United States General Accounting Office

GAO

Report to Congressional Requesters

March 2004

CRITICAL INFRASTRUCTURE PROTECTION

Challenges and Efforts to Secure Control Systems

GAO

Accountability * Integrity * Reliability

GAO-04-354

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-04-354, a report to congressional requesters

March 2004

CRITICAL INFRASTRUCTURE PROTECTION

Challenges and Efforts to Secure Control Systems

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 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 and its Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census asked GAO to report on potential cyber vulnerabilities, focusing 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) efforts to strengthen the cybersecurity of control systems.

What GAO Recommends

GAO recommends that the Secretary of the Department of Homeland Security (DHS) develop and implement a strategy for coordinating with the private sector and other government agencies to improve control system security, including an approach for coordinating the various ongoing efforts to secure control systems. DHS concurred with GAO's recommendation.

www.gao.gov/cgi-bin/getrpt?GAO-04-354.

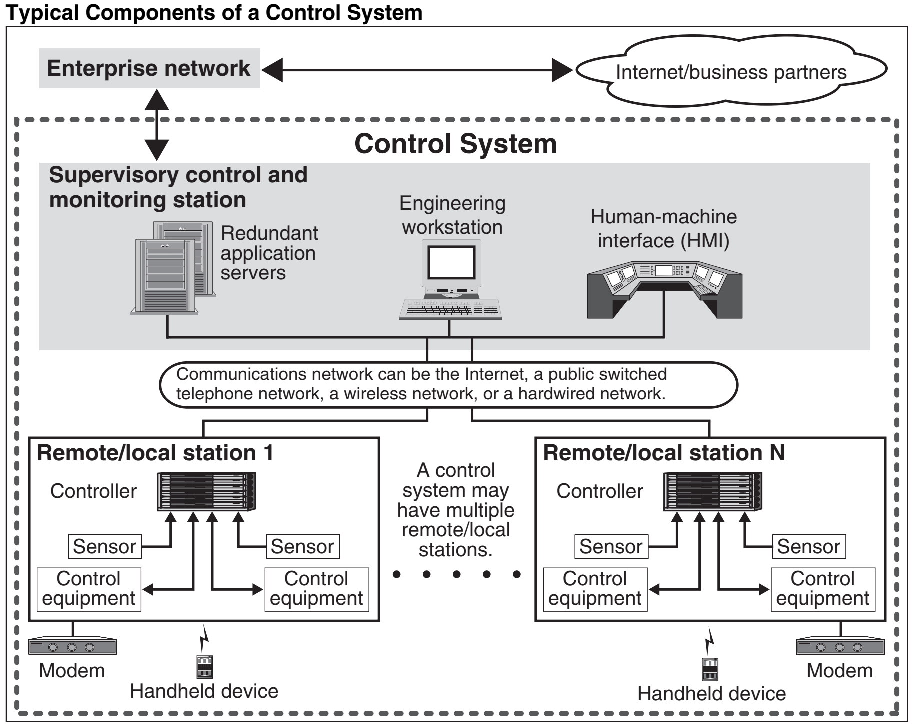
To view the full product, including the scope and methodology, click on the link above. For more information, contact Robert F. Dacey at (202) 512-3317 or daceyr@gao.gov.

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 and the increased connectivity of control systems to other systems. 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.

Securing control systems poses significant challenges, including limited specialized security technologies and lack of economic justification. The government, academia, and private industry have initiated efforts to strengthen the cybersecurity of control systems. The President's *National Strategy to Secure Cyberspace* establishes a role for DHS to coordinate with these entities to improve the cybersecurity of control systems. While some coordination is occurring, DHS's coordination of these efforts could accelerate the development and implementation of more secure systems. Without effective coordination of these efforts, there is a risk of delaying the development and implementation of more secure systems to manage our critical infrastructures.

Typical Components of a Control System



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

Contents

Table

Figures

Abbreviations

AGA	American Gas Association
ANL	Argonne National Laboratory
CERT/CC	CERT® Coordination Center
CIDX	Chemical Industry Data Exchange
CIGRE	International Council on Large Electric Systems
CIP	Critical Infrastructure Protection
CIPAG	Critical Infrastructure Protection Advisory Group
DCS	Distributed Control Systems
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
EPA	Environmental Protection Agency
EPRI	Electric Power Research Institute
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
FERC	Federal Energy Regulatory Commission
IAIP	Information Analysis and Infrastructure Protection
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISA	Instrumentation Systems and Automation Society

ISAC	Information Sharing and Analysis Center
IT	Information Technology
IT R&D	Information Technology Research and Development
JPO-STC	Joint Program Office for Special Technology Countermeasures
NCSD	National Cyber Security Division
NERC	North American Electric Reliability Council
NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSF	National Science Foundation
OEA	Office of Energy Assurance
PCIS	Partnership for Critical Infrastructure Security
PCSCS	Process Control Systems Cyber Security Forum
PCSRF	Process Controls Security Requirements Forum
PLC	Programmable Logic Controller
PNNL	Pacific Northwest National Laboratory
RAM-W	Risk Assessment Methodology–Water
RTU	remote terminal unit
SCADA	Supervisory Control and Data Acquisition
S&T	Science and Technology Directorate
TSWG	Technical Support Working Group

United States General Accounting Office
Washington, DC 20548

March 15, 2004

The Honorable Tom Davis
Chairman, Committee on Government Reform
House of Representatives

The Honorable Adam Putnam
Chairman, Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census
Committee on Government Reform
House of Representatives

Control systems—which include supervisory control and data acquisition (SCADA) systems and distributed control systems[1]—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 the risk of cyber attacks as a specific point of vulnerability in our critical infrastructures, 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."

On October 1, 2003, we testified on the cybersecurity of control systems before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census.[2] Further, your committee and subcommittee asked us to identify (1) significant cybersecurity risks

[1]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. 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.

[2]U.S. General Accounting Office, *Critical Infrastructure Protection: Challenges in Securing Control Systems*, GAO-04-140T (Washington, D.C.: Oct. 1, 2003).

associated with control systems, (2) potential and reported cyber attacks against these systems, (3) key challenges to securing control systems, and (4) efforts to strengthen the cybersecurity of control systems.

To address these objectives, we analyzed research studies and reports, as well as prior GAO reports and testimonies on critical infrastructure protection (CIP), information security, and national preparedness, among others. We analyzed documents from and met with private-sector and federal officials who had expertise in control systems and their security. Our work was performed from July to December 2003, in accordance with generally accepted government auditing standards. Appendix I contains further details on our objectives, scope, and methodology.

Results in Brief

For several years, security risks have been reported in the control systems on which many of the nation's critical infrastructures rely to monitor and control sensitive processes and physical functions. In addition to a steady increase in general cyber threats, 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 with other networks, (3) insecure remote connections, and (4) widespread availability of technical information about control systems.

Control systems can be vulnerable to a variety of types of cyber attacks that could have devastating consequences—such as endangering public health and safety; damaging the environment; or causing a loss of production, generation, or distribution by 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.

Securing control systems poses significant challenges. 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.

Government, academia, and private industry have initiated several efforts that are intended to improve the security of control systems. These initiatives include efforts to promote the research and development of new technologies, the development of requirements and standards, an increased awareness and sharing of information, and the implementation of effective security management programs. The President's *National Strategy to Secure Cyberspace* establishes a role for the Department of Homeland Security (DHS) to coordinate with the private sector and other governments to improve the cybersecurity of control systems. While some coordination is occurring, DHS's coordination of these efforts could accelerate the development and implementation of more secure systems. Without adequate coordination of these efforts, there is a risk of delaying the development and implementation of more secure systems to manage our critical infrastructures.

We are recommending that the Secretary of DHS develop and implement a strategy for coordinating with the private sector and other government agencies to improve control system security, including developing an approach for coordinating the various ongoing efforts to secure control systems. This strategy should also be addressed in the comprehensive national infrastructure plan that the department is tasked to complete by December 2004.

In providing written comments on this draft report, DHS's Undersecretary for the Information Analysis and Infrastructure Protection Directorate concurred with our recommendation (see app. III). DHS agreed that improving the security of control systems against cyberattack is a high priority. We also received technical comments from DHS that we have incorporated into the report, as appropriate.

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 an 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 systems, water supplies, 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. If not properly controlled, the speed and accessibility that create the enormous benefits of the computer age may allow individuals and organizations to 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 Infrastructures Observed by the FBI

Threat	Description
Criminal groups	There is an increased use of cyber intrusions by criminal groups who attack systems for 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, can affect the daily lives of Americans across the country.[a]
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.[3] In addition, the disgruntled organization insider is a significant threat, because these individuals often have knowledge about the organization and its system that allows them to gain unrestricted access and inflict damage or steal assets without knowing a great deal about computer intrusions. As larger 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 download tools from the Internet and literally "point and click" to start an attack. Experts agree that there has been a steady advance in the level of sophistication and effectiveness of attack technology. Intruders quickly develop attacks to exploit vulnerabilities that have been 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 networks for vulnerable systems, attack them, compromise them, and use them to spread the attack even further.

From 1995 through 2003, the CERT® Coordination Center[4] (CERT/CC) reported 12,946 security vulnerabilities that resulted from software flaws.

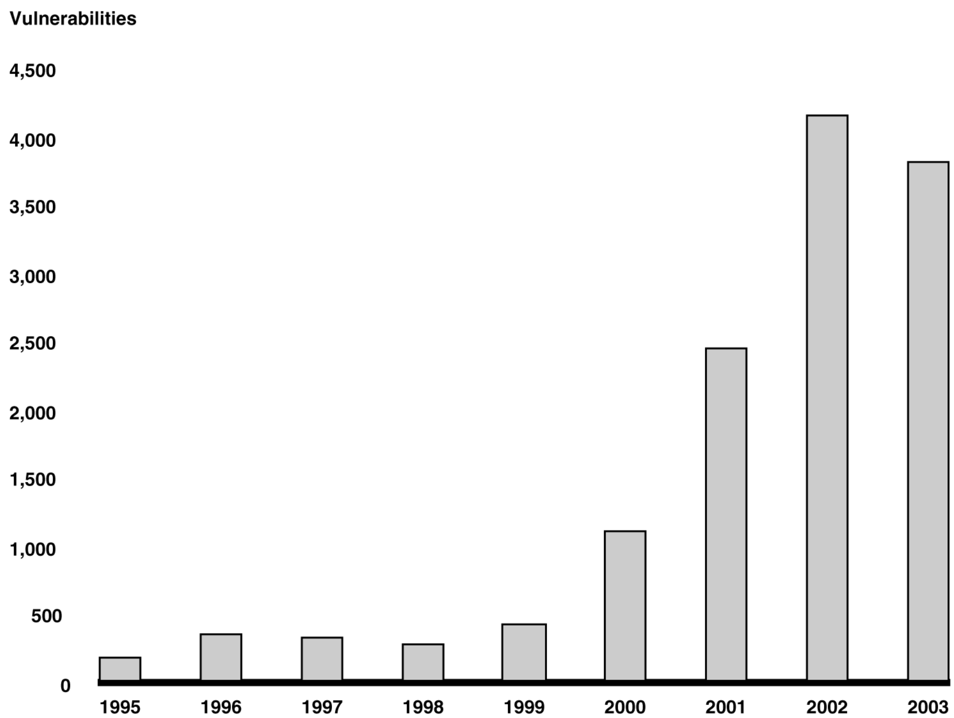
---

[3] *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.

[4] 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.

Figure 1 illustrates the dramatic growth in security vulnerabilities over these years. The growing number of known vulnerabilities increases the potential for attacks by the hacker community. Attacks can be launched against specific targets or widely distributed through viruses and worms.

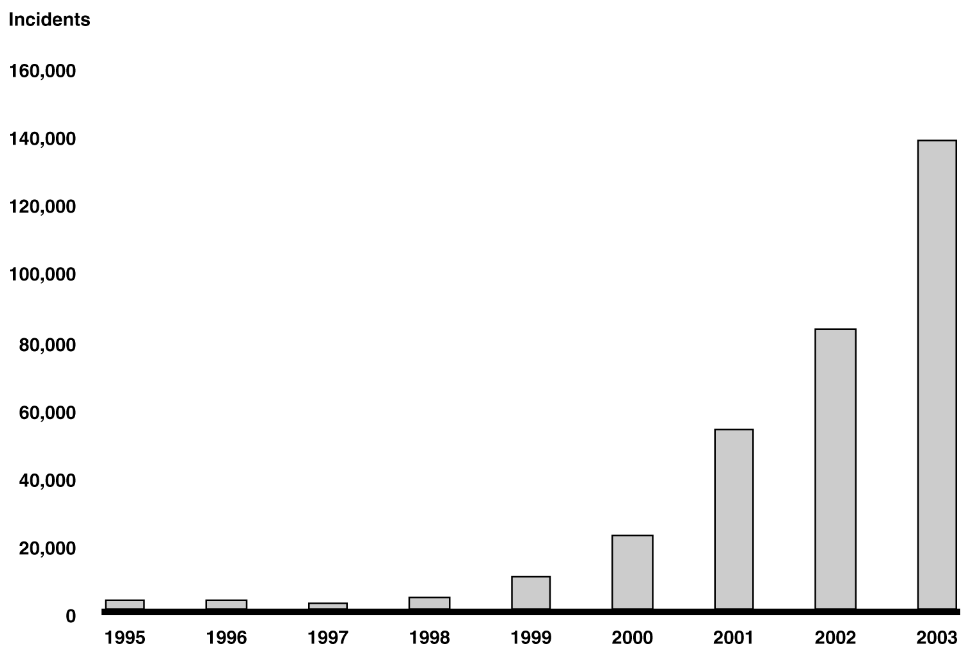
Figure 1: Security Vulnerabilities, 1995–2003



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

Along with these increasing vulnerabilities, the number of computer security incidents reported to CERT/CC has also risen dramatically—from 9,859 in 1999 to 82,094 in 2002 and to 137,529 in 2003. And these are only the reported attacks. The Director of the CERT Centers has estimated that as much as 80 percent of actual security incidents goes unreported, in most cases because (1) there were no indications of penetration or attack, (2) the organization was unable to recognize that its systems had been penetrated, or (3) the organization was reluctant to report. Figure 2 shows the number of incidents that were reported to the CERT/CC from 1995 through 2003.

Figure 2: Computer Security Incidents, 1995–2003



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

According to the National Security Agency (NSA), foreign governments already have or are developing computer attack capabilities, and potential adversaries are developing a body of knowledge about U.S. systems and methods to attack these systems. The National Infrastructure Protection Center (NIPC) reported in January 2002 that a computer belonging to an individual who had indirect links to Osama bin Laden contained computer programs that indicated that the individual was interested in the structural engineering of 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 increased. For example, in his February 2002 statement for the Senate

Select Committee on Intelligence, the Director of Central Intelligence discussed the possibility of a cyber warfare attack by terrorists.[5] He stated that the September 11 attacks demonstrated the nation's dependence on 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. James Woolsey, a former Director of Central Intelligence, shares this concern, and on October 29, 2003, in a speech before several hundred security experts, he warned that the nation should be prepared for continued terrorist attacks on our critical infrastructures. Moreover, a group of concerned scientists warned President Bush in a letter that "the critical infrastructure of the United States, including electrical power, finance, telecommunications, health care, transportation, water, defense and the Internet, is highly vulnerable to cyber attack. Fast and resolute mitigating action is needed to avoid national disaster." According to a study by a computer security organization, during the second half of 2002, the highest rates of global computer attacks were for those aimed at companies that provide critical infrastructures such as power, energy, and financial services.[6] Further, a study that surveyed over 170 security professionals and other executives concluded that, across industries, respondents believe that a large-scale cyber attack in the United States will be launched against their industry by mid-2006.

What Are Control Systems?

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. In the electric power industry, control systems can manage and control the generation, transmission, and distribution 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 at a plant site, remotely monitor the pressure and flow of gas pipelines, and

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

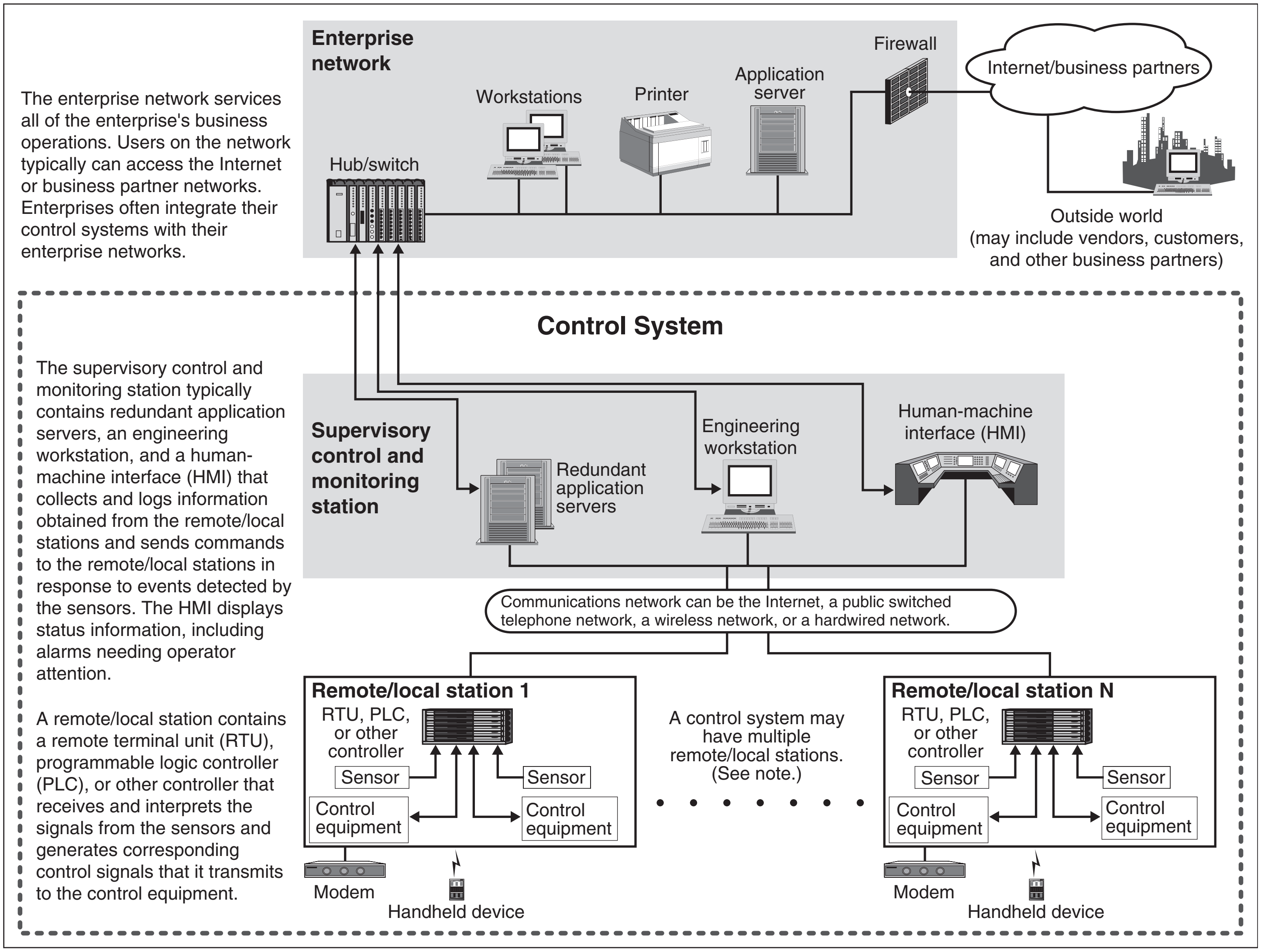
[6] Symantec, *Symantec Internet Security Threat Report: Attack Trends for Q3 and Q4 2002* (February 2003).

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. Control systems also are used in manufacturing and chemical processing. Control systems perform functions that vary from simple to complex; they can be used simply to monitor processes—for example, the environmental conditions in a small office building—or to 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 in order to mitigate a potentially disastrous event if control and other systems should fail. In addition, to guard against both physical attack and system failure, organizations may establish backup 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. For example, 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).

Note: Remote/local stations can include one or more interfaces to allow field operators to perform diagnostic and maintenance operations. Sensors can measure level, pressure, flow, current, voltages, etc., depending on the infrastructure. Control equipment can be valves, pumps, relays, circuit breakers, etc., also depending on the infrastructure.

A control system typically is made up 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/local 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 components of the control system. The supervisory control and monitoring station typically is connected to local controller stations through a hard-wired network or to a remote controller station 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[7]) network. Each controller station has a remote terminal unit (RTU), a programmable logic controller (PLC), or some other controller that communicates with the supervisory control and monitoring station.

The control system also includes sensors and control equipment that connect directly with the working components of the infrastructure—for example, pipelines, water towers, or 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 and relays instructions back to the control equipment. The control system also can be programmed to issue alarms 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 are able to communicate with the supervisory central monitoring and control station less frequently, thus requiring less human intervention.

Control Systems Are at Increasing Risk

Historically, security concerns about control systems were related primarily to protecting them against physical attack and preventing the 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.

[7]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 discussed the potential damaging effects on the electric power and oil and gas industries of successful attacks on control systems.[8] Moreover, in 2002, the National Research Council identified "the potential for attack on control systems" as requiring "urgent attention."[9] In the first half of that year, security experts reported that 70 percent of energy and power companies experienced at least one severe cyber attack. 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."[10]

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) insecure remote connections, and (4) the widespread availability of technical information about control systems.

Control Systems Are Adopting Standardized Technologies with Known Vulnerabilities

In the past, 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, 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

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

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

[10]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 creates further security vulnerabilities in control systems. Unless appropriate security controls are deployed in both the enterprise network and the control system network, breaches in enterprise security can affect the operation of control systems.

Insecure Connections Exacerbate Vulnerabilities

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. If such links are not protected with authentication or encryption, the risk increases 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 little to protect the integrity of the information being transmitted.

Information about Infrastructures and Control Systems Is Publicly Available

Public information about infrastructures and control systems is readily available to potential hackers and intruders. The availability of this infrastructure and vulnerability data was demonstrated last year by a George Mason University graduate student who, in his 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—and not classified.

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. 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 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 who have inside knowledge about the operation of control systems.

Security experts have stated that an individual with very little knowledge of control systems could gain unauthorized access to a control system with the use of a port scanning tool and a factory manual that can be easily found on the Internet and that contains the system's default password. As noted in the following discussion, many times these default passwords are never changed.

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 vital decisions that were once made by humans, the potential effect of a cyber attack becomes more devastating. 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 from 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 critical infrastructure of the United States. 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 of the physical attack—such as controlling fires, coordinating response, and generating light.

According to the National Institute of Standards and Technology (NIST), 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 by 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.

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 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 often are not staffed and may not be physically monitored. If such remote systems are physically breached, attackers could establish a cyber connection to the control network.

Department of Energy (DOE) and industry researchers have speculated on how the following potential attack scenario could affect control systems in the electricity sector. Using war dialers[11] to find modems connected 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[12] to 200 on some circuit breakers; normal power usage would then 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.

Control system researchers at DOE'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.

Experts in the water industry consider control systems to be among the primary vulnerabilities of drinking water systems. A technologist from the water distribution sector has demonstrated how an intruder could hack into the communications channel between the control center of a water distribution pump station and its remote units, located at water storage and pumping facilities, to either block messages or send false commands to the remote units. Moreover, experts are concerned that terrorists could,

[11]War dialers are simple personal computer programs that dial consecutive phone numbers looking for modems.

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

for example, trigger a cyber attack to release harmful amounts of water treatment chemicals, such as chlorine, into the public's drinking water.

Cyber Attacks on Control Systems Have Been Reported

Experts in control systems have verified numerous incidents that have affected control systems. Reported attacks include the following:

- In 1994, the computer system of the Salt River Project, a major water and electricity provider in Phoenix, Arizona, was breached.
- In March 1997, a teenager in Worcester, Massachusetts, remotely disabled part of the public switching network, disrupting telephone service for 600 residents and the fire department and causing a malfunction at the local airport.
- 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. Over a 2-month period, the disgruntled rejected employee reportedly used a radio transmitter on as many as 46 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 the spring of 2001, hackers mounted an attack on systems that were part of a development network at the California Independent System Operator, a facility that is integral to the movement of electricity throughout the state.
- 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 at least five other utilities by propagating so quickly that control system traffic was blocked.

In addition, in 1997, the Department of Defense (DOD) undertook the first systematic exercise to determine the nation's and DOD's vulnerability to cyberwar. During a 2-week military exercise known as Eligible Receiver, staff from NSA used widely available tools to show how to penetrate the control systems that are associated with providers of electric power to DOD installations. Other assessments of control systems at DOD installations have demonstrated vulnerabilities and identified risks in the installations' network and operations.

Securing Control Systems Poses Significant Challenges

The control systems community faces several challenges to securing 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.

Lack of Specialized Security Technologies for Control Systems

According to industry experts, existing security technologies, as well as strong user authentication and patch management practices, are generally not implemented in control systems because control systems usually have limited processing capabilities, operate in real time, and are typically not designed with cybersecurity in mind.

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 fact, some control system devices still use the Intel 8088 processor, which was introduced in 1978. Consequently, it is difficult to install current security technologies without seriously degrading the performance of the control system.

For example, 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 may be either 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. Another constraint on deploying patches is that support agreements with control system vendors often require the vendor's approval before the user can install patches. If a patch is installed in violation of the support agreement, the vendor will not take responsibility for potential impacts on the operations of the system. Moreover, because a control system vendor often requires that it be the sole provider of patches, if the vendor delays in providing patches, systems remain vulnerable without recourse.

Information security organizations have noted that a gap exists between currently available 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. For example, although technologies such as robust firewalls and strong authentication can be employed to better segment control systems from external networks, research and development could help to address the application of security technologies to the control systems themselves. Other 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 use in intrusion detection systems.

Industry experts have identified challenges in migrating system components to newer technologies while maintaining uninterrupted operations. Upgrading all the components of a control system can be a lengthy process, and the enhanced security features of newly installed technologies—such as their ability to interpret encrypted messages—may not be able to be fully utilized until all devices in the system have been replaced and the upgrade is complete.

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, which typically have a lifespan of about 20 years.

Several vendors suggested that since there have been no reports of significant disruptions caused by cyber attacks on U.S. control systems, industry representatives believe the threat of such an attack is low. While incidents have occurred, to date there is no formalized process for collecting and analyzing information about control systems incidents, thus further contributing to the skepticism of control systems vendors. 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.[13] As we discuss in appendix II, establishing such a process is currently under study.

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. We have previously reported that consideration of further federal government efforts is needed to provide appropriate incentives for nonfederal entities to enhance their efforts to implement CIP—including protection of control systems. Without appropriate consideration of public policy tools, such as regulation, grants, and tax incentives, private-sector participation in sector-related CIP efforts may not reach its full potential.[14]

Organizational Priorities Conflict

Finally, several experts and industry representatives indicated that the responsibility for securing control systems typically includes two separate groups: (1) IT security personnel and (2) 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. These experts indicate that, as a result, those two groups do not always fully understand each other's requirements and so may not 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, existing IT security technologies and approaches could be implemented as part of a secure enterprise architecture to protect the perimeters of, and access to, control system networks. Existing IT security technologies include firewalls, intrusion-

[13]U.S. General Accounting Office, *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors*, GAO-03-233 (Washington, D.C.: Feb. 28, 2003).

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

detection systems, encryption, authentication, and authorization. IT security approaches include segmenting control system networks and testing continuity plans to ensure safe and continued operation.

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

Efforts to Strengthen the Cybersecurity of Control Systems Under Way, but Lack Adequate Coordination

Government, academia, and private industry have independently initiated multiple efforts and programs focused on some of the key areas that should be addressed to strengthen the cybersecurity of control systems. Appendix II describes initiatives to secure control systems in greater detail. These key areas—and illustrative examples of ongoing efforts in these areas—include the following:

- **Research and development of new security technologies to protect control systems**. Both federal and nonfederal entities have initiated efforts to develop encryption methods for securing communications on control system networks and field devices. Moreover, DOE is planning to establish a National SCADA Test Bed to test control system vulnerabilities.

- **Development of requirements and standards for control system security**. Several entities are working to develop standards that increase the security of control systems. The Process Controls Security Requirements Forum (PCSRF), established by NIST and NSA, is working to define a common set of information security requirements for control systems. In addition, the North American Electric Reliability Council (NERC) is preparing to draft a standard that will include security requirements for control systems.

- **Increased awareness of security and sharing of information about the implementation of more secure architectures and existing security technologies**. To promote awareness of control system vulnerabilities, DOE has created security programs, trained teams to conduct security reviews, and developed cybersecurity courses. The Instrumentation Systems and Automation Society (ISA) has reported on the known state of the art of cybersecurity technologies as they are applied to the control systems environment, to clearly define what technologies can currently be deployed.

- **Implementation of effective security management programs, including policies and guidance that consider control system security**. Both federal and nonfederal entities have developed guidance to mitigate the security vulnerabilities of control systems. DOE's *21 Steps to Improve Cyber Security of SCADA Networks* provides guidance for improving the security of control systems and establishing underlying management processes and policies to help organizations improve the security of control system networks.

  In previous reports, we have recommended the development of a comprehensive and coordinated national plan to facilitate the federal government's CIP efforts. This plan should clearly delineate the roles and responsibilities of federal and nonfederal CIP entities, define interim objectives and milestones, set time frames for achieving objectives, and establish performance measures.

  The President in his homeland security strategies and Congress in enacting the Homeland Security Act designated DHS as responsible for developing a comprehensive national infrastructure plan. The plan is expected to inform DHS on budgeting and planning for CIP activities and on how to use policy instruments to coordinate among government and private entities to raise the security of our national infrastructures to appropriate levels. According to Homeland Security Presidential Directive 7 (HSPD 7), issued December 17, 2003, DHS is to develop this formalized plan by December 2004.

  In February 2003, the President's *National Strategy to Secure Cyberspace* established a role for DHS to coordinate with other government agencies and the private sector to improve the cybersecurity of control systems. DHS's recommended role includes:

- ensuring that there is broad awareness of the vulnerabilities in control systems and the consequences of exploiting these vulnerabilities,

- developing best practices and new technologies to strengthen the security of control systems, and

- identifying the nation's most critical control system sites and developing a prioritized plan for ensuring cyber security at those sites.

  In addition, the President's strategy recommends that DHS work with the private sector to promote voluntary standards efforts and the creation of security policy for control systems.

DHS recently began to focus on the range of activities that are under way among the numerous entities that are working to address these areas. In October 2003, DHS's Science and Technology Directorate initiated a study to determine the current state of security of control systems. In December 2003, DHS established the Control Systems Section within the Protective Security Division of its Information Analysis and Infrastructure Protection (IAIP) Directorate. The objectives of this section are to identify computer-controlled systems that are vital to infrastructure functions, evaluate the potential threats to these systems, and develop strategies that mitigate the consequences of attacks. In addition, IAIP's National Cyber Security Division (NCSD) is currently planning to develop a methodology for conducting cyber assessments across all critical infrastructures, including control systems. The objectives of this effort include defining specific goals for the assessments and, based on their results, developing sector-specific recommendations to mitigate vulnerabilities. They also plan to examine processes, technology, and available policy, procedures, and guidance. Because these efforts have only recently been initiated, DHS has not yet developed a strategy for implementing the functions mentioned above.

As previously discussed, many government and nongovernment entities are spearheading various initiatives to address the challenge of implementing cybersecurity for the vital systems that operate our nation's critical infrastructures. While some coordination is occurring, both federal and nonfederal control systems experts have expressed their concern that these efforts are not being adequately coordinated among government agencies, the private sector, and standards-setting bodies. DHS's coordination of these efforts could accelerate the development and implementation of more secure systems to manage our critical infrastructures. In contrast, insufficient coordination could contribute to

- delays in the general acceptance of security requirements and the adoption of successful practices for control systems,
- failure to address gaps in the research and development of technologies to better secure control systems,
- impediments to standards-creating efforts across industries that could lead to less expensive technological solutions, and
- reduced opportunities for efficiency that could be gained by leveraging ongoing work.

Conclusions

The systems that monitor and control the sensitive processes and physical functions of the nation's critical infrastructures are at increasing risk from threats of cyber attacks. Securing these systems poses significant challenges. Numerous federal agencies, critical infrastructure sectors, and standards-creating bodies are leading various initiatives to address these challenges. While some coordination is occurring, the cybersecurity of our critical infrastructures' control systems could benefit from greater collaboration among all entities. DHS's implementation of its responsibilities outlined in the *National Strategy to Secure Cyberspace* as well as the coordination of ongoing efforts among the government, industries, and standards-creating bodies could accelerate progress in securing these critical systems.

Recommendation for Executive Action

We recommend that the Secretary of the Department of Homeland Security develop and implement a strategy for coordinating with the private sector and other government agencies to improve control system security, including an approach for coordinating the various ongoing efforts to secure control systems. This strategy should also be addressed in the comprehensive national infrastructure plan that the department is tasked to complete by December 2004.

Agency Comments

DHS's Under Secretary for IAIP transmitted the department's written comments on a draft of this report (see app. III). In his written comments, the Under Secretary concurred with our recommendation and stated that DHS agrees that improving the security of control systems against cyberattack is a high priority. He stated that DHS has engaged with the private sector, academia, and other government entities on this matter as required by HSPD 7. The Under Secretary further noted that DHS is utilizing IAIP's Protective Services Division and NCSD collectively to address both the physical and cyber aspects of control systems security. We also received technical comments from DHS that we have incorporated into the report, as appropriate.

As agreed with your staff, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the date of this report. At that time, we will send copies of this report to other interested congressional committees and the heads of the agencies discussed in this report, as well as to the private-sector participants and other relevant agencies. We will also make copies available to others upon request. In addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov.

Should you or your offices have questions on matters discussed in this report, please contact me at (202) 512-3317 or Elizabeth Johnston, Assistant Director, at (202) 512-6345. We can also be reached by e-mail at daceyr@gao.gov or johnstone@gao.gov, respectively. Key contributors to this report were Shannin Addison, Joanne Fiorino, Alison Jacobs, and Tracy Pierson.

Robert F. Dacey
Director, Information Security Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to assess (1) the 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) efforts to strengthen the cybersecurity of control systems.

We analyzed research studies and reports as well as prior GAO reports and testimonies on critical infrastructure protection (CIP) information security, and national preparedness, among others, to obtain information regarding the risks and vulnerabilities of control systems. We analyzed documents from and met with manufacturers, users, and federal officials with expertise in control systems and their security to identify the challenges to securing control systems. Finally, we analyzed documents from and met with representatives from control systems manufacturing companies, industry users, and federal officials from the Departments of Homeland Security, Defense, and Energy, to identify ongoing initiatives to strengthen the security of control systems. We also reviewed and analyzed technical reports by standards groups to assess the status of efforts to develop guidance and standards for securing control systems.
Our work was conducted from July 2003 to December 2003, in accordance with generally accepted government auditing standards.

Appendix II: Initiatives to Address Cybersecurity Challenges of Control Systems

Following are key initiatives that are aimed at strengthening the security of control systems. They are led by government, academia, and private industry.

Department of Homeland Security

The Department of Homeland Security (DHS) has created a National Cyber Security Division (NCSD) within its Information Analysis and Infrastructure Protection (IAIP) Directorate 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. IAIP coordinates the federal government's initiatives on critical infrastructure assurance and promotes national outreach and awareness campaigns about CIP. On the basis of work conducted by the U.S.-Canada Power Outage Task Force, NCSD is currently in the process of creating a series of recommended preventive measures to better secure the control systems that manage North America's electric power grid.

In October 2003, DHS's Science and Technology Directorate (S&T) initiated a study of the nation's critical infrastructures to determine which sectors use control systems, what cybersecurity risks they face, and which industry players are focusing on mitigating these risks. The study, which focuses on control system security, will reach out to two or three representatives from each sector in an attempt to determine what items to include in DHS S&T's research agenda. In addition, S&T recently issued a solicitation to small businesses seeking research proposals for projects focusing on securing control systems. The objectives of this program will be to (1) develop a concept and formal design to better protect SCADA systems by reducing their vulnerabilities to cyber and physical attacks across industry sectors, (2) test the design, and (3) refine the design and perform qualification tests to validate the design and its performance.

In December 2003, DHS established the Control Systems Section within the Protective Security Division of its IAIP Directorate. The objectives of this section are to identify computer-controlled systems that are vital to critical infrastructure functions, evaluate the potential threats to these systems, and develop strategies that can mitigate the consequences of attacks.

IAIP's NCSD is currently planning to develop a methodology for conducting cyber assessments across all critical infrastructures, including control systems. The objectives of this effort include defining specific goals for the assessments and, based on results, developing sector-specific recommendations to mitigate vulnerabilities. NCSD also plans to examine processes, technology, and available policy, procedures, and guidance. NCSD has identified a number of its additional efforts, including recently hiring personnel with expertise in control systems.

Department of Defense

The Department of Defense's (DOD) Joint Program Office for Special Technology Countermeasures (JPO-STC) has performed vulnerability assessments on control systems, including the areas of awareness, integration, physical testing, analytic testing, and analysis. JPO-STC coordinates its assessments with those performed by the U.S. Army's First Information Operations Command. The Army's assessments are conducted as part of installation assessments to (1) analyze potential risks to the installation network from SCADA infrastructures and (2) assess the vulnerabilities of SCADA systems that could negatively affect installation operations.

Department of Energy

Under the sponsorship of the Department of Energy's (DOE) Office of Energy Assurance (OEA), the National Laboratories have conducted studies of the vulnerabilities of the control systems that are used in the nation's critical infrastructures, and they have developed guidance to help mitigate some of these vulnerabilities. In September 2002, DOE and the President's Critical Infrastructure Protection Board released *21 Steps to Improve Cyber Security of SCADA Networks*. These steps provide guidance for improving the security of control systems and establishing underlying management processes and policies to help organizations improve the security of their control networks. Moreover, OEA is creating the DOE Critical Infrastructure Security Standards Working Group to accelerate the implementation and quality of security standards for those systems that control the energy infrastructure. This working group is also charged with the responsibility of facilitating, coordinating, leveraging, influencing, and leading industrial and government standards-setting activities. We describe in the next section the specific activities related to securing control systems that DOE sponsors at the National Laboratories.

Idaho National Engineering and Environmental Laboratory, Sandia National Laboratories, and National Energy Technology Laboratory

Plans are under way to establish the National SCADA Test Bed, which will be used to facilitate research by testing control system vulnerabilities and proposed hardware and software security features. By teaming with industry, the test bed is expected to become a full-scale infrastructure testing facility for control systems that will allow for testing and validating industry products including computer controls, communications, and field systems; developing new tools to determine the vulnerabilities of control systems; and testing new standards and protocols. Initially focused on the electricity sector, the test bed will now also include the oil and natural gas pipelines sectors. There are plans to include other federal agencies in test bed activities in the future. Funding constraints have delayed the implementation of the initial phases of the plans.

Pacific Northwest National Laboratory

According to DOE, the Pacific Northwest National Laboratory (PNNL) has been integrally involved since 1994 in DOE activities that are associated with CIP—including leading an Electric Power Research Institute research project to characterize the cybersecurity of electric utility systems; providing technical input to the President's Commission on Critical Infrastructure Protection in 1996; starting a multilaboratory vulnerability assessment program in 1997; and participating on the DOE Critical Infrastructure Protection Task Force in 1998. These efforts draw from expertise working with the electric utility industry, which was later embodied in the formation of the North American Electric Reliability Council (NERC) Critical Infrastructure Protection Forum in 2000. PNNL supports a variety of clients that are involved in the security of control systems.

Sandia National Laboratories

For the last six years, Sandia has been involved in various activities to address the security of control systems in our critical infrastructures. Laboratory employees are creating methodologies for assessing risks and have performed vulnerability assessments of control systems within the electric power, oil and gas, transportation, water/wastewater, nuclear power, and manufacturing industries. To promote awareness of control system vulnerabilities, Sandia's staff has created security programs, trained teams to conduct security reviews, developed a threat scenario demonstration system, and developed cybersecurity courses to train those involved in the operation and protection of critical infrastructures. Sandia is also working with standards bodies to include information security in communications protocols.

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.

Argonne National Laboratory

According to DOE, staff at Argonne National Laboratory (ANL) are conducting vulnerability assessments of control systems in the oil and gas industry. ANL is also developing a database that includes information from the vendor and user communities in the various energy sectors regarding the different control system operating systems, and it is evaluating these operating systems to determine their vulnerabilities. The lab is cataloguing various control system failures and their impacts and evaluating them for correlations in order to gather requirements that can be turned into solutions.

Los Alamos National Laboratory

In collaboration with Sandia, Los Alamos has established the National Infrastructure Simulation and Analysis Center, which provides modeling and simulation capabilities for the analysis of critical infrastructures, including the electricity, oil, and gas sectors. Under the Homeland Security Act, the functions of the center were transferred to DHS.

Environmental Protection Agency

Sandia National Laboratories has also collaborated with the Environmental Protection Agency (EPA) and industry groups to develop a risk assessment methodology for assessing the vulnerability of water systems in major U.S. cities.

In June 2000, the American Water Works Association Research Foundation, in collaboration with Sandia, began a project to develop a vulnerability assessment methodology for utilities to use to assess the physical and cyber vulnerabilities of their infrastructures and develop plans to minimize the risks they identify. The first version of the *Risk Assessment Methodology–Water* (RAM-W) was released in November 2001.

In addition, EPA has provided vulnerability assessment training to many water utilities. In accordance with EPA's water security strategy, security vulnerability self-assessment guides for systems serving fewer than 100,000 people have been issued.

All water systems serving more than 3,300 users are required by law[1] to conduct assessments of their water facilities against the threat of sabotage or other malicious acts. These water systems are also required to prepare or revise an emergency response plan incorporating the results of the assessment within 6 months of its completion. EPA is responsible for ensuring that the water systems have met these requirements.

Food and Drug Administration

In August of 1997, part 11 of Title 21 of the Code of Federal Regulations (21 CFR part 11) became effective. It provides criteria for the use of electronic records and electronic signatures in complying with the Food and Drug Administration's (FDA) reporting requirements for all agencies covered by FDA. In addition, the regulations require companies to limit system access to authorized individuals, use authority checks, and enforce appropriate controls over systems documentation.

The food and pharmaceutical industries use control systems in their manufacturing processes—for example, to track information about products, including histories of operator actions, process measurement, raw materials used, and equipment status, and to generate reports based on this information. Therefore, to ensure the security of this vital information, 21 CFR part 11 requires the authentication of electronic signatures and electronic records in systems used in these industries, including control systems.

[1]The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (P.L. 107-188, June 12, 2002) amended the Safe Drinking Water Act to require each community water system serving more than 3,300 individuals to conduct an assessment of the system's vulnerability to terrorist attacks or other deliberate acts to compromise a safe and dependable drinking water supply. Under the law, EPA is to develop protocols to protect the assessments from unauthorized disclosure. The law also establishes deadlines, based on system size, for these systems to certify to EPA that they have conducted a vulnerability assessment and to submit to EPA a copy of the assessment.

National Institute of Standards and Technology and National Security Agency

The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) have organized the Process Controls Security Requirements Forum (PCSRF) to establish security specifications that can be used in the procurement, development, and retrofit of industrial control systems. PCSRF's membership includes representatives from the water, electric, chemical, and petrochemical industries; U.S. government laboratories and organizations; and vendors of control systems.

PCSRF's 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. This work will be based on NIST's and NSA's work to develop the Common Criteria standard (ISO 15408) for IT security evaluation. In addition, the forum has created and is currently using a process control cybersecurity test bed to validate standards for control system security. The forum also plans to develop protection profiles from the security requirements that new industrial control systems and equipment will be built to. PCSRF is working to collaborate with other existing activities such as the Instrumentation Systems and Automation Society's efforts to establish standards and recommended practices for implementing secure control systems.

Technical Support Working Group

The multiagency Technical Support Working Group (TSWG) is supporting several projects that are aimed at enhancing the securing of control systems. One project, the SCADA Security Kit, would develop a self-help security kit (e.g., checklist and operator guide) and a CD/video training program. This project has been approved, but it is not yet funded. In addition, TSWG continues to sponsor the work being conducted by the gas industry to develop an encryption standard, which we discuss in more detail later. TSWG is also working with DHS, DOE, and NIST to further develop aspects of the National Test Bed.

National Science Foundation

The National Science Foundation (NSF) is studying research and development areas related to the security of control systems in order to decide which ones to pursue.

In September 2002, NSF, in collaboration with the White House Office of Science and Technology Policy, organized a workshop to gather industry input about long-term research needs for CIP. A particular focus of the workshop was on securing control systems. Participants from academia, industry, and government conducted a research needs assessment of security technologies. The recommendations resulting from this workshop are expected to lead to a research and development road map for secure control systems. Examples of topics in this road map are (1) architectures and systems concepts for authority management and (2) adaptation of security technologies such as encryption, authentication, and intrusion detection for real-time control.

In October 2003, NSF sponsored a workshop to explore the information infrastructure vulnerabilities of control systems. The workshop brought together a multidisciplinary team of experts on SCADA and IT from industry, academia, and government to identify both the near-term technology solutions and the longer-term research needed to secure the nation's infrastructure. The output of the workshop is a set of four prioritized, cross-cutting research and development topics: (1) standards and methodology, (2) modeling and analysis, (3) next generation platforms, and (4) automated sensing of infrastructure anomalies. In addition, follow-on activities were recommended to drive the development solutions and their transfer to our critical infrastructures.

Finally, on December 3, 2003, NSF announced a new program that will fund up to three research center-level collaborations between industry and academia, as well as individual and team awards to foster ideas and train people in cybersecurity to protect the nation's critical infrastructures.

National Academies

The National Academies established a committee of the nation's top engineering, medical, scientific, and policy experts to help the federal government use science and technology strategically to develop a counterterrorism program plan. Shortly after the September 11 attacks, the committee began identifying current threats to the United States, researching the most common vulnerabilities to these threats, and determining strategic opportunities for science and technology to contribute to combating terrorism in both the short and long terms. The committee's study evolved into the report *Making the Nation Safer: the Role of Science and Technology in Countering Terrorism*, published in September 2002.

Interagency Working Group on Information Technology Research and Development

In November 2002, the Interagency Working Group on Information Technology Research and Development (IT R&D) of the National Science and Technology Council, Executive Office of the President, charged the Networking and IT R&D Grand Challenges Task Force with identifying a set of science, engineering, and societal challenges that will require innovations in IT R&D. High Confidence Infrastructure Control Systems is one of the 16 grand challenges that the task force identified.

North American Electric Reliability Council

Designated by DOE as the electricity sector's information sharing and analysis center (ISAC) coordinator for CIP, the North American Electric Reliability Council (NERC) receives security data from the electricity sector; analyzes the data with input from DHS, other federal agencies, and other critical infrastructure sector ISACs; and disseminates threat indications, analyses, and warnings. NERC has also formed the Critical Infrastructure Protection Advisory Group (CIPAG), which guides security activities and conducts security workshops to raise the awareness of cyber and physical security in the electricity sector. A Process Control Systems Security Task Force within CIPAG specifically addresses the security of electricity control systems.

In response to the Federal Energy Regulatory Commission's June 2002 *Standard Market Design* notice of public rulemaking, which included cybersecurity standards for the electricity sector, the NERC board of trustees adopted a 1-year urgent action Cyber Security Standard on August 13, 2003. The intent of this cybersecurity standard is to provide a minimal level of assurance that key entities responsible for the reliability of the bulk electric systems of North America—specifically, reliability coordinators and control area operators—identify and protect critical cyber assets that control or could impact the reliability of their systems. The standard includes such requirements as policies, controls, physical security, training, and recovery plans. However, it does not apply to control systems or electronic relays (i.e., RTUs or PLCs) that are installed in generation plants, transmission substations, or distribution substations. NERC is currently preparing a standards authorization request (i.e., a scope document), that will be used to solicit NERC board approval to begin drafting of the permanent standard. A number of industry organizations expect that this will require the compliance of control systems and electronic relays. Members of the NERC Balloting Body, made up of representatives of electricity organizations from each of the 10 NERC regions, will be able to vote on the draft standard, and, if they approve it, the board of trustees will vote to adopt it. A NERC representative estimates that the permanent standard would not be formally adopted until 2005. For compliance purposes, the standard is not expected to apply to electricity distribution assets or organizations.

Electric Power Research Institute

The Electric Power Research Institute (EPRI) has released *Scoping Study on Security Processes and Impacts*, a guide to help utilities identify vulnerabilities in their communications systems and link their associated risks to appropriate levels of security countermeasures. In addition, EPRI has launched mock attacks on the control systems of electric utilities to probe for weaknesses and has subsequently provided utilities with reports on their own potential vulnerabilities. EPRI has also provided other members with reports on their potential vulnerabilities and insights on security best practices. The institute is also working on a method to protect the SCADA network directly by identifying anomalous commands that are caused by malicious activities or human error in time to allow operators to take corrective action. EPRI next plans to partner with a major computer vendor to develop ways to secure grid communications, such as by encrypting data at both the control-system network and field-device levels.

International Council on Large Electric Systems

The International Council on Large Electric Systems (CIGRE) is a nonprofit international association based in France. It has established several study committees to promote and facilitate the international exchange of knowledge in the electrical industry by identifying best practices and developing recommendations. Three of its study committees focus on control systems. The objectives of the Substations Committee include the adoption of technological advances in equipment and systems to achieve increased reliability and availability. The System Operation and Control Committee focuses on the technical capabilities needed for the secure and economical operation of existing power systems, and it includes within its scope functionalities to assess security, which support control centers and operators. The Information Systems and Telecommunication for Power Systems Committee monitors emerging technologies in the industry and evaluates their possible impact. In addition, it focuses on the security requirements of the information systems and services of control systems. The technical activities of these committees are carried out by working groups that produce reports and technical brochures for publication.

The Oil Pipeline Industry

The oil pipeline industry is currently developing an industry standard for the protection of control functions and control systems. This standard will focus on communications including the confidentiality of protocols, encryption of data, and access controls such as firewall services and intrusion detection systems. According to a representative from the oil pipeline industry, the standard will provide guidance on managing the sharing of SCADA information while maintaining security, including defining information classification levels and control of access. It will address how to provide for the interchange of data.

In addition, the industry is working on issues related to standards for control systems with other organizations, such as the American Gas Association, the Instrument Society of America, and the Institute of Electrical and Electronics Engineers.

Gas Technology Institute and American Gas Association

Sponsored by the federal government's Technical Support Working Group, the Gas Technology Institute and the American Gas Association (AGA) have researched a number of potential encryption methods to prevent hackers from accessing natural gas companies' control systems. This research has led to the development of a proposed industry standard for encryption. The proposed standard provides energy utilities with a set of standards for protocols, equipment, and procedures to protect the transmission of control systems communications through the data transfer process. Efforts to develop this standard have been under way since October 2001. According to the department head of gas supply operations at AGA, the testing and final release of the proposed standard is targeted for the second quarter of 2004.

Chemical Sector Cybersecurity Program

The Chemical Sector Cybersecurity Program is a forum of 13 trade associations and serves as the ISAC for the chemical sector. Part of this program, the Chemical Industry Data Exchange (CIDX), has established the Cyber-Security Practices, Standards and Technology Initiative to identify immediate opportunities to improve the base level of cybersecurity within the chemical industry. The objective of this initiative is to address the practices and standards for both business systems and manufacturing control systems.

In May of 2003, CIDX completed and issued the first version of its *Guidance for Directing Cybersecurity in the Chemical Sector*. In coordinating with prior work that had been issued by the American Chemistry Council, this guidance provides information on cybersecurity applicability, sample strategies, and available resources. Currently, this document focuses on the security of business systems rather than control systems; however, in the near future, CIDX plans to incorporate issues specific to control systems in this document. In addition, CIDX has plans to start developing prescriptive guidance regarding the risk level for control systems.

In September of 2003, CIDX issued an additional guidance document, *Cybersecurity Vulnerability Assessment Methodology Guidance*. This document compares several methodologies for assessing cybersecurity vulnerabilities. The objective was to find one methodology that performed well in addressing cybersecurity for both business systems and control systems; however, it was discovered that while a given methodology may work well for either the business environment or control systems, it may not work well for both. In addition, CIDX is working to align the chemical industry's initiatives to enhance the security of control systems with the ongoing initiatives at the Instrumentation Systems and Automation Society, NIST, and the American Chemistry Council.

Instrumentation Systems and Automation Society

The Instrumentation Systems and Automation Society's (ISA) Manufacturing and Control Systems Security Standards Committee (also referred to as the SP99 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 is working to establish standards and recommended practices, write technical reports, and develop other information that will define procedures and methodologies for developing, assessing, and implementing effective security practices for manufacturing and control systems and for assessing cybersecurity performance. The committee's guidance is directed toward those responsible for designing, implementing, or managing control systems, as well as toward users, system integrators, security practitioners, and control systems manufacturers and suppliers. Its focus is on improving the confidentiality, integrity, and availability of control systems and their components and providing criteria for procuring and implementing secure control systems.

Two technical reports are expected to be released in March of this year. The first report, *Security Technologies for Manufacturing and Control Systems* (ISA-TR99.00.01), is intended to document the known state of the art 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. The purpose of the second report, *Integrating Electronic Security into the Manufacturing and Control Systems Environment* (ISA-TR99.00.02), is to present a consistent approach for developing, implementing, and operating a program that addresses security for control systems. Plans have been made to create a joint project team with ISA and the International Electrotechnical Commission (IEC) to disseminate ISA's technical reports through the IEC.

Future activities of the committee include updating its technical reports; continuing to develop a complete standard for manufacturing and control systems security; developing control systems security requirements; developing common language and reference models; and formalizing liaisons and interfaces to government, standards-creating organizations, technical organizations, and other groups working in the area of control systems cybersecurity.

International Electrotechnical Commission

The International Electrotechnical Commission (IEC) is a standards organization that prepares and publishes international standards for all electrical, electronic, and related technologies. These standards serve as a basis for creating national standards and as references for drafting international tenders and contracts. IEC's members include manufacturers, providers, distributors, vendors, consumers, users, all levels of governmental agencies, professional societies, trade associations, and standards developers from over 60 countries.

IEC's Technical Committee 65 has been chartered to produce standards for process control. In September 2003, the committee announced its decision to address the cybersecurity of communications for the measurement and control of industrial processes. This new work encompasses technologies such as firewalls, routers, cryptographic security of communications, and authentication technologies. As mentioned previously, plans have been made for IEC and ISA to create a joint project team to advance their efforts to secure control systems.

IEC's Technical Committee 57 is working to develop standards for control systems and control system components, including communications and end devices such as RTUs. It is also establishing data and communication security and communications standards for substations.

Institute of Electrical and Electronics Engineers

The Institute of Electrical and Electronics Engineers (IEEE) is developing standards for defining, specifying, and analyzing control systems in the electric power industry. In addition, IEEE has developed recommended practices for communication between remote terminal units and intelligent electronic devices in a substation. IEEE is also working on a project to develop a standard for substation integrated protection, control, and data acquisition communications. The project will define standards for communications requirements and will specify message delivery time between intelligent electronic devices.

Partnership for Critical Infrastructure Security

The Partnership for Critical Infrastructure Security (PCIS) is comprised of government agencies and private-sector associations that represent each of the critical infrastructure sectors. The partnership coordinates cross-sector initiatives to support CIP by identifying legislative issues that affect such initiatives and by raising awareness of issues in CIP. PCIS has had a control systems working group whose goal has been to raise awareness of control system security and to discuss the existing initiatives to improve the security of control systems.

CERT/CC and KEMA Consulting

CERT/CC at Carnegie Mellon and KEMA Consulting are leading an initiative to establish E-CERT, a team to collect and analyze information about cybersecurity incidents in control systems within the nation's critical infrastructures, assess their effects, and share the results with industry. Already initiated, the first step consists of conducting a scoping study and developing a white paper to determine how to manage vulnerabilities and incidents. KEMA and CERT/CC plan to enlist expertise from the control system community and establish an ongoing rapport with control system vendors. Plans are for DOE, DHS, and private industry groups to fund the team. While this effort, thus far, has been focusing on the energy sector, the issues are applicable to other sectors.

Process Control Systems Cyber Security Forum

The Process Control Systems Cyber Security Forum (PCSCS) is a joint effort of KEMA Consulting and LogOn Consulting, Inc. Formed in 2003, PCSCS is an annual program to study the cybersecurity issues surrounding the effective operation of control systems. It focuses on issues, challenges, threats, vulnerabilities, best practices, lessons learned, and solutions. It currently holds workshops and seminars on control system cybersecurity via the Internet, offers consulting services, and publishes bulletins and white papers aimed at helping those in the process control environment to share information and address the issues they are facing in securing their control systems.

Appendix III: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

February 26, 2004

MEMORANDUM FOR: ROBERT F. DACEY
DIRECTOR, INFORMATION SECURITY SERVICES
GENERAL ACCOUNTING OFFICE

FROM: Frank Libutti
Under Secretary
Information Analysis and Infrastructure Protection Directorate
Department of Homeland Security

SUBJECT: Department of Homeland Security Response to Draft GAO Report (GAO-04-354) Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems

The Department of Homeland Security (DHS) concurs with the recommendation noted in your draft report, and appreciates the opportunity to comment.

DHS agrees that improving the security of control systems against the risk of cyber attacks is a high priority. DHS has engaged with the private sector, academia, and other government entities on this matter, and will continue to do so as outlined in Homeland Security Presidential Directive/HSPD-7. Consistent with the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets and the National Strategy to Secure Cyberspace, we are addressing control systems from both a physical and cyber perspective utilizing the capabilities of our Protective Security Division and National Cyber Security Division collectively.

We understand that our proposed changes to the text of the report have been reviewed and incorporated. We look forward to receiving your final report, and we will review it within the specified timeframe of sixty days after receipt.

If you or your staff have any questions or need additional information, please contact me or my Chief of Staff, John P. Chase, at 202-282-8141.

www.dhs.gov

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