Component lifetime	• Lifetime on the order of 3-5 years.	• Lifetime on the order of 15-20 years.	Design limitation: Security solution should not become obsolete quickly.
Access to components	• Components are usually local and easy to access.	• Components can be isolated, remote, and require extensive physical effort to gain access to them.	Design limitation: Additional time and effort required to access network components.

Source: GAO analysis of NIST, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security, Special Publication 800-82* (Initial Public Draft).

Organizational Issues Pose Challenges to Securing Control Systems

In addition to the technical challenges of securing control systems, critical infrastructure owners face organizational challenges in securing control systems, including difficulty in developing a compelling business case for improving control systems security, a reluctance to share information on control system incidents (which could help build a business case), and the division of technical responsibilities within an organization.

Experts and industry representatives reported that organizations may be reluctant to devote resources to securing control systems. These resources include money, personnel, training, and the early replacement of equipment that may have been originally designed to last 20 years or more. Until industry users of control systems have a business case to justify why additional security is needed, there may be little market incentive for the private sector to develop and implement more secure control systems.

Another challenge is the reluctance to share information on control systems incidents and the resulting lack of attention to this risk. While incidents and attacks on critical infrastructure control systems have occurred, to date there is no authoritative, centralized process for collecting and analyzing information about control systems incidents. Experts we interviewed stated that companies are reluctant to share details of incidents due to factors such as legal liability and impact on their reputation. Several experts stated that they believed incidents were occurring, but are not being reported by industry. One expert suggested that since there have been no reports of significant disruptions caused by cyber attacks on U.S. control systems, industry representatives may believe the threat of such an attack is low. We have previously

recommended that the government work with the private sector to improve the quality and quantity of information being shared among industries and government about attacks on the nation's critical infrastructures.[8]

Another challenge involves the way security responsibilities are structured within organizations that use control systems. Several experts and industry representatives stated that two separate groups often have responsibility for securing control systems: (1) IT security personnel and (2) control system engineers and operators. IT security personnel focus on securing enterprise systems, while control system engineers and operators focus on the reliable performance of their control systems. Because each has a different focus, the two groups face challenges in collaborating to implement secure control systems. For example, IT security personnel may be unaware of the special requirements of a control system and the control systems personnel may be unaware of the full range of security technologies that may be available.

Certain challenges are inherent to control systems. However, according to experts, many of these challenges can be addressed by both the private and public sectors through proper implementation of existing technology, development of new technologies, and implementation of organizational policies and procedures and training.

The Private Sector Has Multiple Initiatives Under Way to Help Secure Control Systems

Industry-specific organizations in various sectors, including the electricity, chemical, oil and gas, and water sectors, have initiatives under way to help improve control system security. These initiatives include developing standards, publishing guidance, and hosting workshops.

[8]See GAO, *Information Sharing: DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure Information*, GAO-06-383 (Washington, DC,: Apr. 17, 2006); *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors*, GAO-04-780 (Washington, D.C.: July 9, 2004); and *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors*, GAO-03-233 (Washington, DC.: Feb. 28, 2003).

Electricity

The electricity system of the United States and Canada has more than $1 trillion in asset value, more than 200,000 miles of transmission lines, and more than 800,000 megawatts of generating capability serving over 300 million people. The effective functioning of this infrastructure is highly dependent on control systems. As a result, private sector organizations in the electricity sector have several activities under way related to control systems security, including establishing mandatory reliability standards, developing guidelines for compliance with these standards, hosting workshops, and other activities. See table 4 for a description of key control systems security initiatives in the electricity sector.

Table 4: Key Control System Security Initiatives in the Electricity Sector

Organization	Initiative
North American Electric Reliability Corporation (NERC) NERC's mission is to ensure that the major transmission components of the electric system in North America are reliable, adequate, and secure. It is a self-regulatory organization that sets standards for the reliable operation and planning of the major transmission components of the electric system and monitors, assesses, and enforces compliance with those standards.	NERC promotes the development of a new mandatory system of reliability standards, authorized by the Federal Energy Regulatory Commission. The standards are meant to apply to systems such as control systems that, if compromised, could cause a threat to the large-scale power distribution system. The Energy Policy Act of 2005 established a process through which NERC is authorized to enforce compliance with these reliability standards.[a] NERC began implementing cybersecurity reliability standards that apply to control systems in June 2007. Electric utilities must be fully compliant with the standards by 2010.

Electric Power Research Institute The institute is an independent nonprofit center for energy and environmental research. It brings together members, participants, the institute's scientists and engineers, and other experts to work on solutions to the challenges of electric power. Its members represent over 90 percent of the electricity generated in the United States.	The institute has released guidelines on control systems security, including a report in 2003 and another in 2005. A recent institute report, *Compliance Guidelines for Cyber Security Reliability Standards-2006 Update*, provides information, recommendations, and tools to help the electric power industry comply with the mandatory NERC cybersecurity reliability standards. The institute is currently developing a tool to help asset managers create better business cases for control system security technology. According to a manager of the institute's CIP efforts, the institute also • has a forum that meets about three times per year during which its members discuss cybersecurity incidents, including those related to control systems; • performs research on policies and procedures for securing control systems, but has not been able to develop security technology for control systems given current funding levels (the institute's security research has included various reviews of SCADA systems, determining how to secure certain products that are being used by the electric power industry, reviewing how a facility could recognize and recover from a control systems attack, and studying the use of wireless technology for SCADA systems and the inherent security risks); and • has worked on control systems-related projects with the national laboratories, and has collaborated with DOE. For example, in 2006, the institute worked with the Pacific Northwest National Laboratory to identify the risks and vulnerabilities associated with using broadband communications for control systems and to develop mitigation strategies. According to a laboratory official, the institute and the laboratory are currently working on a project on electric power utilities' use of wireless technologies. The project is to produce two papers addressing best practices for wireless deployment in the electric sector, and guidelines for securing wireless networks, training personnel, and securely integrating wireless and wired networks.
Institute of Electrical and Electronics Engineers The institute is responsible for developing international standards for telecommunications, IT, and power generation products and services.	The Institute of Electrical and Electronics Engineers has several working groups that address issues related to control systems security in the electric power industry. Some of these work groups are developing standards for defining, specifying, and analyzing control systems. For example, the institute is developing P1689, a standard for retrofitting cybersecurity to various communications links in a control system, and P1711, a cryptographic standard for the same links. The institute is also developing P1686, which will define the functions and features to be provided in substation intelligent electronic devices to accommodate critical infrastructure protection programs.
International Electrotechnical Commission The commission prepares and publishes international standards for all electrical, electronic, and related technologies. World Trade Organization agreements permit use of these standards in international trade.	The commission's Technical Committee 57 is working to develop standards for control systems and control system components of power transmission and distribution systems, including communications and end devices called remote terminal units. It is also establishing data and communications security and communications standards for substations. The commission's Technical Committee 65 is chartered to produce standards in the area of industrial process measurement and control. Working Group 10 of the committee is developing commission standard 62443, which is a three-part standard that will address network and system cybersecurity of industrial process measurement and control systems.

Source: GAO analysis of information provided by North America Electric Reliability Corporation, interviews with Federal Energy Regulatory Commission officials, Electric Power Research Institute, Institute of Electrical and Electronics Engineers, and the International Electrotechnical Commission.

[a]Pub. L. No. 109-58, sec. 1211 (Aug. 8, 2005), 16 U.S.C. § 824o (2006).

Chemical

Control systems are used to monitor and control processes within the chemical industry. A $460 billion critical infrastructure sector, the chemical industry contributes nearly 3 percent of the U.S. gross domestic product and generates 6.2 million jobs. Chemical reactors may use control systems to produce chemicals or regulate temperatures within the production process.

The American Chemistry Council is a trade association that represents major companies in the U.S. chemical manufacturing sector. The council supports research and initiatives related to federal regulation on health, safety, security, and the environment.

The council established a Chemical Sector Cyber Security Program in 2002 to facilitate implementation of the *Chemical Sector Cyber Security Strategy*. Updated in 2006, the strategy, as well as the *Guidance for Addressing Cyber Security in the Chemical Industry*, addresses manufacturing and control system security efforts and guidance on how to secure these systems. Further, within the cybersecurity program, the Manufacturing and Control Systems Security Work Team was developed to collect, identify, and facilitate the use of practices for securing manufacturing and control systems and to establish a network of manufacturing and control systems subject matter experts.

Oil and Gas

The United States has more than 2 million miles of pipelines delivering oil and natural gas. In 2005, the consumption of natural gas totaled about 22,000 billion cubic feet, and in the United States, 20,802,000 barrels of petroleum were consumed per day. Both the gas and oil industries use control systems for process management and monitoring purposes. Employing integrated control systems, these industries can control the refining operations at a plant site, remotely monitor the pressure and flow of gas pipelines, and control the flow and pathways of gas transmissions. The sector-specific plan for the energy sector (which includes oil and gas) includes a discussion of selected control systems security efforts within the sector. The oil and gas sector has multiple control systems security activities under way, in particular, standards relating to security of control systems. See table 6 for a description of key control systems security efforts in the oil and gas sector.

Table 5: Key Control System Security Initiatives in the Oil and Gas Sector

Organization	Initiative
American Gas Association A trade organization that advocates for local natural gas utility companies and provides a broad range of programs and services for member natural gas pipelines, marketers, international gas companies, and industry associates.	The American Gas Association's Automation and Telecommunication and Gas Control committees supported the development of a report that would recommend how to apply encryption to protect gas utility control systems. A task group was organized to develop Standard *AGA Report No.12, Cryptographic Protection of SCADA Communications*, which consists of four parts. The first part, *Background, Policies, and Test Plan*, published in March 2006, is intended to serve as a guideline for voluntary implementation of a comprehensive cybersecurity posture. This report sets up the risk assessment process and allows owners and operators to determine if encryption is a good security practice for their control systems. The second part, *Retrofit Link Encryption for Asynchronous Serial Communications*, has not yet been finalized. This part contains functional requirements and details technical specifications for AGA-12 compliant retrofit devices used in control systems. Both the third and fourth parts have not yet been developed. The third part, *Protection of Networked Systems*, is to focus on high-speed communication systems for control systems, including the Internet. The final part, *Protection Embedded in SCADA Components*, is to focus on protecting control systems by incorporating cryptography into system components at the time of manufacture. The second, third, and fourth parts of this report are expected to be developed under the leadership and technical expertise of the Gas Technology Institute with user input from the membership of the American Gas Association.
American Petroleum Institute A national trade association for America's oil and natural gas industry. The institute's corporate members include various segments of the oil industry, such as producers, refiners, suppliers, pipeline operators and marine transporters, as well as service and supply companies that support all segments of the industry.	The institute published standard 1164, *Pipeline SCADA Security*, in September 2004. This standard provides guidance to the operators of oil and gas liquid pipeline systems for managing critical infrastructure control systems integrity and security. This guideline is specifically designed to provide the operators with a description of industry practices in critical infrastructure control systems security and to provide the framework needed to develop sound security practices within the operator's individual companies. The institute published standard 1165, *Recommended Practice for Pipeline SCADA Displays*, in January 2007. This recommended practice focuses on the design and implementation of displays used for displaying, monitoring, and controlling information on pipeline control systems.

Source: GAO analysis of information provided by American Gas Association, Interview with Department of Energy officials, American Petroleum Institute.

Water

The water sector includes drinking water and water treatment systems. The sector's infrastructures are diverse, complex, and distributed, ranging from systems that serve a few customers to those that serve millions. The sector includes about 150,000 water, wastewater, and storm water organizations; federal water offices at the national, regional, and state levels belonging to several agencies; some 100 state water agency organizations; and many other local government water organizations. Members of the water sector have worked with the Environmental Protection Agency on development of the Water Sector-Specific Plan, which includes some efforts on control systems security. Members of the water sector are also participating in the Process Control Security Forum's

activities. See table 7 for a list of key control system security initiatives by various organizations in the water sector.

Table 6: Key Control System Security Initiatives in the Water Sector

Organization	Initiative
Awwa Research Foundation An international nonprofit organization that sponsors research to enable water utilities, public health agencies, and other professionals to provide safe and affordable drinking water to consumers.	The foundation is currently working on two research projects. The first is the *Cryptographic Protection of SCADA Communications for Water Systems #2969*, which will develop a standard suite of equations and protocols to provide cybersecurity for water utility SCADA systems. The second, which is in collaboration with DHS, is the *Control Systems Cyber Security Self Assessment Tool #3045*, which is to identify, organize, prioritize, and describe the most probable electronic security threats; risks associated with vulnerabilities, available prevention technology, best practices, and critical areas of uncertainty. In 2002, the foundation developed a vulnerability assessment methodology for large drinking water utilities to assist them in meeting federally mandated vulnerability assessments. Now that deadlines for vulnerability assessments have passed, utilities may still use the methodology to develop emergency response plans. The methodology has also been adapted for use at small and medium-sized utilities.
Association of Metropolitan Water Agencies An organization of the largest publicly owned drinking water systems in the United States. The association collects and exchanges management, security, legislative, and technical information to support competitive utility operations, effective utility leadership, safe and secure water supplies, and effective public communication on drinking water quality.	The association served as the U.S. EPA-designated liaison between the water sector and the federal government on critical infrastructure protection and currently operates the Water Information Sharing and Analysis Center and the Water Security Channel. The Water Information Sharing and Analysis Center offers a secure database, expert analysis, information gathering, and the rapid distribution of reports and government alerts about threats to America's drinking water and wastewater utilities, including control systems. The center went online in December 2002. The Water Security Channel is a free service of the center designed to disseminate security information to the broadest wastewater and drinking water community, including information about control systems security issues. Members of the association have held workshops, events, formed committees, and written papers that deal with cyber and control systems security.

Source: American Water Works Association, Association of Metropolitan Water Agencies.

Other Organizations

Other organizations are working on efforts to improve control systems security that are not sector-specific. The organization formerly known as the Instrumentation, Systems, and Automation Society, and now called ISA, is currently working on control systems security efforts, and InfraGard, a nonprofit organization associated with the Federal Bureau of Investigation, has recently started a control systems-related effort. See table 8 for a description of these initiatives.

Table 7: Control System Security Initiatives that Affect Multiple Sectors

Organization	Initiative
ISA (formerly the Instrumentation, Systems, and Automation Society) The society develops standards, certifies industry professionals, provides education and training, and publishes books and technical articles.	The society's industrial automation and control systems' Security Standards Committee is composed of representatives from many industries, including water/wastewater, fossil fuels, nuclear energy, food and beverages, pharmaceuticals, chemicals, petrochemicals, U.S. government labs and organizations, and automotive and educational institutions. The committee intends to establish standards, recommend practices, and develop technical reports and related information that will define procedures for implementing electronically secure industrial automation and control systems and security practices and assess electronic security performance. The committee has finished two technical reports. One report documents the current state of cybersecurity technologies as they are applied to the control systems environment to clearly define what can reasonably be deployed today and to define areas where more research is needed. A second report presents an approach for developing, implementing, and operating a program that addresses security for control systems. The committee is currently working on a standard to establish and operate an industrial automation and control systems security program and specific security requirements for industrial automation and control systems. The first part deals with terminology and has been approved by the society. The second part deals with establishing a security program and is currently awaiting approval by the committee. The third part deals with operating the program and has not been started. The fourth part deals with technical security requirements and was started in October 2006. The committee has also recently started a related working group on patch management.
InfraGard/ SCADAGard InfraGard is a nonprofit organization associated with the Federal Bureau of Investigation. The program consists of 86 regional chapters with representatives from the public and private sectors. The program focuses on activities related to critical infrastructure protection and cyber crime.	InfraGard recently established a SCADAGard special interest group. According to the head of the group, the group will be used to share control systems security information with InfraGard members who are control systems vendors, owners, and operators and have previously been vetted by the Federal Bureau of Investigation.

Source: GAO analysis of information provided by ISA and InfraGard.

Federal Agencies Have Multiple Initiatives to Help Secure Critical Infrastructure Control Systems, but More Remains to Be Done

Over the past few years, federal agencies—including DHS, DOE, NIST, FERC, and others—have initiated efforts to improve the security of critical infrastructure control systems. However, DHS has not yet established a strategy to coordinate the various control systems activities across federal agencies and the private sector. Further, more can be done to address specific weaknesses in DHS's ability to share information on control systems vulnerabilities. Until DHS develops an overarching strategy, there is an increased risk that the federal government and private sector will invest in duplicative initiatives and miss opportunities to learn from other organization's activities. Further, until DHS addresses specific weaknesses in sharing information, there is an increased risk that the agency will not be able to effectively carry out its responsibility for sharing information on vulnerabilities, and that there could be a disruption to our nation's critical infrastructures.

Federal Agencies Have Many Initiatives Under Way, but DHS Lacks a Comprehensive Strategy that Delineates Responsibilities and Coordinates Activities

There are many federal efforts under way to help improve the security of critical infrastructure control systems. For example, DHS is sponsoring multiple control systems security initiatives across critical infrastructure sectors, including a program to improve control systems cybersecurity that includes vulnerability reporting and response, activities to promote security awareness within the control systems community, and efforts to build relationships with control systems vendors and infrastructure asset owners. See appendix II for a detailed description of DHS's key initiatives and projects involving control systems security.

Additionally, DOE sponsors control systems security efforts within the electric, oil, and natural gas industries. These efforts include the National SCADA Test Bed Program, which funds testing, assessments, and training in control systems security and the development of a road map for securing control systems in the energy sector. Also, several of DOE's national laboratories play an important role in implementing many DHS and DOE efforts and provide support directly to asset owners and vendors. For example, the national laboratories perform site assessments, test vendor equipment, and conduct outreach and awareness activities for infrastructure asset owners and vendors. See appendix III for more information on DOE's initiatives.

Other federal agencies, such as NIST and FERC, have also undertaken efforts to help secure control systems. For example, NIST is working with federal and industry stakeholders to develop standards, guidelines, checklists, and test methods to help secure critical control systems, while FERC is working to implement electricity reliability standards that address

control systems. See appendix IV for more information on these and other initiatives.

Several industry experts we spoke with stated that many federal programs in control systems security have been helpful. For example, experts stated that developing the road map was a positive step for the energy sector. An official who participated in the development of DOE's road map stated that the process succeeded in identifying industry needs and was a catalyst for bringing agencies and government coordinating councils together and that it was a good idea for other industries to develop plans similar to the road map. In addition, experts we interviewed said the testing and site assessments conducted by the national laboratories for DHS and DOE made individual products more secure and helped improve overall attention to control systems security.

However, the federal government does not yet have an overall strategy for guiding and coordinating control systems security efforts across the multiple agencies and sectors. To evaluate activities related to critical infrastructure protection, we developed a risk management framework for protecting critical infrastructures based on the standards and practices of leading organizations.[9] The first phase of this framework is the development of a strategy that includes the goals, objectives, constraints, specific activities, milestones, and performance measures needed to achieve a particular end result. In 2004, we reported that federal agencies, standards organizations, and the private sector were leading various initiatives on control systems security, but lacked coordination and oversight to effectively improve the cybersecurity of the nation's control systems.[10] We recommended that DHS develop and implement a strategy for coordinating control systems security efforts among government agencies and the private sector.

DHS agreed with our recommendation to develop a control systems security strategy and, in 2004, issued a strategy that focuses primarily on DHS's initiatives. However, the strategy does not include ongoing work by DOE, FERC, NIST, and others. Further, it does not include the various

[9]See GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, GAO-06-91, (Washington, D.C.: Dec. 15, 2005).

[10]GAO, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*, GAO-04-354, (Washington, D.C.: Mar. 15, 2004).

agencies' responsibilities, goals, milestones, or performance measures. Agency officials stated they have convened a federal working group that will develop a list of control systems security activities across the government. Further, in commenting on a draft of this report, DHS officials stated that this baseline list of activities will serve as the foundation for a comprehensive strategy across the public and private sectors. However, they did not provide a date for when the baseline and the comprehensive strategy would be completed. In addition, they did not state whether the list or the strategy would include responsibilities, goals, milestones, or performance measures.

Until DHS develops an overarching strategy that delineates various public and private entities' roles and responsibilities and uses it to guide and coordinate control systems security activities, the federal government and private sector risk investing in duplicative activities and missing opportunities to learn from other organization's activities.

DHS Faces Challenges in Sharing Sensitive Information on Control Systems Vulnerabilities

DHS is responsible for sharing information with critical infrastructure owners on control systems vulnerabilities, but faces challenges in doing so. In 2006, DHS developed a formal process for managing control systems vulnerabilities reported to the U.S. Computer Emergency Readiness Team (US-CERT).[11] DHS gathers this information and works with vendors and others to identify mitigation strategies. It then releases this information to critical infrastructure owners and operators, control systems vendors, and the public.

However, DHS's sharing of sensitive information on control systems to date has been limited. As of June 2007, US-CERT has issued only nine notices related to control systems security since the inception of the control systems security program in 2003. DHS's information sharing is limited in part because of reluctance by those in the private sector to inform the agency of vulnerabilities they have identified and in part because of weaknesses in DHS's ability to disseminate potentially sensitive information to the private sector. We previously reported on difficulties DHS has had in collecting information from, and sharing it

[11]US-CERT's mission is to protect the nation's Internet infrastructure. US-CERT coordinates defense against and responses to cyber attacks by analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.

with, the private sector.[12] Industry officials stated that they are reluctant to share information about incidents because of uncertainties about how the information will be used and the value of reporting such incidents.

In addition, DHS lacks a rapid, efficient process for disseminating sensitive information to private industry owners and operators of critical infrastructures. An agency official noted that sharing information with the private sector can be slowed by staff turnover and vacancies at DHS, the need to brief agency and executive branch officials and congressional staff before briefing the private sector, and difficulties in determining the appropriate classification level for the information. DHS's control systems security program manager acknowledged the need to share information more quickly. In commenting on a draft of this report, DHS officials stated that after the start of our review, the agency began developing a process to formalize and improve information sharing. However, this process was not evident during our review. Further, DHS did not provide evidence of this process or examples of how the process had actually been used to share information.

Until DHS establishes an approach for rapidly assessing the sensitivity of vulnerability information and disseminating it—and thereby demonstrates the value it can provide to critical infrastructure owners—the agency's ability to effectively serve as a focal point in the collection and dissemination of sensitive vulnerability information will continue to be limited. Without a trusted focal point for sharing sensitive information on vulnerabilities, there is an increased risk that attacks on control systems could cause a significant disruption to our nation's critical infrastructures.

Conclusions

Control systems are an essential component of our nation's critical infrastructure. Past incidents involving control systems, system vulnerabilities, and growing threats from a wide variety of sources highlight the risk facing these systems. The public and private sectors have begun numerous activities to improve the cybersecurity of these systems. However, the federal government lacks an overall strategy for coordinating public and private sector efforts. DHS also lacks an efficient process for sharing sensitive information on vulnerabilities with private sector critical infrastructure owners. Until an overarching strategy is in

[12]See GAO, *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors*, GAO-04-780 (Washington, D.C.: July 9, 2004), and GAO-06-383.

place, public and private sectors risk undertaking duplicative efforts. Also, without a streamlined process for advising private sector infrastructure owners of vulnerabilities, DHS is unable to fulfill its responsibility as a focal point for disseminating this information. If key vulnerability information is not in the hands of those who can mitigate its potentially severe consequences, there is an increased risk that attacks on control systems could cause a significant disruption to our nation's critical infrastructures.

Recommendations for Executive Action

To improve federal government efforts to secure control systems governing critical infrastructure, we recommend that the Secretary of the Department of Homeland Security implement the following two actions:

- develop a strategy to guide efforts for securing control systems, including agencies' responsibilities, as well as overall goals, milestones, and performance measures, and
- establish a rapid and secure process for sharing sensitive control system vulnerability information with critical infrastructure control system stakeholders, including vendors, owners, and operators.

Agency Comments and Our Evaluation

We received comments via e-mail on a draft of this report from DHS officials, including the Deputy Director of the National Cyber Security Division. In the comments, agency officials neither agreed nor disagreed with our recommendations. Instead, they stated that DHS would take the recommendations under advisement. Additionally, officials stated that the agency has recently begun working with its partners in the Federal Control System Security Working Group to establish a baseline of ongoing activities. This baseline is to serve as a foundation for developing a comprehensive strategy that will encompass the public and private sectors, set a vision to secure control systems, describe roles and responsibilities, and identify future requirements for resources and action. Moreover, officials stated that the agency has recently developed a process to formalize the sharing of sensitive information related to control systems vulnerabilities. The officials reported that this process describes the information flow from vulnerability discovery, to validation, public and private coordination, and outreach and awareness. Further, it identifies the deliverables and outcomes expected at each step in the process.

While DHS's intention to develop a comprehensive public/private strategy is consistent with our recommendation, the agency did not provide a date

by which this strategy will be completed. Until DHS completes the comprehensive strategy, the public and private sectors risk undertaking duplicative efforts.

Additionally, while DHS officials stated that the agency had developed a process for sharing sensitive information on control system vulnerabilities, it did not have such a process in place during our review. Further, the agency has not provided evidence of its process for sharing control system vulnerability information or evidence that this process has been used to share information. Until such a process is formalized and implemented, key vulnerability information may not be available to those who can mitigate its potentially severe consequences, therefore increasing the risk that attacks on control systems could cause a significant disruption to our nation's critical infrastructures.

DHS officials and officials from other agencies who contributed to this report provided technical comments, which we have incorporated as appropriate.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the report date. At that time, we will send copies of this report to interested congressional committees, the Secretary of the Department of Homeland Security, and other interested parties. In addition, this report will be available at no charge on GAO's Web site at www.gao.gov.

If you have any questions on matters discussed in this report, please contact Dave Powner at (202) 512-9286 or Keith Rhodes at (202) 512-6412, or by e-mail at pownerd@gao.gov and rhodesk@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix V.

David A. Powner
Director, Information Technology Management Issues

Keith A. Rhodes
Chief Technologist
Director, Center for Technology and Engineering

List of Requesters

The Honorable Joseph I. Lieberman
Chairman
The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

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

The Honorable Sheila Jackson-Lee
Chairwoman
The Honorable Daniel L. Lungren
Ranking Member
Subcommittee on Transportation Security and Infrastructure Protection
Committee on Homeland Security
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) determine cyber threats, vulnerabilities, and the potential impact of attacks on critical infrastructure control systems; (2) determine the challenges to securing critical infrastructure control systems; (3) identify private sector initiatives to strengthen the cybersecurity of control systems; and (4) assess the adequacy of public sector initiatives to strengthen the cybersecurity of control systems.

To determine the cyber threats, vulnerabilities, and the potential impact of attacks on critical infrastructure control systems, we reviewed prior GAO reports on control systems as well as reports prepared by other government agencies and private organizations, including documentation of prior control system security incidents. We conducted interviews with individuals in the private sector, including representatives of private companies that operate control systems. These individuals were selected based on their knowledge of and participation in both private and public sector control system security activities. We also met with representatives from trade associations and federal agencies. On the basis of the information and documentation we received from these individuals, and information we collected during site visits to three of the national laboratories, we were able to compile information on the cyber threats, vulnerabilities, and the potential impact of attacks on critical infrastructure control systems.

To determine the challenges to securing critical infrastructure control systems, we reviewed prior GAO reports and testimonies and materials written by other public and private organizations on control systems security, critical infrastructure protection, and national preparedness. We conducted interviews with experts and industry representatives, including managers of federal control systems programs at the Department of Homeland Security (DHS) and Department of Energy (DOE), experts from the national laboratories, vendors, owners and operators, and standards and trade associations.

To identify the private sector initiatives to strengthen cybersecurity of control systems, we researched current standards and accepted trade practices and analyzed current efforts to better secure control systems. We spoke to private sector owners and operators, vendors, trade associations, industry experts, and standards associations. These organizations included the North American Electric Reliability Corporation (NERC), the American Gas Association, and ISA.

To assess the adequacy of public sector initiatives to strengthen the cybersecurity of control systems, we researched relevant federal laws and

regulations and initiatives by federal agencies to better secure control systems, and reviewed documentation and project plans on federal control systems efforts. We also reviewed GAO's prior work analyzing best practices from leading organizations and interviewed private sector and other experts in control systems security for their perspectives on federal efforts. We interviewed officials from federal agencies including DHS, DOE, the National Institute of Standards and Technology (NIST), and the Federal Energy Regulatory Commission (FERC). In addition, we visited three of the national laboratories that are leading control systems security research and outreach efforts. These labs were selected because of their extensive participation in DOE and DHS control systems security programs. We then compared the activities of federal agencies with best practices and the perspectives of experts.

Our work was conducted from March 2007 to July 2007 at agencies' headquarters in Washington, D.C., and at national laboratories in Idaho, New Mexico, and Washington state in accordance with generally accepted government auditing standards.

Appendix II: The Department of Homeland Security's Control Systems Security Initiatives

DHS supports multiple control systems security initiatives across government and the private sector. Table 9 lists key initiatives and projects conducted by DHS in control system security.

Table 8: Selected DHS Control Systems Security Initiatives

Initiative	Description
Coordination with US-CERT	DHS's control systems program is working to enhance management of control system incidents and provide timely situational awareness information to control systems owners and operators through coordination with the United States Computer Emergency Readiness Team (US-CERT). According to agency officials, a person from the program works in the US-CERT operations center and handles any incoming threats or vulnerabilities related to control systems. The Idaho National Laboratory provides backup technical support if needed. DHS also provides outreach and awareness on the role of US-CERT in reporting and mitigating control systems cyber vulnerabilities, and is developing the capability to analyze software harmful to control systems.
Control System Cyber Security Self Assessment Tool	DHS has developed the Control Systems Cyber Security Self Assessment Tool to assist control systems owners and operators in evaluating vulnerabilities and recommending mitigation strategies. This software takes users through a series of questions to determine the current status of their control systems network. It includes specific control systems architectures recommended by the National Institute of Standards and Technology as examples for end users and uses existing standards and recommended practices to provide the user a set of requirements for addressing specific security measures. The software was piloted in 2006 in several critical infrastructure sectors, and was deployed to the water sector in June 2007. According to agency officials, the software has also been tested in the electric sector and oil and gas sectors. According to DHS officials, in the future, the department plans to turn over development and maintenance of the software to a commercial vendor.
Process Control System Forum	In February 2005, DHS launched the first Process Control System Forum. The forum is primarily a means for the government to reach out to academia, vendors, and owners and operators of critical infrastructure. In March 2007, the forum was held in Atlanta, Georgia, and included approximately 200 attendees.
Cyber Security Procurement Language for Control Systems	The Cyber Security Procurement Language for Control Systems project is an initiative that DHS sponsored together with Idaho National Laboratory, the Multi-State Information Sharing and Analysis Center, and private industry. The purpose of the project is to summarize security principles that should be considered when designing and procuring control systems products and provide examples of language to incorporate into procurement specifications. According to an industry expert, the language has been used by owners procuring new control systems equipment. NIST officials stated that they are considering integrating this project into the Control System Cyber Security Self Assessment Tool (see previous section), by identifying the procurement language that would be necessary to address an identified vulnerability. In January 2007 the National Infrastructure Advisory Council[a] issued a report recommending that the Office of Management and Budget mandate that federal agencies apply the procurement language when procuring control systems and services.

Initiative	Description
Catalog of Control System Security Requirements	DHS is also in the process of developing a Catalog of Control System Security Requirements. This initiative will provide a catalog of recommended requirements to facilitate the development and implementation of control systems cybersecurity standards to be applied to critical infrastructure. DHS and NIST officials stated that this will provide a common terminology that can be used for standards development and can therefore promote collaboration or convergence of industry standards. The catalog was used by NIST during the development of control systems-related guidance and, according to agency officials, was sent to ISA, a standards association, and the International Electrotechnical Commission for consideration. The catalog is currently in draft form.
Monthly Vendor Phone Calls	DHS hosts monthly teleconference meetings with control systems vendors to provide a forum for the vendors to share information and common concerns, and to discuss control systems security needs for legacy and next generation products. According to agency officials, approximately 30 vendors representing most of the sectors using control systems are participating in the calls. At the most recent Process Control System Forum conference, the vendors held their first face-to-face meeting. The DHS Control System Security Program Director stated that approximately 90 percent of the control systems manufacturers in the United States were represented at this meeting.
Federal Control Systems Working Group	This group represents the federal control systems community and it is currently working on development of a baseline of federal control systems security efforts and enhancing information sharing with relevant stakeholders.
National Laboratory Assessments and Training	DHS funds initiatives at DOE laboratory facilities including control systems site and vendor assessments and training. For more information, see appendix III.
Institute for Information Infrastructure Protection	In January 2002, the Institute for Information Infrastructure Protection, a consortium made up of 27 entities managed by Dartmouth College, began operation. In 2005, the institute launched the Process Control Systems Security Research Project. This project focuses on cybersecurity-related research in the oil and gas sector. Initiatives completed include a source code checking tool, an intrusion detection and event correlation tool for process control systems, and a tool for building a business case for investing in security. According to program officials, currently there are two main bodies of work: (1) work that is drawing to a close from $8.5 million in funding from DHS's Science and Technology Directorate and (2) a new body of work that received $4.1 million in funding from DHS's National Cyber Security Division. Institute officials stated that the new work is under way as of April 2007, and will also focus on solutions for survivability and recovery of process control systems in the oil, gas, and chemical industries.
Linking the Oil and Gas Industry to Improve Cyber Security	The Linking the Oil and Gas Industry to Improve Cyber Security project was a cooperative initiative between DHS's Science and Technology Directorate and companies in the oil and gas industry that ran from July 2005 to June 2006. The program's purpose was to identify new technologies for protecting process control systems. The program included a 14-member consortium of private sector oil and gas companies. DHS officials stated that the project was a precompetitive research and development project, and therefore the agency was able to provide support to begin the project and will likely play a role in the technology transfer process. The consortium of companies selected six vendor products to be included in the project. The consortium worked with Sandia National Laboratories on integrating and testing the six products, which resulted in a potentially viable security solution. The integrated solution was demonstrated to the participating organizations at a wrap-up meeting in Houston, Texas, on September 11, 2006.

Initiative	Description
Small Business Innovation Research Awards	According to agency officials, from 2004 to 2005 DHS's Science and Technology Directorate funded 13 research proposals related to control systems security. The proposals received individual awards of up to $100,000 and lasted no more than 6 months in duration. On the basis of the results of these proposals, DHS awarded five small business innovation research awards. These awards were up to $750,000 and typically were for no more than 2 years in duration. The last of these awards was completed in February 2007. Agency officials stated that oil and gas owners and operators have shown particular interest in continuing work on intrusion detection, encryption, and authentication of users.
Chemical Facilities Security Standards	The 2007 DHS Appropriations Act required that DHS issue interim final regulations establishing security standards for chemical facilities. The regulations require vulnerability assessments and the development and implementation of site security plans for these facilities, and DHS must audit and inspect the facilities. DHS issued the regulations in April 2007, explicitly extending their applicability to control systems.
Pipeline Control Systems Safety	The Transportation Security Administration's Pipeline Security Division conducts a corporate security review process for major pipeline operators that includes a high-level review of control systems security. As of June 2007, the division has conducted approximately 65 reviews. In addition, the administration is working on a pilot project involving assessments of security policies and control systems security for a particular pipeline operator.

Source: GAO analysis of information provided by DHS and the Institute for Information Infrastructure Protection.

[a]The National Infrastructure Advisory Council was chartered on July 1, 2005 to provide the President, through the Secretary of the Department of Homeland Security, with advice on the security of the critical infrastructure sectors and their information systems.

Appendix III: The Department of Energy's Initiatives to Support Control Systems Security within the Energy Sector

Since 2003, the Department of Energy's Office of Electricity Delivery and Energy Reliability has led control systems security efforts within the electric, oil, and natural gas industries by establishing the National SCADA Test Bed Program and developing a 10-year strategic framework for securing control systems in the energy sector. DOE's national laboratory facilities also play an important role in control systems security research. In particular, the Idaho National Laboratory, Sandia National Laboratories, and the Pacific Northwest National Laboratory lead key efforts in control systems security research for DOE, DHS, and other public and private organizations.

The National SCADA Test Bed Program

In 2004, DOE launched the National SCADA Test Bed Program, a multilaboratory effort to identify control systems vulnerabilities, conduct control systems research and development, and provide cybersecurity training and outreach to industry. The test bed program includes five DOE laboratories and has a budget of $10 million for fiscal year 2007. To date, the test bed program has completed 12 control systems vulnerability assessments in cooperation with control systems vendors and energy sector owners and operators. As a result of these assessments, the test bed team has provided vendors with recommendations to improve control systems security, and owners and operators with strategies for mitigating existing system security risks. The test bed program also has 10 ongoing control systems research and development projects that are peer-reviewed biannually to ensure they meet the needs of the government and the end users. In addition to its testing and research efforts, the program has led training workshops on control systems security for over 1,500 industry personnel, and has established a working group to evaluate control systems security standards in the energy sector.

Strategic Framework for Securing Control Systems in the Energy Sector

In January 2006, DOE released the *Roadmap to Secure Control Systems in the Energy Sector*, a collaborative public-private strategy for securing control systems infrastructures over the next 10 years. Developed jointly by energy owners and operators, researchers, vendors, and the government, the road map links near-, mid-, and long-term security needs with four main goals: (1) measure and assess the current security posture; (2) develop and integrate protective measures; (3) detect intrusion and implement response strategies; and (4) sustain security improvements.

The road map outlines the energy sector's top control systems security concerns and existing mitigation efforts, and is serving as a model for other sectors to develop similar plans. For example, in January 2007,

DHS's National Infrastructure Advisory Council recommended that DHS and the sector-specific agencies develop plans using DOE's road map as a model. DOE has used the road map to align its test bed projects with strategic goals. In addition, DOE has created an online road map that uses the strategic framework to track public and private sector control systems security projects.

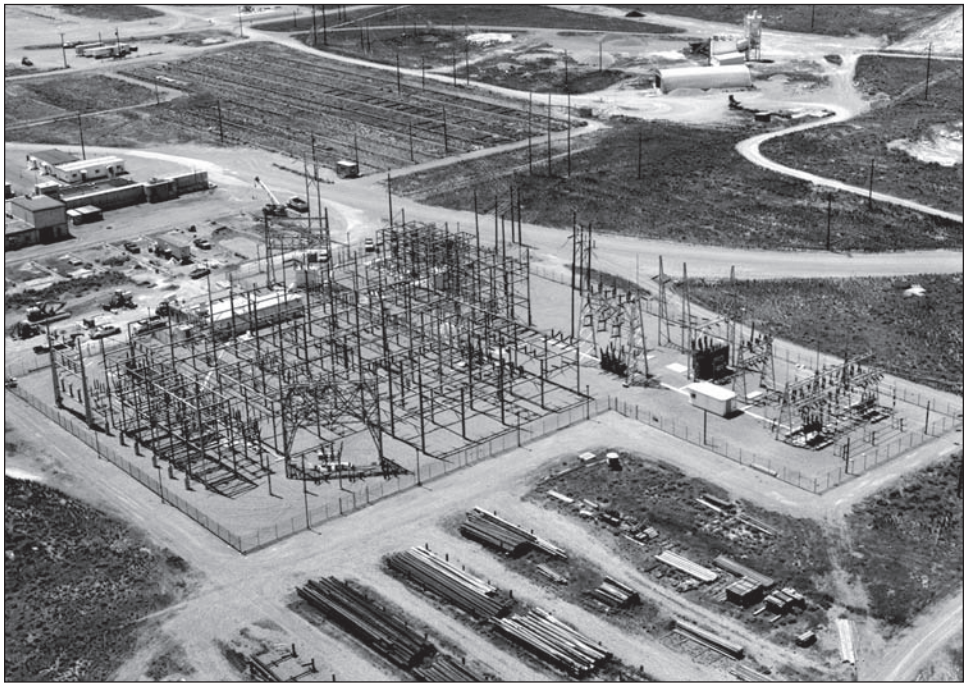
National Laboratories Are Leading Significant Portions of Control Systems Security Work

DOE owns 17 laboratories and research facilities around the country that play an important role in control systems security research. In particular, the Idaho National Laboratory, the Sandia National Laboratories, and the Pacific Northwest National Laboratory manage and conduct key efforts in control systems security research for DOE, DHS, and other public and private organizations. Using their research facilities, the laboratories are able to conduct work for DHS, DOE, and other organizations.

Research Facilities

The laboratories are able to use a number of unique research facilities to test control systems equipment. For example, Idaho National Laboratory operates its own electrical power transmission facility, which consists of 61 miles of high-voltage transmission lines, feeders, transformers, and independent substations (see fig. 5). According to laboratory officials, because portions of the transmission facility are easy to separate from the overall power grid, control systems equipment can be tested on the grid without fear of effects on the larger power grid.

Figure 5: A Substation That Is Part of Idaho National Laboratory's Facilities for Testing Control Systems



Source: Idaho National Laboratory.

The Pacific Northwest National Laboratory has the Electricity Infrastructure Operations Center, which is a replica of a typical operations center used in the electric industry, with consoles, displays, hardware, and software that can be used for control of electricity transmission (see fig. 6). The center receives live transmission data from actual utility control systems, and is used as a platform for research, development, and demonstration.

Figure 6: The Pacific Northwest National Laboratory's Electricity Infrastructure Operations Center

Source: Pacific Northwest National Laboratory.

DHS Sponsors Laboratory Activities Involving Control Systems Security

The national laboratories manage key efforts for DHS related to control systems security. For example, the Idaho National Laboratory is the lead laboratory to support and execute the DHS Control Systems Security Program. According to laboratory officials, the laboratories coordinate activities funded through DHS with those funded through the National SCADA Test Bed of the Department of Energy. For example, Idaho National Laboratory has conducted five vendor assessments and six site assessments using DHS funds and eight vendor assessments and four site assessments using DOE funds.

Additionally, the Idaho, Pacific Northwest, and Sandia National Laboratories developed training for asset owners and operators. The Idaho National Laboratory has developed 4- and 8-hour classes on control systems security that it has given to approximately 1,500 industry personnel since 2005. In 2006, the Pacific Northwest National Laboratory developed online control systems security awareness training that has been published on US-CERT's Web site. In 2007, Sandia National Laboratories developed training to educate owners and operators on how to effectively use red teaming to improve the security posture of their

control systems.[1] Further, the Idaho National Laboratory has worked with George Mason University and New York University to develop a draft master's level course curriculum on critical infrastructure and control systems security.

DOE's National SCADA Test Bed Sponsors Laboratory Activities

Under DOE's National SCADA Test Bed Program, the national laboratories have worked both independently and collaboratively on performing vendor vulnerability assessments, conducting control systems research and development, and leading industry training and outreach.[2] For example, between 2004 and 2007, the Idaho National Laboratory conducted assessments of eight different control systems for the electricity sector. According to laboratory officials, vendors provide the lab with the hardware, software, and training necessary to run the control system; this represents a $1 million to $1.5 million investment by the vendor. Largely on the basis of the results of these assessments, vendors have chosen to develop system patches, reconfigure system architectures, and build enhanced systems, which have been retested by the laboratory. Furthermore, according to an agency official, the results of the vendor assessments have helped inform other federal control systems efforts, such as the development of the control system self assessment tool. In addition, the Idaho National Laboratory has conducted four on-site control system assessments for electricity sector owners and operators.

In addition to vendor assessments, the laboratories are engaged in 10 research projects that are to help industry stakeholders analyze control systems operations and improve the security and reliability of architectures for control systems. For example, the Pacific Northwest National Laboratory has developed a technology to encapsulate control systems communications between two devices with a unique identifier and authenticator. This technology enables the devices to verify that the communication has not been tampered with. Unlike comparable technologies for standard information technology (IT) systems, the authentication technology does not require substantial amounts of bandwidth or processing power. Importantly, this technology has the potential to be applied to both new systems and older control systems. In

[1]Red teaming is assembling a team to attack a computer system for the purpose of identifying and reporting its vulnerabilities.

[2]Five national laboratories currently participate in the National SCADA Test Bed program: Idaho National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, Oak Ridge National Laboratory, and Argonne National Laboratory.

addition, the Idaho, Pacific Northwest, and Sandia National Laboratories are working on identifying vulnerabilities in the current communications protocol used between control centers, testing mitigation techniques, and, ultimately, assisting industry in implementing a secure version of the protocol.

Other Organizations Sponsor Laboratory Activities

In addition to work for DHS and DOE, the laboratories have conducted control systems security work for other public and private organizations, including research, security assessments, and training. For example, the laboratories have performed security assessments of control systems for federal operators of critical infrastructure, including the Bureau of Reclamation, Tennessee Valley Authority, Bonneville Power Administration, and the Strategic Petroleum Reserve, as well as private sector utility companies. Moreover, the Pacific Northwest National Laboratory worked with the Nuclear Regulatory Commission and the Nuclear Energy Institute to develop a self-assessment methodology for nuclear plants to determine compliance with standards.

Appendix IV: Other Agencies' Initiatives to Help Secure Critical Infrastructure Control Systems

In addition to DHS and DOE, multiple other federal agencies and entities are working to help secure critical infrastructure control systems. Initiatives undertaken by the Federal Energy Regulatory Commission, the National Institute of Standards and Technology, the Environmental Protection Agency, and others are described here.

Federal Energy Regulatory Commission

Under the Energy Policy Act of 2005, the Federal Energy Regulatory Commission (FERC) was authorized to (1) appoint an electricity reliability organization to develop and enforce mandatory electricity reliability standards, including cybersecurity, and (2) approve, remand, or require modification to each proposed standard. The agency may also direct the reliability organization to develop a new standard or modify existing standards. Both the agency and the reliability organization have the authority to enforce approved standards, investigate incidents, and impose penalties (up to $1 million a day) on noncompliant electricity asset users, owners, or operators.

FERC has conducted several activities to begin implementing the requirements of the act. In July 2006, FERC certified the North American Electric Reliability Corporation (NERC) as the electric reliability organization. In December 2006, FERC released a staff assessment of NERC's eight Critical Infrastructure Protection (CIP) reliability standards, which include standards for control systems security. FERC found that while the standards were a good start, there were a number of items that required improvement, including ambiguous language for standards requirements, measurability, and degrees of compliance; insufficient technical requirements to ensure grid reliability; and the use of "fill-in-the-blank standards," which are not enforceable. NERC agreed that the standards represented a starting point and has proposed a work plan to address the deficiencies. In July 2007, FERC issued a notice of public rulemaking in which it proposed to approve eight CIP reliability standards while directing NERC to modify the areas of these standards that require improvement. After considering public comments on the notice of public rulemaking, which are due in late September 2007, FERC plans to issue its final rule on the CIP reliability standards.

The National Institute of Standards and Technology Is Developing Standards and Guidance to Improve Control Systems Security

The National Institute of Standards and Technology (NIST) is working with federal and industry stakeholders to develop standards, guidelines, checklists, and test methods to help secure critical control systems. For example, NIST is currently developing guidance for federal agencies that own or operate control systems to comply with federal information system security standards and guidelines.[1] The guidance identifies issues and modifications to consider in applying information security standards and guidelines to control systems. Table 10 lists key NIST efforts.

Table 9: NIST Control Systems Security Efforts

Initiative	Description
Industrial Control Systems Security Project	The project intends to build on current federal security standards and provide targeted extensions and/or interpretations of those standards for industrial and process control systems where needed.
Special Publication 800-53, *Recommended Security Controls for Federal Information Systems, Revision 1 — Appendix I: Industrial Control Systems: Interim Guidance on the Application of Security Controls*	NIST is currently working on applying Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, to control systems. NIST SP 800-53 was originally developed for the traditional IT environment, and it treats control systems as information systems. However, organizations have had difficulties in using SP 800-53 to protect their control systems due to the unique needs of control systems. Through the results of NIST workshops held in April 2006 and March 2007, NIST developed and, in July 2007, released an augmentation to SP 800-53 that addresses control systems. According to agency officials, while most controls in SP 800-53 are applicable to control systems as written, several controls do require supplemental guidance and enhancements. NIST officials stated they plan to hold a workshop in late summer 2007, to include representatives from national and international control systems communities to share information, obtain input, and determine their level of interest in voluntarily adopting and using NIST's industrial control system interpretation of SP 800-53.
Special Publication 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*	NIST is developing Special Publication 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*. The publication is a guidance document on how to secure control systems, including the security of legacy systems. An initial public draft was released in September 2006, and the publication is due for second public draft release in August 2007.
NIST Special Publication 1058, *Using Host-Based Antivirus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts*	NIST and Sandia National Laboratories, under the guidance and sponsorship of DOE's Office of Electricity Delivery and Energy Reliability and its National SCADA Test Bed Program, investigated and tested the impacts of commercial, off-the-shelf antivirus software on control system performance. A guidance document was released in September 2006.

[1]See National Institute of Standards and Technology, *Special Publication 800-82 Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security: Recommendations of the National Institute of Standards and Technology*, (Gaithersburg, Maryland, September 2006).

Initiative	Description
Process Controls Security Requirements Forum	NIST organized the Process Controls Security Requirements Forum to establish security specifications that can be used in the procurement, development, and retrofit of industrial control systems. The forum's membership includes representatives from the water, electric, chemical, and petrochemical industries; U.S. government laboratories and organizations; and vendors of control systems. Its immediate goal is to increase the security of control systems through the definition and application of a common set of information security requirements for these systems.
Catalog of Control System Security Requirements	In collaboration with DHS, NIST is developing a catalogue of requirements that provides a detailed list of security requirements to facilitate the development and convergence of cybersecurity standards applied to control systems across the industries, domestic and foreign.
NIST Industrial Control System Security Test Bed	NIST initiated the development of a test bed consisting of several implementations of typical industrial control systems including SCADA, networking equipment, and relevant sensors. The test bed is being used at NIST to develop test methods for validation and conformance testing of security implementations. The test bed is also being used to help identify system vulnerabilities and to establish best practices.

Source: NIST.

Other Federal Agencies Are Working with DHS, DOE, and NIST on Control Systems Security Initiatives

Environmental Protection Agency

The Environmental Protection Agency (EPA) assisted DHS in developing a control systems self-assessment tool, a software program that assists owners and operators in identifying control systems vulnerabilities and mitigation strategies for addressing these vulnerabilities. EPA began work on a water security assessment tool in response to the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, which required the agency to conduct vulnerability assessments of community water systems serving more than 3,300 individuals. EPA's preliminary work in this area served as the foundation for DHS's Control Systems Cyber Security Self Assessment Tool project. The agency initially launched the tool within the water sector in July 2007.

In addition, EPA actively participates in control systems security information sharing activities through the Water Information Sharing and Analysis Center and DHS's Homeland Infrastructure Threat and Risk

Analysis Center, and has been involved with control systems standards development efforts.

Federal Bureau of Investigation

The Federal Bureau of Investigation's Cyber Crime division participates in DHS's US-CERT program and coordinates with DHS's National Cyber Security Division on general cybersecurity issues. According to an agency official, the Cyber Crime division is in the process of establishing a control systems work group within its Intelligence and Information Sharing group.

In addition, since 1996, the bureau's cyber division has sponsored InfraGard, a cooperative government and private sector program to exchange information about infrastructure threats and vulnerabilities. As previously mentioned, SCADAGard, a special interest group within InfraGard, is to be used to share information with control systems owners and operators who have been vetted by the bureau.

Nuclear Regulatory Commission

The Nuclear Regulatory Commission has conducted several activities related to enhancing the cybersecurity of control systems. The commission, which has regulatory authority over nuclear power plant safety control systems, completed a cybersecurity self-assessment project with technical assistance from the Pacific Northwest National Laboratory in October 2004 and documented the results in two technical reports published in 2004 and 2005.[2] According to agency officials, on the basis of the information in these reports, a nuclear industry task force developed *NEI 04-04, Cyber Security Program for Power Reactors*, to provide nuclear power reactor licensees a means for developing and maintaining effective cybersecurity programs at their sites. In December 2005, the commission's staff accepted this document as an acceptable method for establishing and maintaining cybersecurity programs at nuclear power plants.

In January 2006, the commission issued a revision to Regulatory Guide 1.152, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*, which provides cybersecurity-related guidance for the design of nuclear power plant safety systems. In addition, the commission has initiated a rulemaking process providing security requirements for digital computer and communication networks, including systems that are

[2]U.S. Nuclear Regulatory Commission, *NUREG/CR-6847: Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants*, (Washington D.C., October, 2004) and *NUREG/CR-6852: An Examination of Cyber Security at Several U.S. Nuclear Power Plants*, (Washington D.C.: May, 2005)

needed for safety, security, or emergency response. The public comment period for this rulemaking closed in March 2007.

According to agency officials, in May 2007, all nuclear plants had completed an inventory and assessment of their critical digital systems. Agency officials stated that the commission staff is planning to conduct oversight inspections after completion of ongoing security-related rulemaking that will clearly establish the requirements for nuclear power plant cybersecurity programs.

Appendix V: GAO Contacts and Staff Acknowledgments

GAO Contacts

David A. Powner, (202) 512-9286 or pownerd@gao.gov

Keith A. Rhodes, (202) 512-6412 or rhodesk@gao.gov

Staff Acknowledgments

In addition to those named above, Scott Borre, Heather A. Collins, Neil J. Doherty, Vijay D'Souza, Nancy Glover, Sairah Ijaz, Patrick Morton, and Colleen M. Phillips (Assistant Director) made key contributions to this report.

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 "Subscribe to 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, D.C. 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

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Susan Becker, Acting Manager, Beckers@GAO.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548