United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House Committee on Government Reform

For Release on Delivery
Expected at 1:00 p.m. EDT
Wednesday, October 1, 2003

CRITICAL INFRASTRUCTURE PROTECTION

Challenges in Securing Control Systems

Statement of Robert F. Dacey,
Director, Information Security Issues

October 1, 2003

CRITICAL INFRASTRUCTURE PROTECTION

Challenges in Securing Control Systems

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-140T, testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House Committee on Government Reform

Why GAO Did This Study

Computerized control systems perform vital functions across many of our nation's critical infrastructures. For example, in natural gas distribution, they can monitor and control the pressure and flow of gas through pipelines; in the electric power industry, they can monitor and control the current and voltage of electricity through relays and circuit breakers; and in water treatment facilities, they can monitor and adjust water levels, pressure, and chemicals used for purification.

In October 1997, the President's Commission on Critical Infrastructure Protection emphasized the increasing vulnerability of control systems to cyber attacks. The House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census asked GAO to testify on potential cyber vulnerabilities.

GAO's testimony focused on (1) significant cybersecurity risks associated with control systems; (2) potential and reported cyber attacks against these systems; (3) key challenges to securing control systems; and (4) steps that can be taken to strengthen the security of control systems, including current federal and private-sector initiatives.

www.gao.gov/cgi-bin/getrpt?GAO-04-140T.

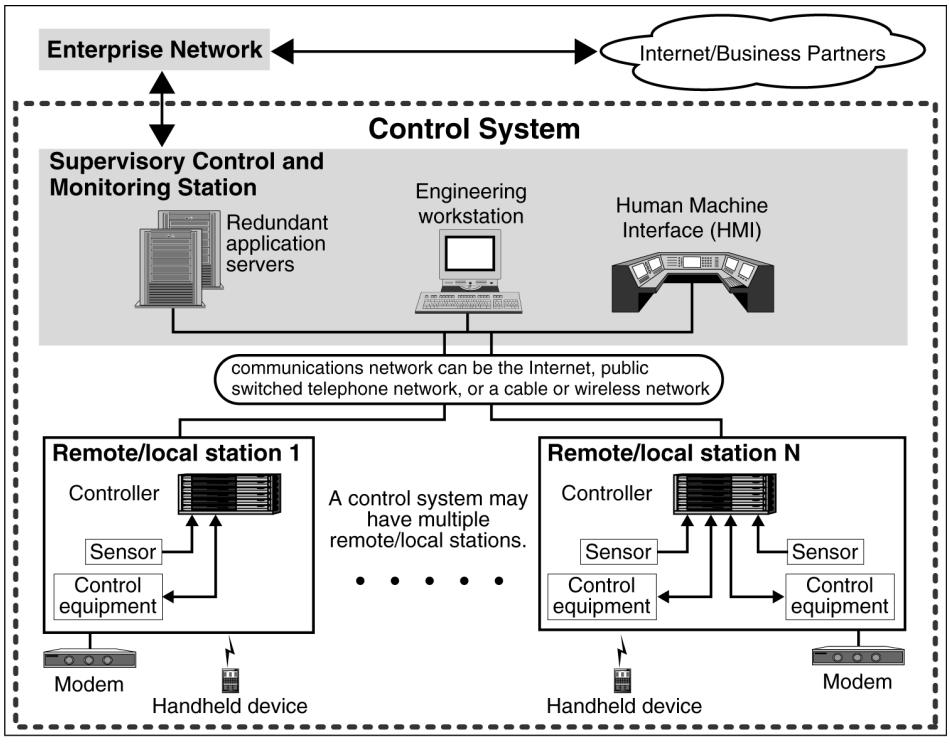
To view the full product, including the scope and methodology, click on the link above. For more information, contact Robert F. Dacey at (202) 512-3317 or daceyr@gao.gov.

What GAO Found

In addition to general cyber threats, which have been steadily increasing, several factors have contributed to the escalation of the risks of cyber attacks against control systems. These include the adoption of standardized technologies with known vulnerabilities, the increased connectivity of control systems to other systems, constraints on the use of existing security technologies for control systems, and the wealth of information about them that is publicly available. Common control system components are illustrated in the graphic below.

Control systems can be vulnerable to a variety of attacks, examples of which have already occurred. Successful attacks on control systems could have devastating consequences, such as endangering public health and safety; damaging the environment; or causing a loss of production, generation, or distribution of public utilities.

Securing control systems poses significant challenges, including technical limitations, perceived lack of economic justification, and conflicting organizational priorities. However, several steps can be taken now and in the future to promote better security in control systems, such as implementing effective security management programs and researching and developing new technologies. The government and private industry have initiated several efforts intended to improve the security of control systems.



Source: GAO (analysis), Art Explosion (clipart)

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to participate in the Subcommittee's hearing on the security of control systems. Control systems—which include supervisory control and data acquisition (SCADA) systems and distributed control systems—perform vital functions across 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. In October 1997, the President's Commission on Critical Infrastructure Protection highlighted cyber attacks as specific points of vulnerability, stating that "the widespread and increasing use of SCADA systems for control of energy systems provides increasing ability to cause serious damage and disruption by cyber means."

In my testimony today I will discuss the (1) significant cybersecurity risks associated with control systems; (2) potential and reported cyber attacks against these systems; (3) key challenges to securing control systems; and (4) steps that can be taken to strengthen the security of control systems, including current federal and private-sector initiatives.

In preparing for this testimony, we conducted a literature search and analyzed research studies and reports about the vulnerabilities of control systems. We met with private-sector and federal officials with expertise in control systems and their security. Finally, we relied on prior GAO reports and testimonies on critical infrastructure protection, information security, and national preparedness, among others. Our work was performed from July to September 2003 in accordance with generally accepted government auditing standards.

Results in Brief

For several years, security risks have been reported in control systems, upon which many of the nation's critical infrastructures rely to monitor and control sensitive processes and physical functions. In addition to general cyber threats, which have been steadily increasing, several factors have contributed to the escalation of risks specific to control systems, including the (1) adoption of standardized technologies with known vulnerabilities, (2) connectivity of control systems to other networks, (3) constraints on the use of existing security technologies and practices, (4) insecure remote connections, and (5) widespread availability of technical information about control systems.

Control systems can be vulnerable to a variety of attacks. These attacks could have devastating consequences, such as endangering public health and safety; damaging the environment; or causing a loss of production, generation, or distribution of public utilities. Control systems have already been subject to a number of cyber attacks, including attacks on a sewage treatment system in Australia in 2000 and, more recently, on a nuclear power plant in Ohio.

Several challenges must be addressed in order to effectively secure control systems. These include: the limitations of current security technologies in securing control systems, the perception that securing control systems may not be economically justifiable, and conflicting priorities within organizations regarding the security of control systems.

Several steps can be considered when addressing potential threats to control systems, including (1) researching and developing new security technologies to protect control systems; (2) developing security policies, guidance, and standards for control systems; (3) increasing security awareness and sharing information about implementing more secure architectures and existing security technologies, for example, by segmenting process control networks with robust firewalls and strong authentication; (4) implementing effective security management programs that include consideration of control system security; and (5) developing and testing continuity plans within organizations and industries, to ensure safe and continued operation in the event of an interruption, such as a power outage or cyber attack on control systems. Government and private industry have initiated several efforts intended to improve the security of control systems. These initiatives include efforts to promote research and development activities, form information sharing and analysis centers, and develop new standards. In addition, we have made several recommendations for improving the federal government's critical infrastructure protection efforts, which include control systems.

Background

Cyberspace Introduces Risks for Control Systems

Dramatic increases in computer interconnectivity, especially in the use of the Internet, continue to revolutionize the way our government, our nation, and much of the world communicate and conduct business. The benefits have been enormous. Vast amounts of information are now literally at our fingertips, facilitating research on virtually every topic imaginable; financial and other business transactions can be executed almost instantaneously, often 24 hours a day; and electronic mail, Internet

Web sites, and computer bulletin boards allow us to communicate quickly and easily with a virtually unlimited number of individuals and groups.

However, this widespread interconnectivity poses significant risks to the government's and our nation's computer systems and, more important, to the critical operations and infrastructures they support. For example, telecommunications, power distribution, water supply, public health services, national defense (including the military's warfighting capability), law enforcement, government services, and emergency services all depend on the security of their computer operations. The speed and accessibility that create the enormous benefits of the computer age, if not properly controlled, may allow individuals and organizations to inexpensively eavesdrop on or interfere with these operations from remote locations for mischievous or malicious purposes, including fraud or sabotage. Table 1 summarizes the key threats to our nation's infrastructures, as observed by the Federal Bureau of Investigation (FBI).

Table 1: Threats to Critical Infrastructure Observed by the FBI

Threat	Description
Criminal groups	There is an increased use of cyber intrusions by criminal groups who attack systems for purposes of monetary gain.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities.
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, while attack tools have become more sophisticated, they have also become 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.
Information warfare	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 Central Intelligence,a can affect the daily lives of Americans across the country.
Insider threat	The disgruntled organization insider 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 outsourcing vendors.
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.

Government officials remain concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. According to the FBI, terrorists, transnational criminals, and intelligence services are quickly becoming aware of and using information exploitation tools such as computer

viruses, Trojan horses, worms, logic bombs, and eavesdropping sniffers that can destroy, intercept, degrade the integrity of, or deny access to data.[1] In addition, the disgruntled organization insider is a significant threat, since these individuals often have knowledge that allows them to gain unrestricted access and inflict damage or steal assets without possessing a great deal of knowledge about computer intrusions. As greater amounts of money and more sensitive economic and commercial information are exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on standardized information technology (IT), the likelihood increases that information attacks will threaten vital national interests.

As the number of individuals with computer skills has increased, more intrusion or "hacking" tools have become readily available and relatively easy to use. A hacker can literally download tools from the Internet and "point and click" to start an attack. Experts agree that there has been a steady advance in the sophistication and effectiveness of attack technology. Intruders quickly develop attacks to exploit vulnerabilities discovered in products, use these attacks to compromise computers, and share them with other attackers. In addition, they can combine these attacks with other forms of technology to develop programs that automatically scan the network for vulnerable systems, attack them, compromise them, and use them to spread the attack even further.

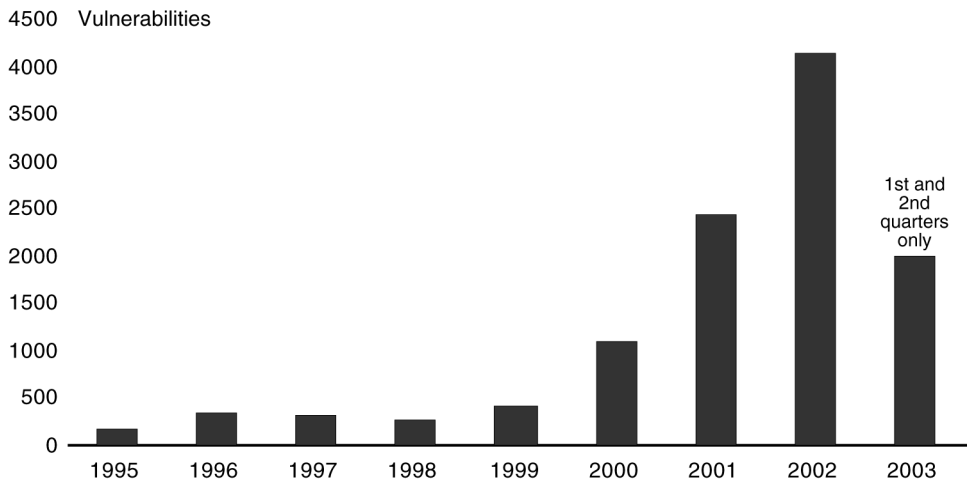
Between 1995 and the first half of 2003, the CERT® Coordination Center[2] (CERT/CC) reported 11,155 security vulnerabilities that resulted from software flaws. Figure 1 illustrates the dramatic growth in security

[1]*Virus*: a program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the "infected" file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate. *Trojan horse*: a computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute. *Worm*: an independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate. *Logic bomb*: in programming, a form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as termination of the programmer's employment. *Sniffer*: synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.

[2]The CERT/CC is a center of Internet security expertise at the Software Engineering Institute, a federally funded research and development center operated by Carnegie-Mellon University.

vulnerabilities over these years. The growing number of known vulnerabilities increases the number of potential attacks created by the hacker community. Attacks can be launched against specific targets or widely distributed through viruses and worms.

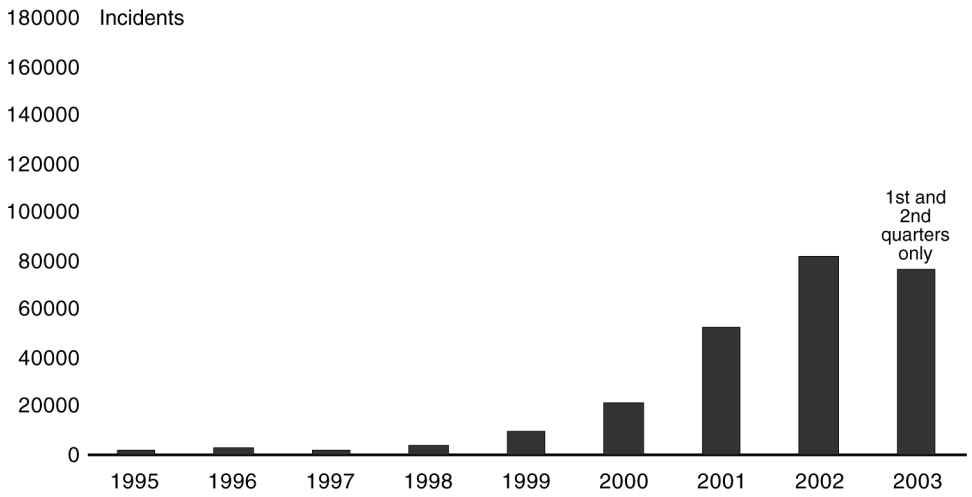
Figure 1: Security Vulnerabilities, 1995—first half of 2003



Source: GAO analysis based on Carnegie-Mellon University's CERT® Coordination Center data.

Along with these increasing threats, the number of computer security incidents reported to the CERT/CC has also risen dramatically—from 9,859 in 1999 to 82,094 in 2002 and 76,404 for just the first half of 2003. And these are only the reported attacks. The Director of CERT Centers stated that he estimates that as much as 80 percent of actual security incidents goes unreported, in most cases because (1) the organization was unable to recognize that its systems had been penetrated or there were no indications of penetration or attack or (2) the organization was reluctant to report. Figure 2 shows the number of incidents that were reported to the CERT/CC from 1995 through the first half of 2003.

Figure 2: Information Security Incidents, 1995—first half of 2003



Source: GAO analysis based on Carnegie-Mellon University's CERT® Coordination Center data.

According to the National Security Agency, foreign governments already have or are developing computer attack capabilities, and potential adversaries are developing a body of knowledge about U.S. systems and about methods to attack these systems. The National Infrastructure Protection Center (NIPC) reported in January 2002 that a computer belonging to an individual with indirect links to Osama bin Laden contained computer programs that suggested that the individual was interested in structural engineering as it related to dams and other water-retaining structures. The NIPC report also stated that U.S. law enforcement and intelligence agencies had received indications that Al Qaeda members had sought information about control systems from multiple Web sites, specifically on water supply and wastewater management practices in the United States and abroad.

Since the terrorist attacks of September 11, 2001, warnings of the potential for terrorist cyber attacks against our critical infrastructures have also increased. For example, in his February 2002 statement for the Senate Select Committee on Intelligence, the director of central intelligence discussed the possibility of cyber warfare attack by terrorists.[3] He stated that the September 11 attacks demonstrated the nation's dependence on

[3]Testimony of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence, Feb. 6, 2002.

critical infrastructure systems that rely on electronic and computer networks. Further, he noted that attacks of this nature would become an increasingly viable option for terrorists as they and other foreign adversaries become more familiar with these targets and the technologies required to attack them.

What are control systems?

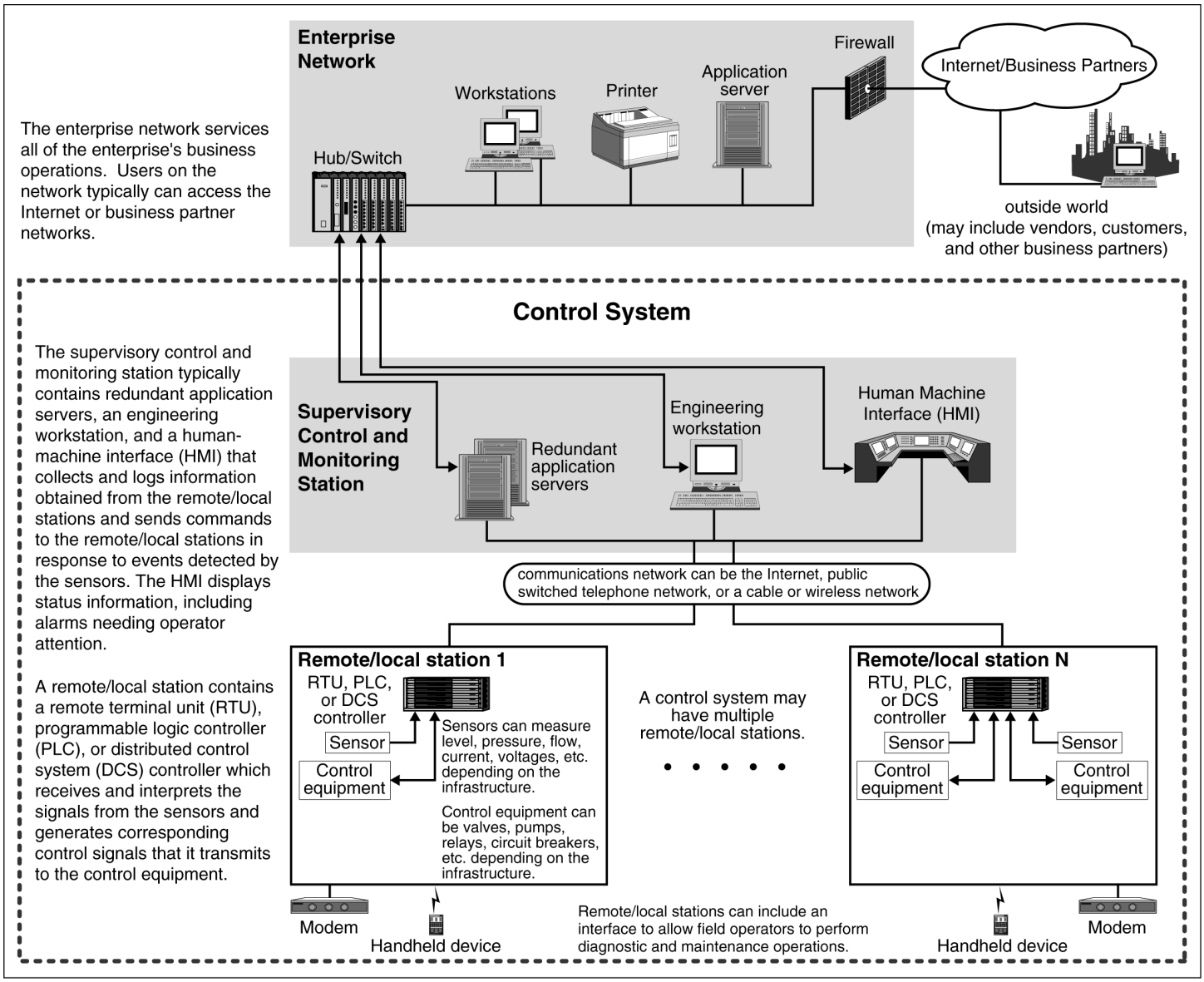
Control systems are computer-based systems that are used by many infrastructures and industries to monitor and control sensitive processes and physical functions. Typically, control systems collect sensor measurements and operational data from the field, process and display this information, and relay control commands to local or remote equipment. In the electric power industry they can manage and control the transmission and delivery of electric power, for example, by opening and closing circuit breakers and setting thresholds for preventive shutdowns. Employing integrated control systems, the oil and gas industry can control the refining operations on a plant site as well as remotely monitor the pressure and flow of gas pipelines and control the flow and pathways of gas transmission. In water utilities, they 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. Control system functions vary from simple to complex; they can be used to simply monitor processes—for example, the environmental conditions in a small office building—or manage most activities in a municipal water system or even a nuclear power plant.

In certain industries such as chemical and power generation, safety systems are typically implemented to mitigate a disastrous event if control and other systems fail. In addition, to guard against both physical attack and system failure, organizations may establish back-up control centers that include uninterruptible power supplies and backup generators.

There are two primary types of control systems. Distributed Control Systems (DCS) typically are used within a single processing or generating plant or over a small geographic area. Supervisory Control and Data Acquisition (SCADA) systems typically are used for large, geographically dispersed distribution operations. A utility company may use a DCS to generate power and a SCADA system to distribute it.

Figure 3 illustrates the typical components of a control system.

Figure 3: Typical Components of a Control System



Source: GAO (analysis), Art Explosion (clipart).

A control system typically consists of a "master" or central supervisory control and monitoring station consisting of one or more human-machine interfaces where an operator can view status information about the remote sites and issue commands directly to the system. Typically, this station is located at a main site along with application servers and an

engineering workstation that is used to configure and troubleshoot the other control system components. The supervisory control and monitoring station is typically connected to local controller stations through a hard-wired network or to remote controller stations through a communications network—which could be the Internet, a public switched telephone network, or a cable or wireless (e.g. radio, microwave, or Wi-Fi[4]) network. Each controller station has a Remote Terminal Unit (RTU), a Programmable Logic Controller (PLC), DCS controller, or other controller that communicates with the supervisory control and monitoring station. The controller stations also include sensors and control equipment that connect directly with the working components of the infrastructure—for example, pipelines, water towers, and power lines. The sensor takes readings from the infrastructure equipment—such as water or pressure levels, electrical voltage or current—and sends a message to the controller. The controller may be programmed to determine a course of action and send a message to the control equipment instructing it what to do—for example, to turn off a valve or dispense a chemical. If the controller is not programmed to determine a course of action, the controller communicates with the supervisory control and monitoring station before sending a command back to the control equipment. The control system also can be programmed to issue alarms back to the operator when certain conditions are detected. Handheld devices, such as personal digital assistants, can be used to locally monitor controller stations. Experts report that technologies in controller stations are becoming more intelligent and automated and communicate with the supervisory central monitoring and control station less frequently, requiring less human intervention.

Control Systems Are at Increasing Risk

Historically, security concerns about control systems were related primarily to protecting against physical attack and misuse of refining and processing sites or distribution and holding facilities. However, more recently, there has been a growing recognition that control systems are now vulnerable to cyber attacks from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and other malicious intruders.

[4]*Wi-Fi* (short for "wireless" fidelity) is the popular term for a high-frequency wireless local area network.

In October 1997, the President's Commission on Critical Infrastructure Protection specifically discussed the potential damaging effects on the electric power and oil and gas industries of successful attacks on control systems.[5] Moreover, in 2002, the National Research Council identified "the potential for attack on control systems" as requiring "urgent attention."[6] In February 2003, the President clearly demonstrated concern about "the threat of organized cyber attacks capable of causing debilitating disruption to our Nation's critical infrastructures, economy, or national security," noting that "disruption of these systems can have significant consequences for public health and safety" and emphasizing that the protection of control systems has become "a national priority."[7]

Several factors have contributed to the escalation of risk to control systems, including (1) the adoption of standardized technologies with known vulnerabilities, (2) the connectivity of control systems to other networks, (3) constraints on the implementation of existing security technologies and practices, (4) insecure remote connections, and (5) the widespread availability of technical information about control systems.

Control Systems Are Adopting Standardized Technologies with Known Vulnerabilities

Historically, proprietary hardware, software, and network protocols made it difficult to understand how control systems operated—and therefore how to hack into them. Today, however, to reduce costs and improve performance, organizations have been transitioning from proprietary systems to less expensive, standardized technologies such as Microsoft's Windows and Unix-like operating systems and the common networking protocols used by the Internet. These widely used standardized technologies have commonly known vulnerabilities, and sophisticated and effective exploitation tools are widely available and relatively easy to use. As a consequence, both the number of people with the knowledge to wage attacks and the number of systems subject to attack have increased. Also, common communication protocols and the emerging use of Extensible Markup Language (commonly referred to as XML) can make it easier for a

[5]President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (Washington, D.C.: October 1997).

[6]The National Research Council, *Making the Nation Safer: the Role of Science and Technology in Countering Terrorism* (Washington, D.C.: December 2002).

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

hacker to interpret the content of communications among the components of a control system.

Control Systems Are Connected to Other Networks

Enterprises often integrate their control systems with their enterprise networks. This increased connectivity has significant advantages, including providing decision makers with access to real-time information and allowing engineers to monitor and control the process control system from different points on the enterprise network. In addition, the enterprise networks are often connected to the networks of strategic partners and to the Internet. Furthermore, control systems are increasingly using wide area networks and the Internet to transmit data to their remote or local stations and individual devices. This convergence of control networks with public and enterprise networks potentially exposes the control systems to additional security vulnerabilities. Unless appropriate security controls are deployed in the enterprise network and the control system network, breaches in enterprise security can affect the operation of control systems.

Use of Existing Security Technologies and Practices Is Constrained

According to industry experts, the use of existing security technologies, as well as strong user authentication and patch management practices, are generally not implemented in control systems because control systems operate in real time, typically are not designed with cybersecurity in mind, and usually have limited processing 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. Because controller stations are generally designed to do specific tasks, they use low-cost, resource-constrained microprocessors. In fact, some devices in the electrical industry still use the Intel 8088 processor, introduced in 1978. Consequently, it is difficult to install existing security technologies without seriously degrading the performance of the control system.

Further, complex passwords and other strong password practices are not always used to prevent unauthorized access to control systems, in part because this could hinder a rapid response to safety procedures during an emergency. As a result, according to experts, weak passwords that are easy to guess, shared, and infrequently changed are reportedly common in control systems, including the use of default passwords or even no password at all.

In addition, although modern control systems are based on standard operating systems, they are typically customized to support control system applications. Consequently, vendor-provided software patches are generally either incompatible or cannot be implemented without compromising service by shutting down "always-on" systems or affecting interdependent operations.

Insecure Connections Exacerbate Vulnerabilities

Potential vulnerabilities in control systems are exacerbated by insecure connections. Organizations often leave access links—such as dial-up modems to equipment and control information—open for remote diagnostics, maintenance, and examination of system status. Such links may not be protected with authentication or encryption, which increases the risk that hackers could use these insecure connections to break into remotely controlled systems. Also, control systems often use wireless communications systems, which are especially vulnerable to attack, or leased lines that pass through commercial telecommunications facilities. Without encryption to protect data as it flows through these insecure connections or authentication mechanisms to limit access, there is limited protection for the integrity of the information being transmitted.

Information about Infrastructures and Control Systems Is Publicly Available

Public information about infrastructures and control systems is available to potential hackers and intruders. The availability of this infrastructure and vulnerability data was demonstrated earlier this year by a George Mason University graduate student, whose dissertation reportedly mapped every business and industrial sector in the American economy to the fiber-optic network that connects them—using material that was available publicly on the Internet, none of which was classified. Many of the electric utility officials who were interviewed for the National Security Telecommunications Advisory Committee's Information Assurance Task Force's Electric Power Risk Assessment expressed concern over the amount of information about their infrastructure that is readily available to the public.

In the electric power industry, open sources of information—such as product data and educational videotapes from engineering associations—can be used to understand the basics of the electrical grid. Other publicly available information—including filings of the Federal Energy Regulatory Commission (FERC), industry publications, maps, and material available on the Internet—is sufficient to allow someone to identify the most heavily loaded transmission lines and the most critical substations in the power grid.

In addition, significant information on control systems is publicly available—including design and maintenance documents, technical standards for the interconnection of control systems and RTUs, and standards for communication among control devices—all of which could assist hackers in understanding the systems and how to attack them. Moreover, there are numerous former employees, vendors, support contractors, and other end users of the same equipment worldwide with inside knowledge of the operation of control systems.

Cyber Threats to Control Systems

There is a general consensus—and increasing concern—among government officials and experts on control systems about potential cyber threats to the control systems that govern our critical infrastructures. As components of control systems increasingly make critical decisions that were once made by humans, the potential effect of a cyber threat becomes more devastating. Such cyber threats could come from numerous sources, ranging from hostile governments and terrorist groups to disgruntled employees and other malicious intruders. Based on interviews and discussions with representatives throughout the electric power industry, the Information Assurance Task Force of the National Security Telecommunications Advisory Committee concluded that an organization with sufficient resources, such as a foreign intelligence service or a well-supported terrorist group, could conduct a structured attack on the electric power grid electronically, with a high degree of anonymity and without having to set foot in the target nation.

In July 2002, NIPC reported that the potential for compound cyber and physical attacks, referred to as "swarming attacks," is an emerging threat to the U.S. critical infrastructure. As NIPC reports, the effects of a swarming attack include slowing or complicating the response to a physical attack. For instance, a cyber attack that disabled the water supply or the electrical system in conjunction with a physical attack could deny emergency services the necessary resources to manage the consequences—such as controlling fires, coordinating actions, and generating light.

According to the National Institute of Standards and Technology, cyber attacks on energy production and distribution systems—including electric, oil, gas, and water treatment, as well as on chemical plants containing potentially hazardous substances—could endanger public health and safety, damage the environment, and have serious financial implications, such as loss of production, generation, or distribution of public utilities; compromise of proprietary information; or liability issues. When backups

for damaged components are not readily available (e.g., extra-high-voltage transformers for the electric power grid), such damage could have a long-lasting effect.

Although experts in control systems report that they have substantiated reports of numerous incidents affecting control systems, there is no formalized process to collect and analyze information about control systems incidents. CERT/CC and KEMA, Inc. have proposed establishing a center that will proactively interact with industry to collect information about potential cyber incidents, analyze them, assess their potential impact, and make the results available to industry. I will now discuss potential and reported cyber attacks on control systems.

Control Systems Can Be Vulnerable to Cyber Attacks

Entities or individuals with malicious intent might take one or more of the following actions to successfully attack control systems:

- disrupt the operation of control systems by delaying or blocking the flow of information through control networks, thereby denying availability of the networks to control system operators;
- make unauthorized changes to programmed instructions in PLCs, RTUs, or DCS controllers, change alarm thresholds, or issue unauthorized commands to control equipment, which could potentially result in damage to equipment (if tolerances are exceeded), premature shutdown of processes (such as prematurely shutting down transmission lines), or even disabling of control equipment;
- send false information to control system operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators;
- modify the control system software, producing unpredictable results; and
- interfere with the operation of safety systems.

In addition, in control systems that cover a wide geographic area, the remote sites are often unstaffed and may not be physically monitored. If such remote systems are physically breached, the attackers could establish a cyber connection to the control network.

Department of Energy and industry researchers have speculated on how the following potential attack scenario could affect control systems in the electricity sector. Using war dialers[8] to find modem phone lines that connect to the programmable circuit breakers of the electric power control system, hackers could crack passwords that control access to the circuit breakers and could change the control settings to cause local power outages and even damage equipment. A hacker could lower settings from, for example, 500 amperes[9] to 200 on some circuit breakers; normal power usage would activate, or "trip," the circuit breakers, taking those lines out of service and diverting power to neighboring lines. If, at the same time, the hacker raised the settings on these neighboring lines to 900 amperes, circuit breakers would fail to trip at these high settings and the diverted power would overload the lines and cause significant damage to transformers and other critical equipment. The damaged equipment would require major repairs that could result in lengthy outages.

Additionally, control system researchers at the Department of Energy's national laboratories have developed systems that demonstrate the feasibility of a cyber attack on a control system at an electric power substation, where high-voltage electricity is transformed for local use. Using tools that are readily available on the Internet, they are able to modify output data from field sensors and take control of the PLC directly in order to change settings and create new output. These techniques could enable a hacker to cause an outage, thus incapacitating the substation.

The consequences of these threats could be lessened by the successful operation of any safety systems, which I discussed earlier in my testimony.

Cyber Attacks to Control Systems Have Been Reported

There have been a number of reported exploits of control systems, including the following:

- In 1998, during the two-week military exercise known as Eligible Receiver, staff from the National Security Agency used widely available tools to simulate how sections of the U.S. electric power grid's control network could be disabled through cyber attack.

[8]War dialers are simple PC programs that dial consecutive phone numbers looking for modems.

[9]An ampere is a unit of measurement for electric current.

- In the spring of 2000, a former employee of an Australian company that develops manufacturing software applied for a job with the local government, but was rejected. The disgruntled former employee reportedly used a radio transmitter on numerous occasions to remotely hack into the controls of a sewage treatment system and ultimately release about 264,000 gallons of raw sewage into nearby rivers and parks.

- In August 2003, the Nuclear Regulatory Commission confirmed that in January 2003, the Microsoft SQL Server worm—otherwise known as Slammer—infected a private computer network at the 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. Slammer reportedly also affected communications on the control networks of other electricity sector organizations by propagating so quickly that control system traffic was blocked.

Media reports have also indicated that the Blaster worm, which broke out three days before the August blackout, might have exacerbated the problems that contributed to the cascading effect of the blackout by blocking communications on computers that are used to monitor the power grid. FirstEnergy Corp., the Ohio utility that is the chief focus of the blackout investigation, is reportedly exploring whether Blaster might have caused the computer trouble that was described on telephone transcripts as hampering its response to multiple line failures.

Securing Control Systems Poses Significant Challenges

Several challenges must be addressed to effectively secure control systems against cyber threats. These challenges include: (1) the limitations of current security technologies in securing control systems; (2) the perception that securing control systems may not be economically justifiable; and (3) the conflicting priorities within organizations regarding the security of control systems.

Current Cybersecurity Technologies Have Limitations in Securing Control Systems

A significant challenge in effectively securing control systems is the lack of specialized security technologies for these systems. As I previously mentioned, the computing resources in control systems that are needed to perform security functions tend to be quite limited, making it very difficult to use security technologies within control system networks without severely hindering performance.

Although technologies such as robust firewalls and strong authentication can be employed to better segment control systems from enterprise networks, research and development could help address the application of security technologies to the control systems themselves. Information security organizations have noted that a gap exists between current security technologies and the need for additional research and development to secure control systems.

Research and development in a wide range of areas could lead to more effective technologies to secure control systems. Areas that have been noted for possible research and development include identifying the types of security technologies needed for different control system applications, determining acceptable performance trade-offs, and recognizing attack patterns for intrusion-detection systems.

Securing Control Systems May Not Be Perceived as Economically Justifiable

Experts and industry representatives have indicated that organizations may be reluctant to spend more money to secure control systems. Hardening the security of control systems would require industries to expend more resources, including acquiring more personnel, providing training for personnel, and potentially prematurely replacing current systems that typically have a lifespan of about 20 years.

Several vendors suggested that since there has been no confirmed serious cyber attack on U.S. control systems, industry representatives believe the threat of such an attack is low. Until industry users of control systems have a business case to justify why additional security is needed, there may be little market incentive for vendors to fund research to develop more secure control systems.

Organizational Priorities Conflict

Finally, several experts and industry representatives indicated that the responsibility for securing control systems typically includes two separate groups: IT security personnel and control system engineers and operators. IT security personnel tend to focus on securing enterprise systems, while control system engineers and operators tend to be more concerned with the reliable performance of their control systems. Further, they indicate that, as a result, those two groups do not always fully understand each other's requirements and collaborate to implement secure control systems.

These conflicting priorities may perpetuate a lack of awareness of IT security strategies that could be deployed to mitigate the vulnerabilities of control systems without affecting their performance. Although research

and development will be necessary to develop technologies to secure individual control system devices, IT security technologies are currently available that could be implemented as part of a secure enterprise architecture to protect the perimeter of, and access to, control system networks. These technologies include firewalls, intrusion-detection systems, encryption, authentication, and authorization.

Officials from one company indicated that, to reduce its control system vulnerabilities, it formed a team composed of IT staff, process control engineers, and manufacturing employees. This team worked collaboratively to research vulnerabilities and test fixes and workarounds.

Steps Can Be Taken to Strengthen Control System Security

Several steps can be considered when addressing potential threats to control systems, including:

- Researching and developing new security technologies to protect control systems.
- Developing security policies, guidance, and standards for control system security. For example, the use of consensus standards could be considered to encourage industry to invest in stronger security for control systems.
- Increasing security awareness and sharing information about implementing more secure architectures and existing security technologies. For example, a more secure architecture might be attained by segmenting control networks with robust firewalls and strong authentication. Also, organizations may benefit from educating management about the cybersecurity risks related to control systems and sharing successful practices related to working across organizational boundaries.
- Implementing effective security management programs that include consideration of control system security. We have previously reported on the security management practices of leading organizations.[10] Such programs typically consider risk assessment, development of appropriate policies and procedures, employee awareness, and regular security monitoring.

[10]U.S. General Accounting Office, *Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

- Developing and testing continuity plans within organizations and industries, to ensure safe and continued operation in the event of an interruption, such as a power outage or cyber attack on control systems. Elements of continuity planning typically include (1) assessing the criticality of operations and identifying supporting resources, (2) taking steps to prevent and minimize potential damage and interruption, (3) developing and documenting a comprehensive continuity plan, and (4) periodically testing the continuity plan and making appropriate adjustments.[11] Such plans are particularly important for control systems, where personnel may have lost familiarity with how to operate systems and processes without the use of control systems.

In addition, earlier this year we reviewed the federal government's critical infrastructure protection efforts related to selected industry sectors, including electricity and oil and gas.[12] We recommended that the federal government assess the need for grants, tax incentives, regulation, or other public policy tools to encourage increased critical infrastructure protection activities by the private sector and greater sharing of intelligence and incident information among these industry sectors and the federal government. In addition, we have made other recommendations related to critical infrastructure protection, including: developing a comprehensive and coordinated plan for national critical infrastructure protection; improving information sharing on threats and vulnerabilities between the private sector and the federal government, as well as within the government itself; and improving analysis and warning capabilities for both cyber and physical threats.[13] Although improvements have been made, further efforts are needed to address these challenges in implementing critical infrastructure protection.

[11]U.S. General Accounting Office, *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999).

[12]U.S. General Accounting Office, *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors*, GAO-03-233 (Washington, D.C.: February 28, 2003) and U.S. General Accounting Office, *Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats*, GAO-03-173 (Washington, D.C.: January 30, 2003).

[13]U.S. General Accounting Office, *Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues*, GAO-03-1165T (Washington, D.C.: September 17, 2003).

Government and private industry have taken a broad look at the cybersecurity requirements of control systems and have initiated several efforts to address the technical, economic, and cultural challenges that must be addressed. These cybersecurity initiatives include efforts to promote research and development activities; develop process control security policies, guidance, and standards; and encourage security awareness and information sharing. For example, several of the Department of Energy's national laboratories have established or plan to establish test beds for control systems, the government and private sector are collaborating on efforts to develop industry standards, and Information Sharing and Analysis Centers such as the Chemical Sector Cybersecurity Program (for the chemical sector) and the North American Electric Reliability Council (for the electricity sector) have been developed to coordinate communication between industries and the federal government. Attachment I describes selected current and planned initiatives in greater detail.

In summary, it is clear that the systems that monitor and control the sensitive processes and physical functions of the nation's infrastructures are at increasing risk to threats of cyber attacks. Securing these systems poses significant challenges. Both government and industry can help to address these challenges by lending support to ongoing initiatives as well as taking additional steps to overcome barriers that hinder better security.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the Subcommittee may have at this time. Should you have any further questions about this testimony, please contact me at (202) 512-3317 or at daceyr@gao.gov.

Individuals making key contributions to this testimony included Shannin Addison, Joanne Fiorino, Alison Jacobs, Elizabeth Johnston, Steven Law, David Noone, and Tracy Pierson.

Appendix I: Selected Initiatives to Improve Control System Security

Initiatives to Research and Develop Security Technologies for Control Systems

Research and development of new technologies is being performed to provide additional security options to protect control systems. Several federally funded entities have ongoing efforts to research, develop, and test new technologies.

Entity	Initiative
Sandia National Laboratories	At Sandia's SCADA Security Development Laboratory, industry can test and improve the security of its SCADA architectures, systems, and components. Sandia also has initiatives under way to advance technologies that strengthen control systems through the use of intrusion detection, encryption/authentication, secure protocols, system and component vulnerability analysis, secure architecture design and analysis, and intelligent self-healing infrastructure technology.
Idaho National Engineering and Environmental Laboratory, Sandia National Laboratories, National Energy Technology Laboratory, and other entities	Plans are under way to establish the National SCADA Test Bed, which is expected to become a full-scale infrastructure testing facility that will allow for large-scale testing of SCADA systems before actual exposure to production networks and for testing of new standards and protocols before rolling them out.
Los Alamos National Laboratory and Sandia National Laboratories	Los Alamos and Sandia have established a critical infrastructure modeling, simulation, and analysis center known as the National Infrastructure Simulation and Analysis Center. The center provides modeling and simulation capabilities for the analysis of critical infrastructures, including the electricity, oil, and gas sectors.
National Science Foundation	The National Science Foundation is considering pursuing cybersecurity research and development options related to the security of control systems.

Initiatives to Develop Process Control Security Policies, Guidance, and Standards

Several efforts to develop policies, guidance, and standards to assist in securing control systems are in progress. There are coordinated efforts between government and industry to identify threats, assess infrastructure vulnerabilities, and develop guidelines and standards for mitigating risks through protective measures. Actions that have been taken so far or are under way include the following.

Entity	Initiative
The President's Critical Infrastructure Protection Board	In February 2003, the board released the National Strategy to Secure Cyberspace. The document provides a general strategic picture, specific recommendations and policies, and the rationale for these initiatives. The strategy ranks control network security as a national priority and designates the Department of Homeland Security to be responsible for developing best practices and new technologies to increase control system security.
Instrumentation, Systems, and Automation Society	The Instrumentation, Systems, and Automation Society is composed of users, vendors, government, and academic participants representing the electric utilities, water, chemical, petrochemical, oil and gas, food and beverage, and pharmaceutical industries. It has been working on a proposed standard since October 2002. The new standard addresses the security of manufacturing and control systems. It is to provide users with the tools necessary to integrate a comprehensive security process. Two technical reports are planned for release in October 2003. One report, ISA-TR99.00.01, Security Technologies for Manufacturing and Control Systems, will describe electronic security technologies and discuss specific types of applications within each category, the vulnerabilities addressed by each type, suggestions for deployment, and known strengths and weaknesses. The other report, ISA-TR99.00.02, Integrating Electronic Security into the Manufacturing and Control Systems Environment, will provide a framework for developing an electronic security program for manufacturing and control systems, as well as a recommended organization and structure for the security plan.
Gas Technology Institute and Technical Support Working Group	Sponsored by the federal government's Technical Support Working Group, the Gas Technology Institute has researched a number of potential encryption methods to prevent hackers from accessing natural gas company control systems. This research has led to the development of an industry standard for encryption. The standard would incorporate encryption algorithms to be added to both new and existing control systems to control a wide variety of operations. This standard is outlined in the American Gas Association's report, numbered 12-1.
National Institute of Standards and Technology and National Security Agency	The National Institute of Standards and Technology and the National Security Agency have organized the Process Controls Security Requirements Forum to establish security specifications that can be used in procurement, development, and retrofit of industrial control systems. They have also developed a set of security standards and certification processes.
North American Energy Reliability Council	The North American Energy Reliability Council has established a cybersecurity standard for the electricity industry. The council requires members of the electricity industry to self-certify that they are meeting the cyber-security standards. However, as currently written, the standard does not apply to control systems.
Electric Power Research Institute	The Electric Power Research Institute has developed the Utility Communications Architecture, a set of standardized guidelines that provides interconnectivity and interoperability for utility data communication systems for real-time information exchange.

Initiatives to Encourage Security Awareness and Share Information

Many efforts are under way to spread awareness about cyber threats and control system vulnerabilities and to take proactive measures to strengthen the security of control systems. The Federal Energy Regulatory Commission, the Department of Homeland Security and other federal agencies and organizations are involved in these efforts.

Entity	Initiative
Department of Homeland Security	The Department of Homeland Security created a National Cyber Security Division to identify, analyze, and reduce cyber threats and vulnerabilities, disseminate threat warning information, coordinate incident response, and provide technical assistance in continuity of operations and recovery planning. The Critical Infrastructure Assurance Office within the Department coordinates the federal government's initiatives on critical infrastructure assurance and promotes national outreach and awareness campaigns about critical infrastructure protection.
Sandia National Laboratories, the Environmental Protection Agency, and industry groups	Sandia National Laboratories has collaborated with the Environmental Protection Agency and industry groups to develop a risk assessment methodology for assessing the vulnerability of water systems in major U.S. cities. Sandia has also conducted vulnerability assessments of control systems within the electric power, oil and gas, transportation, and manufacturing industries. Sandia is involved with various activities to address the security of our critical infrastructures, including developing best practices, providing security training, demonstrating threat scenarios, and furthering standards efforts.
North American Energy Reliability Council	Designated by the Department of Energy as the electricity sector's Information Sharing and Analysis Center coordinator for critical infrastructure protection, the North American Energy Reliability Council facilitates communication between the electricity sector, the federal government, and other critical infrastructure sectors. The council has formed the Critical Infrastructure Protection Advisory Group, which guides cybersecurity activities and conducts security workshops to raise awareness of cyber and physical security in the electricity sector. The council also formed a Process Controls subcommittee within the Critical Infrastructure Protection Advisory Group to specifically address control systems.
Federal Energy Regulatory Commission	The Federal Energy Regulatory Commission regulates interstate commerce in oil, natural gas, and electricity. The commission has published a rule to promote the capturing of critical energy infrastructure information, which may lead to increased information sharing between industry and the federal government.
Process Control Systems Cyber Security Forum	The Process Control Systems Cyber Security Forum is a joint effort between Kema Consulting and LogOn Consulting, Inc. The forum studies the cybersecurity issues surrounding the effective operation of control systems and focuses on issues, challenges, threats, vulnerabilities, best practices/lessons learned, solutions, and related topical areas for control systems. It currently holds workshops on control system cybersecurity.
Chemical Sector Cybersecurity Program	The Chemical Sector Cybersecurity Program is a forum of 13 trade associations and serves as the Information Sharing and Analysis Center for the chemical sector. The Chemical Industry Data Exchange is part of the Chemical Sector Cybersecurity Program and is working to establish a common security vulnerability assessment methodology and to align the chemical industry with the ongoing initiatives at the Instrumentation Systems and Automation Society, the National Institute of Standards and Technology, and the American Chemistry Council.

Entity	Initiative
The President's Critical Infrastructure Protection Board and Department of Energy	The President's Critical Infrastructure Protection Board and the Department of Energy developed 21 Steps to Improve the Cyber Security of SCADA Networks. These steps provide guidance for improving implementation and establishing underlying management processes and policies to help organizations improve the security of their control networks.
Joint Program Office for Special Technology Countermeasures	The Joint Program Office has performed vulnerability assessments on control systems, including the areas of awareness, integration, physical testing, analytic testing, and analysis.

GAO's Mission

The General Accounting 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 the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

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. General Accounting 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

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548