

May 2008

INFORMATION SECURITY

TVA Needs to Address Weaknesses in Control Systems and Networks





Highlights of GAO-08-526, a report to congressional requesters

Why GAO Did This Study

Securing the control systems that regulate the nation's critical infrastructures is vital to ensuring our economic security and public health and safety. The Tennessee Valley Authority (TVA), a federal corporation and the nation's largest public power company, generates and distributes power in an area of about 80,000 square miles in the southeastern United States.

GAO was asked to determine whether TVA has implemented appropriate information security practices to protect its control systems. To do this, GAO examined the security practices in place at several TVA facilities; analyzed the agency's information security policies, plans, and procedures against federal law and guidance; and interviewed agency officials who are responsible for overseeing TVA's control systems and their security.

What GAO Recommends

To help implement effective information security practices over its control systems, GAO is making recommendations to TVA to improve the implementation of its agencywide information security program. In comments on a draft of this report, TVA agreed with the recommendations and provided information on steps it was taking to implement them.

In a separate report designated "Limited Official Use Only," GAO is also making recommendations to correct specific information security weaknesses.

To view the full product, including the scope and methodology, click on [GAO-08-526](#). For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

May 2008

INFORMATION SECURITY

TVA Needs to Address Weaknesses in Control Systems and Networks

What GAO Found

TVA has not fully implemented appropriate security practices to secure the control systems and networks used to operate its critical infrastructures. Both its corporate network infrastructure and control systems networks and devices were vulnerable to disruption. The corporate network was interconnected with control systems networks GAO reviewed, thereby increasing the risk that security weaknesses on the corporate network could affect those control systems networks. On TVA's corporate network, certain individual workstations lacked key software patches and had inadequate security settings, and numerous network infrastructure protocols and devices had limited or ineffective security configurations. In addition, the intrusion detection system had significant limitations. On control systems networks, firewalls reviewed were either inadequately configured or had been bypassed, passwords were not effectively implemented, logging of certain activity was limited, configuration management policies for control systems software were inconsistently implemented, and servers and workstations lacked key patches and effective virus protection. In addition, physical security at multiple locations did not sufficiently protect critical control systems. As a result, systems that operate TVA's critical infrastructures are at increased risk of unauthorized modification or disruption by both internal and external threats.

An underlying reason for these weaknesses is that TVA had not consistently implemented significant elements of its information security program. Although TVA had developed and implemented program activities related to contingency planning and incident response, it had not consistently implemented key activities related to developing an inventory of systems, assessing risk, developing policies and procedures, developing security plans, testing and monitoring the effectiveness of controls, completing appropriate training, and identifying and tracking remedial actions. For example, the agency lacked a complete inventory of its control systems and had not categorized all of its control systems according to risk, thereby limiting assurance that these systems were adequately protected. Agency officials stated that they plan to complete these risk assessments and related activities but have not established a completion date. Key information security policies and procedures were also in draft or under revision. Additionally, the agency's patch management process lacked a way to effectively prioritize vulnerabilities. TVA had only completed one system security plan, and another plan was under development. The agency had also tested the effectiveness of its control systems' security using outdated federal guidance, and many control systems had not been tested for security. In addition, only 25 percent of relevant agency staff had completed required role-based security training in fiscal year 2007. Furthermore, while the agency had developed a process to track remedial actions for information security, this process had not been implemented for the majority of its control systems. Until TVA fully implements these security program activities, it risks a disruption of its operations as a result of a cyber incident, which could impact its customers.

Contents

Letter		1
Results in Brief		2
Background		4
TVA Had Not Fully Implemented Appropriate Security Practices to Protect Its Critical Infrastructures		20
Information Security Management Program Was Not Consistently Implemented across TVA's Critical Infrastructure		29
Conclusions		41
Recommendations for Executive Action		42
Agency Comments and Our Evaluation		43
Appendix I	Objective, Scope, and Methodology	46
Appendix II	Comments from the Tennessee Valley Authority	49
Appendix III	GAO Contacts and Staff Acknowledgments	57
<hr/>		
Tables		
Table 1: Sources of Cyber Threats to Critical Infrastructures		8
Table 2: Key TVA Information Security Responsibilities		17
<hr/>		
Figures		
Figure 1: Major Components of a SCADA System		7
Figure 2: TVA's Seven State Service Area and Generating Facilities		15
Figure 3: Examples of TVA Generation Facilities		16
Figure 4: TVA Organizational Responsibilities for Control Systems		19

Abbreviations

CIO	chief information officer
FERC	Federal Energy Regulatory Commission
FIPS	Federal Information Processing Standard
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act of 2002
NEI	Nuclear Energy Institute
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OMB	Office of Management and Budget
SCADA	supervisory control and data acquisition
SP	Special Publication
TVA	Tennessee Valley Authority
US-CERT	U.S. Computer Emergency Readiness Team
VPN	virtual private network

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



**United States Government Accountability Office
Washington, DC 20548**

May 21, 2008

Congressional Requesters

Securing the control systems that perform vital functions in the complex networks of digital information systems on which the nation's critical infrastructures rely is critical to ensuring our national and economic security and public health and safety. Control systems are computer-based systems used by critical infrastructure sectors and industries to monitor and control sensitive processes and physical functions such as electric power generation and its transmission, oil and gas refining, water treatment and its distribution, and transportation.

We have previously reported that critical infrastructure control systems face increasing risks due to cyber threats, system vulnerabilities, and the serious potential impact of attacks as demonstrated by reported incidents.¹ If control systems are not adequately secured, their system vulnerabilities could be exploited, and our critical infrastructures could be disrupted or disabled, possibly resulting in loss of life, physical damage, or economic losses.

The majority of our nation's critical infrastructures are owned by the private sector; however, the federal government owns and operates critical infrastructure facilities including those in energy, water treatment and distribution, and transportation. One such entity, the Tennessee Valley Authority (TVA)—a federal corporation and the nation's largest public power company—generates electricity using its 52 fossil, hydro, and nuclear facilities—all of which use control systems. As a wholly owned government corporation, TVA must comply with the Federal Information Security Management Act of 2002² (FISMA) by developing a risk-based information security program and implementing information security controls for its computer systems.

¹GAO, *Critical Infrastructure Protection: Federal Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, GAO-07-1036 (Washington, D.C.: Sept. 10, 2007).

²FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347 (Dec.17, 2002).

Our objective was to determine whether TVA has effectively implemented appropriate information security practices for the control systems used to operate its critical infrastructures. To accomplish this objective, we examined the security practices in place at six TVA facilities. In addition, we analyzed the agency's information security policies, plans, and procedures and interviewed agency officials who are responsible for overseeing TVA's control systems and their security. See appendix I for a complete description of our objective, scope, and methodology.

We conducted this performance audit from March 2007 to May 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Results in Brief

TVA has not fully implemented appropriate security practices to protect the control systems used to operate its critical infrastructures. TVA's corporate network infrastructure and its control systems networks and devices at individual facilities and plants reviewed were vulnerable to disruption. For example, on the corporate network, one remote access system we reviewed that was used for the network was not securely configured, and individual workstations we reviewed lacked key patches and had inadequate security settings for key programs. Further, network infrastructure protocols and devices provided limited protections. In addition, the intrusion detection system³ that TVA used had significant limitations on its ability to effectively monitor the network. For example, although a network intrusion detection system was deployed by TVA to monitor network traffic, it could not effectively monitor certain data for key computer assets. On control systems networks, firewalls⁴ were bypassed or inadequately configured, passwords were not effectively implemented, logging of certain activity was limited, configuration management policies for control systems software were not consistently

³An intrusion detection system detects inappropriate, incorrect, or anomalous activity that is aimed at disrupting the confidentiality, integrity, or availability of a protected network and its computer systems.

⁴A firewall is a hardware or software component that protects computers or networks from attacks by outside network users by blocking and checking all incoming traffic.

implemented, and servers and workstations lacked key patches and effective virus protection. In addition, physical security at multiple locations did not sufficiently protect critical control systems. Moreover, the interconnections between TVA's control system networks and its corporate network increase the risk that security weaknesses on the corporate network could affect control systems networks. Although TVA used multiple network segments to separate more sensitive equipment, such as control systems, from the corporate network, weaknesses in the separation of these network segments could allow an attacker who gained access to a less secure portion of the interconnected network, such as the corporate network, to compromise equipment in a more secure portion of the interconnected network. This could include equipment that has access to control systems. As a result, TVA's control systems that operate its critical infrastructures are at increased risk of unauthorized modification or disruption by both internal and external threats.

An underlying reason for these weaknesses is that TVA had not consistently implemented significant elements of its information security program. Although TVA had developed and implemented program activities related to contingency planning and incident response, it had not consistently implemented key activities related to developing an inventory of systems, assessing risk, developing policies and procedures, developing security plans, testing and monitoring the effectiveness of controls, establishing sufficient training, and identifying and tracking remedial actions. For example, the agency lacked a complete and accurate inventory of its control systems and had included only two control systems on its federally required inventory of information systems. Of these two systems, TVA had only completed a security plan for one, while the plan for the other system was under development. The agency had also not categorized all of its control systems according to risk or magnitude of harm from compromise, leaving these systems at risk of harm due to inadequate security. Agency officials stated that they plan to complete these risk assessments and related activities but have not established a completion date for all facilities. Key information security policies and procedures were also in draft or under revision. TVA's patch management process also lacked a way to effectively prioritize vulnerabilities. In addition, only 25 percent of relevant TVA staff completed required role-based security training in fiscal year 2007. TVA also tested the effectiveness of its control systems' security using outdated federal guidance and did not test many control systems for security at all. Furthermore, while the agency had developed a process to track remedial actions for information security, this process had been implemented for only one of its control systems. Until TVA addresses the control systems

security weaknesses we have identified, it risks a disruption of its operations as a result of a cyber incident, which could impact both TVA and its customers.

To help implement effective information security practices over its control systems, we are making 19 recommendations to the Chief Executive Officer of TVA to improve the implementation of TVA's agencywide information security program.

In a separate report designated "Limited Official Use Only,"⁵ we are also making 73 recommendations to correct specific information security weaknesses.

In written comments on a draft of this report, the TVA Executive Vice President, Administrative Services, agreed on the importance of protecting critical infrastructures, concurred with all 19 recommendations in this report, and provided information on steps the agency was taking to implement the recommendations.

Background

Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies, where maintaining the public's trust is essential. The dramatic expansion in computer interconnectivity and the rapid increase in the use of the Internet have changed the way our government, the nation, and much of the world communicate and conduct business. However, without proper safeguards, systems are unprotected from individuals and groups with malicious intent to intrude and use the access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. This concern is well-founded for a number of reasons, including the increase in reports of security incidents, the ease of obtaining and using hacking tools, the steady advance in the sophistication and effectiveness of attack technology, and the dire warnings of new and more destructive attacks to come. Computer-supported federal operations are likewise at risk. Our previous reports and those of agency inspectors general describe persistent information security weaknesses that place a variety of federal operations at risk of

⁵GAO, *Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks*, GAO-08-459SU (Washington, D.C.: May 21, 2008).

disruption, fraud, and inappropriate disclosure. Thus, we have designated information security as a governmentwide high-risk area since 1997,⁶ a designation that remains in effect.⁷

Control Systems Are Used in Critical Infrastructures, Including Those Operated by the Federal Government

We have specifically recognized the importance of information security related to critical infrastructures. Critical infrastructures are physical or virtual systems and assets so vital to the nation that their incapacitation or destruction would have a debilitating impact on national and economic security and on public health and safety. These systems and assets—such as the electric power grid, chemical plants, and water treatment facilities—are essential to the operations of the economy and the government. Recent terrorist attacks and threats have underscored the need to protect these critical infrastructures. If their vulnerabilities are exploited, our nation's critical infrastructures could be disrupted or disabled, possibly causing loss of life, physical damage, and economic losses.

Although the majority of our nation's critical infrastructures are owned by the private sector, the federal government owns and operates key facilities that use control systems, including oil, gas, water, energy, and nuclear facilities. Control systems are used within these infrastructures to monitor and control sensitive processes and physical functions. Typically, control systems collect sensor measurements and operational data from the field, process and display this information, and relay control commands to local or remote equipment. Control systems perform functions that range from simple to complex. They can be used to simply monitor processes—for example, the environmental conditions in a small office building—or to manage the complex activities of a municipal water system or a nuclear power plant. In the electric power industry, control systems can be used to manage and control the generation, transmission, and distribution of electric power. For example, control systems can open and close circuit breakers and set thresholds for preventive shutdowns.

⁶GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997).

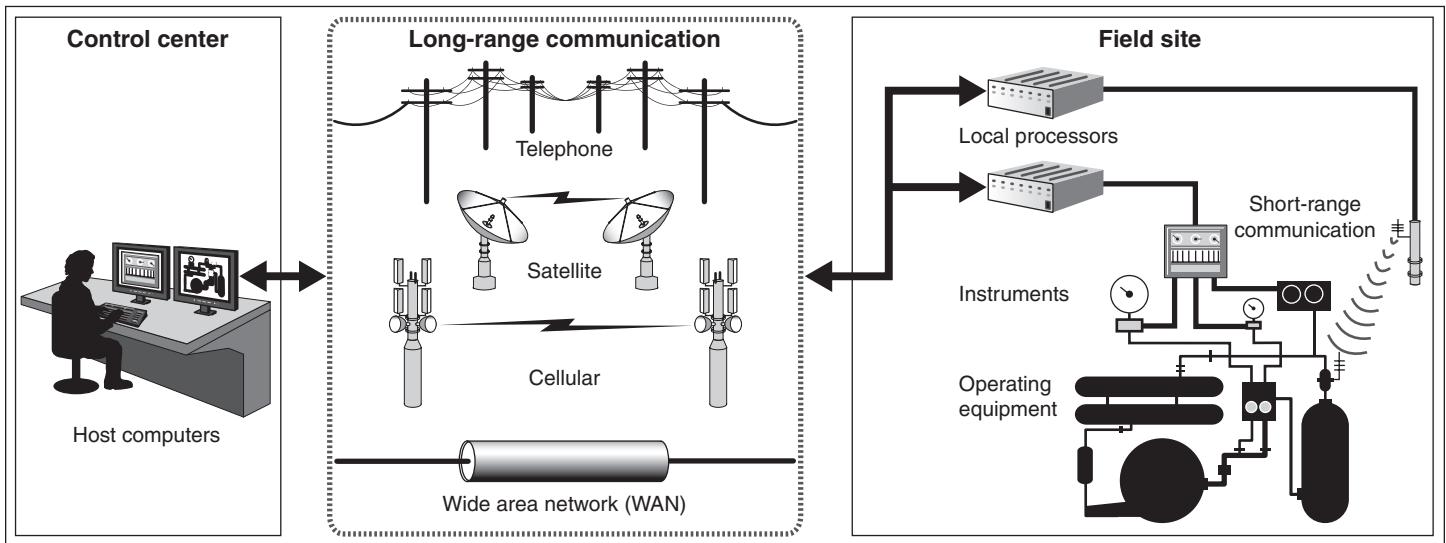
⁷GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007).

Control Systems: Types and Components

There are two primary types of control systems: distributed control systems and supervisory control and data acquisition (SCADA) systems. Distributed control systems typically are used within a single processing or generating plant or over a small geographic area and communicate using local area networks, while SCADA systems typically are used for large, geographically dispersed operations and rely on long-distance communication networks. In general, critical infrastructure sectors and industries depend on both types of control systems to fulfill their missions or conduct business. For example, a utility company that serves a large geographic area may use distributed control systems to manage power generation at each power plant and a SCADA system to manage power distribution to its customers.

A SCADA system is generally composed of these six components (see fig. 1): (1) operating equipment, which includes pumps, valves, conveyors, and substation breakers; (2) instruments, which sense conditions such as pH, temperature, pressure, power level, and flow rate; (3) local processors, which communicate with the site's instruments and operating equipment, collect instrument data, and identify alarm conditions; (4) short-range communication, which carries analog and discrete signals between the local processors and the instruments and operating equipment; (5) host computers, where a human operator can supervise the process, receive alarms, review data, and exercise control; and (6) long-range communication, which connects local processors and host computers using, for example, leased phone lines, satellite, and cellular packet data. A distributed control system is similar to a SCADA system but does not operate over a large geographic area or use long-range communications.

Figure 1: Major Components of a SCADA System



Source: GAO analysis of NIST guidance.

Control Systems for Critical Infrastructures Face Increasing Cyber Threats

We have previously reported that critical infrastructure control systems face increasing risks due to cyber threats, system vulnerabilities, and the potential impact of attacks as demonstrated by reported incidents.⁸ Cyber threats can be intentional or unintentional, targeted or nontargeted, and can come from a variety of sources. The Federal Bureau of Investigation has identified multiple sources of threats to our nation's critical infrastructures, including foreign nation states engaged in information warfare, domestic criminals and hackers, and disgruntled employees working within an organization. Table 1 summarizes those groups or individuals that are considered to be key sources of threats to our nation's infrastructures.

⁸See GAO-07-1036.

Table 1: Sources of Cyber Threats to Critical Infrastructures

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

Source: Federal Bureau of Investigation, unless otherwise indicated.

^aPrepared statement of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence, February 2, 2000.

Disruptions to control systems can have a significant effect on utilities such as electricity and water. The following are selected examples of disruptions that we previously reported in GAO-07-1036:

Maroochy Shire sewage spill:

In the spring of 2000, a former employee of an Australian organization that developed manufacturing software applied for a job with the local government, but was rejected. Over a 2-month period, this individual reportedly used a radio transmitter on as many as 46 occasions to remotely break into the controls of a sewage treatment system, ultimately releasing about 264,000 gallons of raw sewage into nearby rivers and parks.

Davis-Besse power plant:

The Nuclear Regulatory Commission confirmed that in January 2003, the Microsoft SQL Server worm known as Slammer infected a computer network at the idled Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly 5 hours and the plant's process computer for about 6 hours.

Northeast power blackout:

In August 2003, failure of the alarm processor in the control system of FirstEnergy, an Ohio-based electric utility, prevented control room operators from having adequate awareness of critical changes to the electrical grid. This problem was compounded when the state estimating program at the Midwest Independent System Operator failed. When several key transmission lines in northern Ohio tripped due to contact with trees, they initiated a cascading failure of 508 generating units at 265 power plants across eight states and a Canadian province.

Taum Sauk Water Storage Dam failure:

In December 2005, the Taum Sauk Water Storage Dam, approximately 100 miles south of St. Louis, Missouri, suffered a catastrophic failure, releasing a billion gallons of water. According to the dam's operator, the incident may have occurred because the gauges at the dam read differently than the gauges at the dam's remote monitoring station.

Control systems are more vulnerable to cyber threats, including intentional attacks and unintended incidents, than in the past for several reasons, including their increasing standardization and their increased connectivity to other systems and the Internet. For example, in August 2006, two circulation pumps at Unit 3 of the Browns Ferry, Alabama, nuclear power plant operated by TVA failed, forcing the unit to be shut down manually. The failure of the pumps was traced to an unintended incident involving excessive traffic on the control system network caused by the failure of another control system device.

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

Federal Regulations, Standards, and Guidance Establish Requirements to Secure Control Systems

To address the increasing threat to control systems governing critical infrastructures, both federal and private organizations have begun efforts to develop requirements, guidance, and best practices for securing control systems. For example, FISMA outlines a comprehensive, risk-based approach to securing federal information systems, which encompass control systems. Federal organizations, including the National Institute of Standards and Technology (NIST), the Federal Energy Regulatory

Commission (FERC), and the Nuclear Regulatory Commission (NRC), have used a risk-based approach to develop guidance and standards to secure control systems. NIST guidance has been developed that currently applies to federal agencies; however, much FERC and NRC guidance and many standards have not been finalized. Once implemented, FERC and NRC standards will apply to both public and private organizations that operate covered critical infrastructures.

We have previously reported on the importance of using a risk-based approach for securing critical infrastructures, including control systems.⁹ Risk management has received widespread support within and outside government as a tool that can help set priorities on how to protect critical infrastructures. While numerous and substantial gaps in security may exist, resources for closing these gaps are limited and must compete with other national priorities.

FISMA Established Requirements to Strengthen Information Security Practices at Federal Agencies

Recognizing the importance of securing federal agencies' information and systems, Congress enacted FISMA to strengthen the security of information and information systems within federal agencies, which include control systems.¹⁰

FISMA requires each agency to develop, document, and implement an agencywide information security program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Specifically, this program is to include

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- risk-based policies and procedures that cost effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each information system;

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

¹⁰FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002).

-
- subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;
 - security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency;
 - periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;
 - a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;
 - procedures for detecting, reporting, and responding to security incidents; and
 - plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

Furthermore, FISMA established a requirement that each agency develop, maintain, and annually update an inventory of major information systems (including major national security systems) operated by the agency or under its control. This inventory is to include an identification of the interfaces between each system and all other systems or networks, including those not operated by or under the control of the agency.

NIST Has Developed Standards and Guidance to Implement FISMA

FISMA also directs NIST to develop standards and guidelines for systems other than national security systems. As required by FISMA and based on the objectives of providing appropriate levels of information security, NIST developed

- standards for all agencies to categorize their information and information systems according to a range of risk levels,¹¹

¹¹NIST, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS 199 (Gaithersburg, Md.: February 2004).

-
- guidelines recommending the types of information and information systems to be included in each category,¹² and
 - minimum information security requirements for information and information systems in each category.¹³

NIST standards and guidelines establish a risk management framework that instructs agencies on providing an acceptable level of information security for all agency operations and assets and that guides the testing and evaluation of information security control effectiveness within an agencywide information security program. Recognizing the importance of documenting standards and guidelines as part of an agencywide information security program, NIST emphasizes that agencies must develop and promulgate formal, documented policies and procedures in order to ensure the effective implementation of security requirements.

NIST also collaborates with federal and industry stakeholders to develop standards, guidelines, checklists, and test methods to help secure federal information and information systems, including control systems. For example, NIST is currently developing guidance for federal agencies that own or operate control systems to comply with federal information system security standards and guidelines.¹⁴ The guidance identifies issues and modifications to consider in applying information security standards and guidelines to control systems. In December 2007, NIST released an augmentation to Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, which provides a security control framework for control systems.¹⁵ According to NIST officials, while most controls in SP 800-53 are applicable to control systems as written, several controls do require supplemental guidance and enhancements.

¹²NIST, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*, SP 800-60 (Gaithersburg, Md.; June 2004) and NIST, *Volume II: Appendixes to Guide for Mapping Types of Information and Information Systems to Security Categories*, SP 800-60 (Gaithersburg, Md.: June 2004).

¹³NIST, *Minimum Security Requirements for Federal Information and Information Systems*, FIPS 200 (Gaithersburg, Md.: March 2006).

¹⁴See NIST, *Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations Such As Programmable Logic Controllers (PLC)*, Draft SP 800-82 (Gaithersburg, Md.: September 2007).

¹⁵NIST, *Recommended Security Controls for Federal Information Systems*, SP 800-53 Revision 2 (Gaithersburg, Md.: December 2007).

FERC Has Recently Approved Reliability Standards That Address Control Systems Security

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

FERC has conducted several activities to begin implementing the requirements of the act. In July 2006, FERC certified the North American Electric Reliability Corporation (NERC) as the national electric reliability organization. In August 2003, prior to passage of the Energy Policy Act of 2005, NERC adopted Urgent Action 1200, a temporary, voluntary cyber security standard for the electric industry. Urgent Action 1200 directed electricity transmission and generation owners and operators to develop a cyber security policy, identify critical cyber assets, and establish controls for and monitor electronic and physical access to critical cyber assets. Urgent Action 1200 remained in effect on a voluntary basis until June 1, 2006, at which time NERC proposed eight critical infrastructure protection reliability standards to replace the Urgent Action 1200 standard.

In July 2007, FERC issued a notice of proposed rulemaking in which it proposed to approve eight critical infrastructure reliability standards, which included standards for control systems security. FERC also proposed to direct NERC to modify the areas of these standards that required improvement. In January 2008, after considering public comments on the notice of proposed rulemaking, FERC approved the reliability standards and the accompanying implementation plan. It also directed NERC to develop modifications to strengthen the standards and to monitor the development and implementation of the NIST standards to determine if they contain provisions that will protect the bulk-power system better than NERC's reliability standards. The organizations subject to the standards, including utilities like TVA, must be auditably compliant with the standards by 2010.

NRC Is Conducting A Rulemaking Process on Cyber Security, Including Control Systems

The NRC, which has regulatory authority over nuclear power plant safety and security, has conducted several activities related to enhancing the cyber security of control systems. In 2005, an industry task force led by the Nuclear Energy Institute (NEI) developed and released the *Cyber Security Program for Power Reactors* (NEI 04-04) to provide nuclear power reactor licensees a means for developing and maintaining effective cyber security

programs at their sites. In December 2005, the commission staff accepted the method outlined in NEI 04-04 for establishing and maintaining cyber security programs at nuclear power plants. TVA officials stated that the agency has begun a program to comply with NEI 04-04 guidelines and plans to complete implementation of corrective actions identified as a result of these guidelines over the next 3 years, consistent with planned plant outages and upgrade projects.

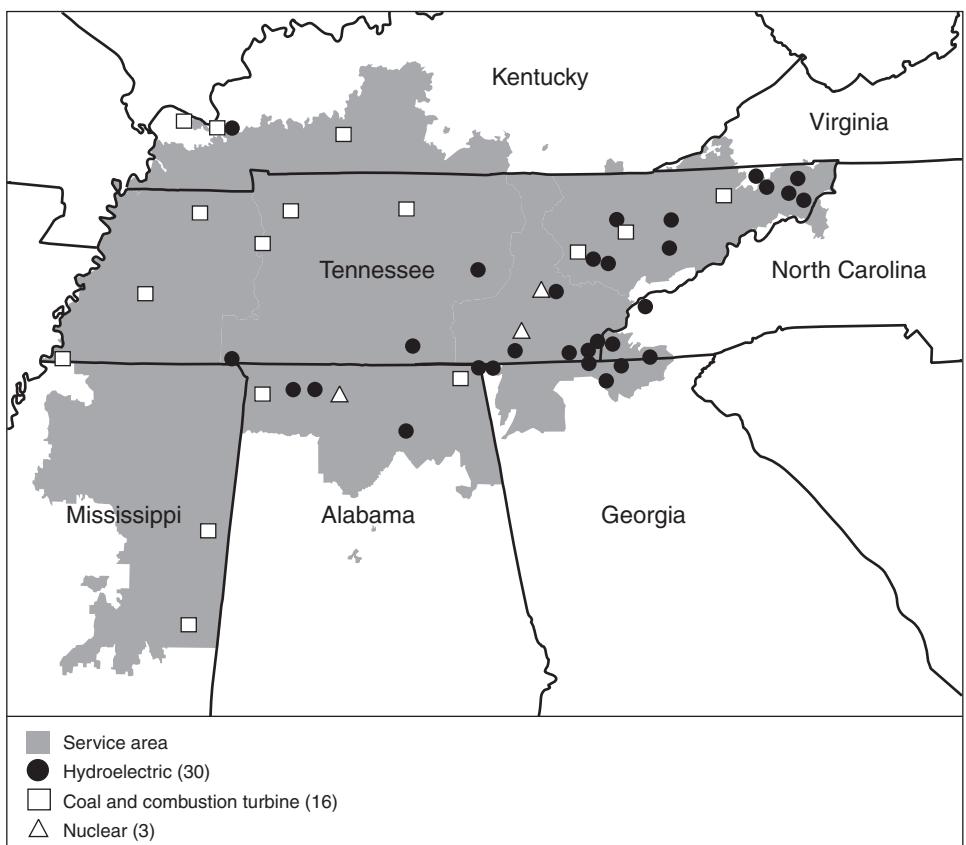
In January 2006, the commission issued a revision to Regulatory Guide 1.152, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*, which provides cyber security-related guidance for the design of nuclear power plant safety systems. In April 2007, the commission finalized a rule that added “external cyber attack” to the events that power reactor licensees are required to prepare to defend against. In addition, the commission initiated a rulemaking process that provides cyber security requirements for digital computer and communication networks, including systems that are needed for plant safety, security, or emergency response. The public comment period for this rulemaking closed in March 2007. Commission officials stated that they estimate this rulemaking process will be completed in early 2009. Once the rulemaking process is completed and requirements for nuclear power plant cyber security programs are finalized, the commission is planning to conduct a range of oversight activities, including inspections at power plants. According to commission officials, all nuclear plant operators have committed to complete implementation of the NEI-04-04 program at their sites.

TVA Provides Power to the Southeastern United States

The TVA is a federal corporation and the nation’s largest public power company. Its mission is to supply affordable, reliable power, support a thriving river system, and stimulate sustainable economic development in the public interest. In addition to generating and transmitting power, TVA also manages the nation’s fifth-largest river system to minimize flood risk, maintain navigation, provide recreational opportunities, and protect water quality. TVA is governed by a nine-member Board of Directors that is led by the Chairman. Each board member is nominated by the President of the United States and confirmed by the Senate. The TVA Chief Executive Officer reports to the TVA Board of Directors.

TVA’s power service area covers 80,000 square miles in the southeastern United States, an area that includes almost all of Tennessee and parts of Mississippi, Kentucky, Alabama, Georgia, North Carolina, and Virginia, and has a total population of about 8.7 million people (see fig. 2).

Figure 2: TVA's Seven State Service Area and Generating Facilities



Source: GAO analysis of TVA data.

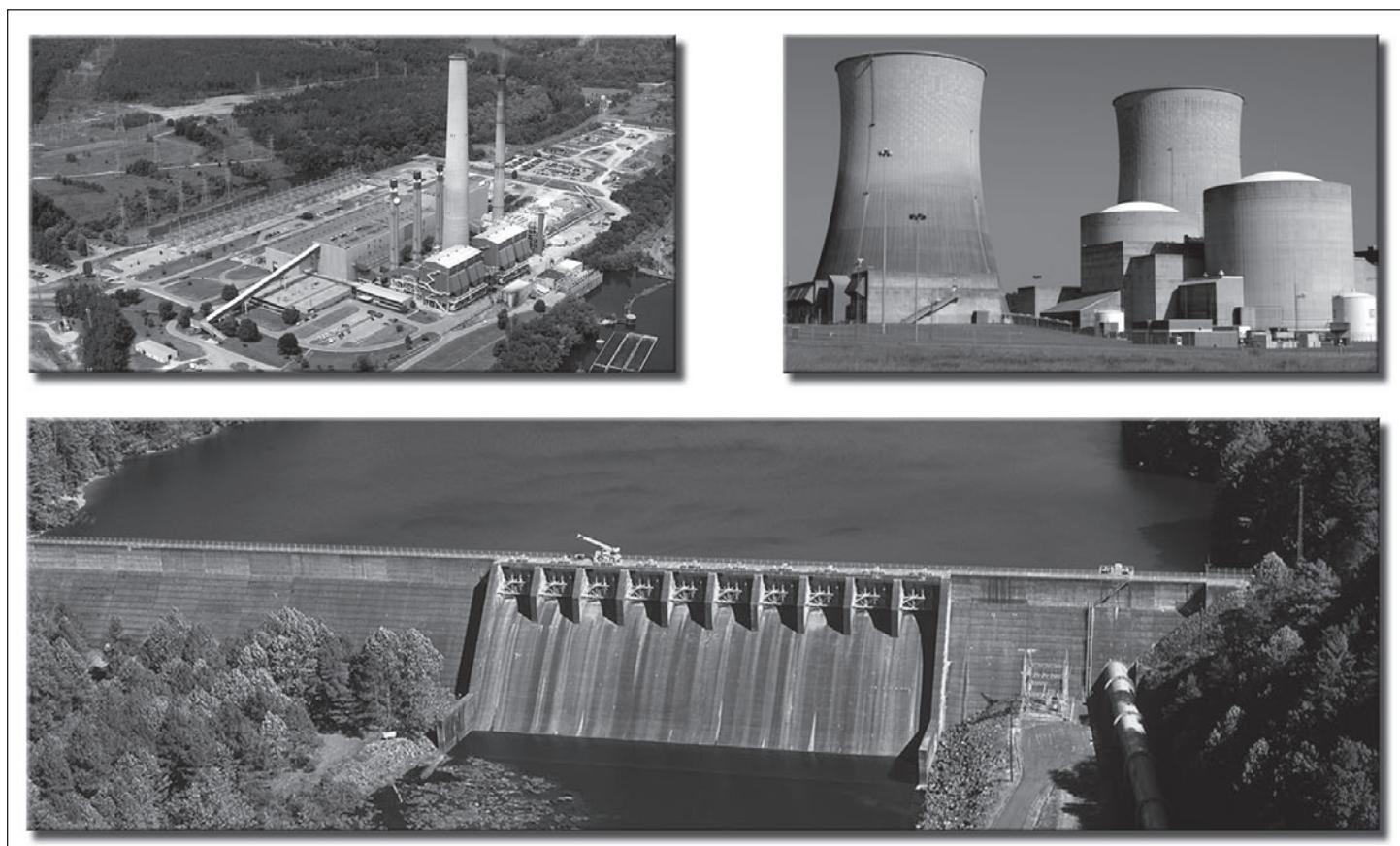
TVA operates 11 coal-fired fossil plants, 8 combustion turbine plants,¹⁶ 3 nuclear plants, and a hydroelectric system that includes 29 hydroelectric dams and one pumped storage facility (see fig. 2 and fig. 3).¹⁷ Fossil plants produce about 60 percent of TVA's power, nuclear plants about 30 percent, and the hydroelectric system about 10 percent. TVA also owns and

¹⁶Three of the combustion turbine plants are located immediately adjacent to coal generation facilities.

¹⁷A pumped-storage plant uses two reservoirs, with one located at a much higher elevation than the other. During periods of low demand for electricity, such as nights and weekends, energy is stored by reversing the turbines and pumping water from the lower to the upper reservoir. The stored water can later be released to turn the turbines and generate electricity as it flows back into the lower reservoir.

operates one of the largest transmission systems in North America. TVA's transmission system moves electric power from the generating plants where it is produced to distributors of TVA power and to industrial and federal customers across the region.

Figure 3: Examples of TVA Generation Facilities



Source: TVA.

Note: Clockwise from upper left are coal, nuclear, and hydroelectric generation facilities.

TVA provides power to three main customer groups: distributors, directly served customers, and off-system customers. There are 159 distributors—109 municipal utility companies and 50 cooperatives—that resell TVA power to consumers. These groups represent the base of TVA's business, accounting for 85 percent of their total revenue. Fifty-three large industrial customers and six federal installations buy TVA power directly. They represent 11 percent of TVA's total revenue. Twelve surrounding utilities

buy power from TVA on the interchange market. Sales to these utilities represent 4 percent of TVA's total revenue.

Control systems are essential to TVA's operation. TVA uses control systems to both generate and deliver power. In generation, control systems are used within power plants to open and close valves, control equipment, monitor sensors, and ensure the safe and efficient operation of a generating unit. Many control systems networks connect with TVA's corporate network to transmit information about system status.

To deliver power, TVA monitors the status of its own and surrounding transmission facilities from two operations centers. Each center is staffed 24 hours a day and can serve as a backup for the other center. Control systems at these centers are used to open and close breakers and balance the transmission of power across the TVA network while accounting for changes in network capacity due to outages and changes in demand that occur continuously throughout the day. TVA's control systems range in capacity from simple systems with limited functionality located in one facility to complex, geographically dispersed systems with multiple functions. The ages of these control systems range from modern systems to systems dating back 20 or more years to the original construction of a facility.

As shown in table 2, TVA has designated certain senior managers to serve the key roles in information security designated by FISMA.

Table 2: Key TVA Information Security Responsibilities

FISMA role	TVA official	Key responsibilities
Agency head	President and Chief Executive Officer	The agency head is responsible for the agencywide information security program. The agency head provides oversight for TVA's Information Security and Privacy Program and ensures that adequate resources are available to support the success of the program.
Inspector general	TVA Inspector General	The inspector general is responsible for promoting the efficiency, effectiveness, and integrity of TVA's Information Security and Privacy Program. This responsibility is accomplished, in part, by performing security audits, investigations, and inspections to evaluate compliance of the program with established federal laws, regulations, and accepted best practices. The Inspector General's responsibilities are also met by performing an annual, comprehensive review of TVA's Information Security and Privacy Program to include policies, procedures, and practices.

FISMA role	TVA official	Key responsibilities
Chief information officer	Vice President, Information Services	The chief information officer (CIO) is responsible for the organization's information system planning, budgeting, investment, performance, and acquisition. As such, the CIO provides advice and assistance to senior agency officials in acquiring the most efficient and effective information system to fit the organization's enterprise architecture. The CIO is also responsible for managing TVA's Information Security and Privacy Program, both within TVA and with external business partners and other federal agencies and ensuring compliance with the program.
Senior agency information security officer	Senior Manager, Enterprise IT Security	<p>The senior agency information security officer is responsible for carrying out the CIO information security responsibilities such as developing and maintaining TVA's Information Security and Privacy Program and ensuring compliance with the program. The officer plays a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize information security risks to an organization. The senior agency information security officer</p> <ul style="list-style-type: none"> • serves as the CIO's principal point of contact for all matters relating to the security of TVA's systems and information resources; • develops, maintains, and enforces information security policies, procedures, and standards to ensure the confidentiality, integrity, and availability of TVA's information resources and to ensure compliance with federal laws and regulations and accepted best practices in information security and privacy; • facilitates the development of agency-level implementing procedures for security controls; • monitors, evaluates, and reports to the CIO on the status and adequacy of the Information Security and Privacy Program within TVA; and • provides oversight, guidance, and support to TVA's information security and privacy personnel.

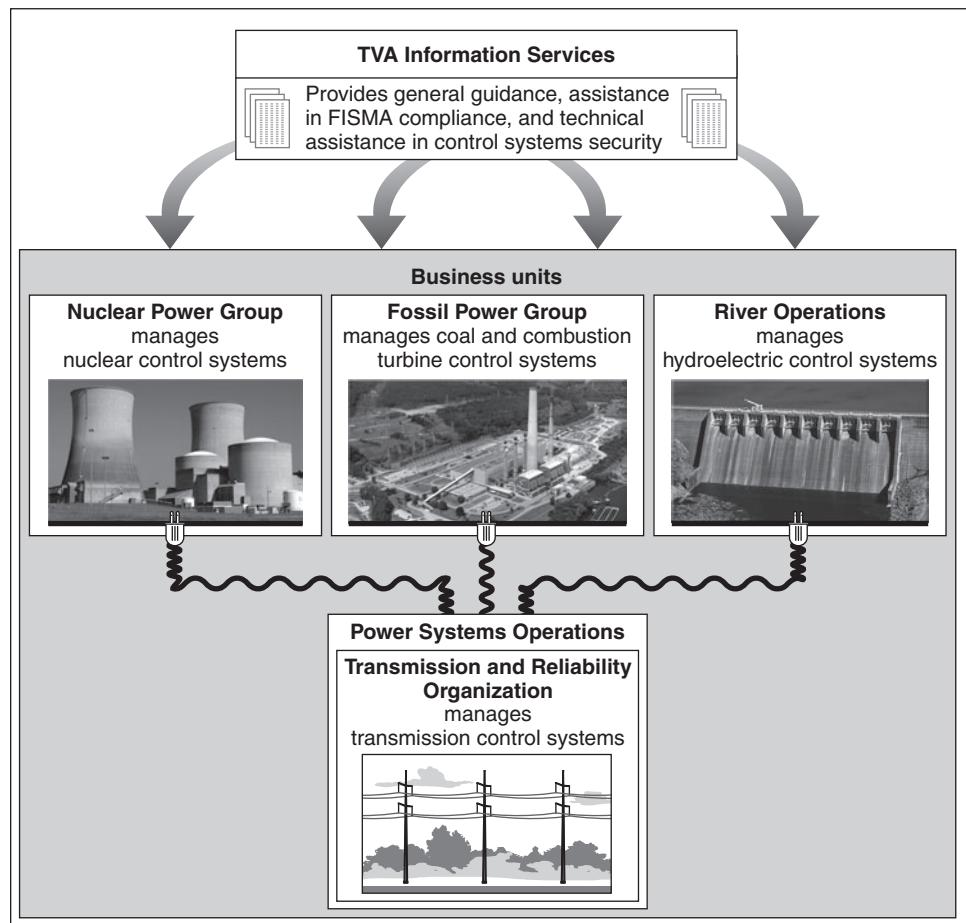
Source: GAO analysis of TVA data.

Responsibility for control systems security is distributed throughout TVA (see fig. 4). TVA's Information Services organization provides general guidance, assistance in FISMA compliance, and technical assistance in control systems security. The Information Services organization also manages the overall TVA corporate computer network that links facilities throughout the TVA service area and is connected to the Internet. As of February 2008, the Enterprise IT Security organization within Information Services was given specific responsibility for cyber security throughout the agency.

However, the control systems located within a plant are integrated with and managed as part of the generation equipment, safety and environmental systems, and other physical equipment located at that plant. This means that development, day-to-day maintenance and operation, and upgrades of control systems are handled by the business units responsible for the facilities where the systems are located. Specifically, nuclear systems are managed by the Nuclear Power Group; coal and combustion turbine control systems are managed by the Fossil Power Group; and hydroelectric facilities are managed by River

Operations. Transmission control systems are managed by TVA's Transmission and Reliability Organization, located within its Power Systems Operations business unit.

Figure 4: TVA Organizational Responsibilities for Control Systems



Sources: GAO analysis of TVA data (text), TVA (photos).

The Transmission and Reliability Organization is highly dependent on control systems. To comply with NERC Urgent Action 1200, and in an effort to ensure its systems are secure, the Transmission and Reliability Organization has handled additional aspects of information security compared with other TVA organizations. For example, the organization manages portions of its own network infrastructure. It also has arranged for both internal and external security assessments in order to enhance the security of its control systems.

TVA Had Not Fully Implemented Appropriate Security Practices to Protect Its Critical Infrastructures

TVA had not fully implemented appropriate security practices to secure the control systems used to operate its critical infrastructures. Both the corporate network infrastructure and control systems networks and devices at individual facilities and plants were vulnerable to disruption. In addition, physical security controls at multiple locations did not sufficiently protect critical control systems. The interconnections between TVA's control system networks and its corporate network increase the risk that security weaknesses on the corporate network could affect control systems networks. For example, because of weaknesses in the separation of lower security network segments from higher security network segments on TVA networks, an attacker who gained access to a less secure portion of a network such as the corporate network could potentially compromise equipment in a more secure portion of the network, including equipment that has access to control systems. As a result, TVA's control systems that operate its critical infrastructures are at increased risk of unauthorized modification or disruption by both internal and external threats.

TVA Corporate Network Was Vulnerable to Disruption

The TVA corporate network infrastructure had multiple weaknesses that left it vulnerable to intentional or unintentional compromise of the confidentiality, integrity, and availability of the network and devices on the network. These weaknesses applied both at TVA headquarters and to the portions of the corporate network located at the individual facilities we reviewed. For example, one remote access system used for the network that we reviewed was not securely configured. Further, individual servers and workstations lacked key patches and were insecurely configured. In addition, the configuration of numerous network infrastructure protocols and devices provided limited or ineffective security protections. Moreover, the intrusion detection system that TVA used had significant limitations. As a result, TVA's control systems were at an increased risk of unauthorized access or disruption via access from the corporate network. Furthermore, weaknesses in the intrusion detection system could limit the ability of TVA to detect malicious or unintended events on its network.

TVA Remote Access Was Insecurely Configured

Remote access is any access to an organizational information system by a user (or an information system) that communicates through an external, nonorganization-controlled network (e.g., the Internet). NIST guidance states that information systems should establish a trusted communications path between remote users and an information system and that two-factor authentication should be part of an organization's remote access authentication requirements. Additionally, TVA policy requires that if

remote access technology is used to connect to the network, it must be configured securely. One device used for remote access is a virtual private network (VPN).¹⁸

TVA did not configure a VPN system to include effective security mechanisms. This could allow an attacker who compromised a remote user's computer to remotely access the user's secure session to TVA, thereby increasing the risk that unauthorized users could gain access to TVA systems and sensitive information.

Individual Servers and Workstations Were Insecurely Configured

Federal and agency guidance call for effective patch management, firewall configuration, and application security settings. TVA has a patch management¹⁹ policy that requires it to regularly monitor, identify, and remediate vulnerabilities to applications in its software inventory. NIST guidance also states that firewalls should be carefully configured to provide adequate protection. Furthermore, NIST guidance states that organizations should effectively configure security settings in key applications to the highest level possible.

However, almost all of the workstations and servers that we examined on the corporate network lacked key security patches or had inadequate security settings. Furthermore, TVA did not effectively implement host firewall controls on its laptops. In addition, inadequate security settings existed in key applications installed on laptops, servers, and workstations we examined. Consequently, TVA is at an increased risk that known vulnerabilities in these applications could allow an attacker to execute malicious code and gain control of or compromise a system.

Network Infrastructure Protocols and Devices Provided Limited or Ineffective Protections

Federal and agency guidance state that organizations should have strong passwords, identification and authentication, and network segmentation. National Security Agency guidance states that Windows passwords should be 12 or more characters long, include upper and lower case letters, numbers, and special characters, and not consist of dictionary words and has advised against the use of weak encryption. NIST guidance states that

¹⁸A VPN is a private network that is maintained across a shared or public network, such as the Internet, by means of specialized security procedures. VPNs are intended to provide secure connections between remote clients, such as branch offices or traveling personnel, and a central office.

¹⁹Patch management is a critical process used to help alleviate many of the challenges involved with securing computing systems from attack. It includes acquiring, testing, applying, and monitoring patches to a computer system.

systems should uniquely identify and authenticate users with passwords or other authentication mechanisms or implement other compensating controls. NIST guidance also states that organizations should take steps to secure their e-mail systems. Finally, NIST guidance states that organizations should partition networks containing higher risk systems from lower risk systems and configure interfaces between those systems to manage risk.

However, the TVA corporate network used several protocols and devices that did not provide sufficient security controls. For example, certain network protocols and devices were not adequately protected by password or authentication controls or encryption. In addition, TVA had network services that spanned different security network segments. As a result, a malicious user could exploit these weaknesses to gain access to sensitive systems or to otherwise modify or disrupt network traffic.

Intrusion Detection System Had Significant Limitations

Even strong controls may not block all intrusions and misuse, but organizations can reduce the risks associated with such events if they take steps to promptly detect, report, and respond to them before significant damage is done. In addition, analyzing security events allows organizations to gain a better understanding of the threats to their information and the costs of their security-related problems. Such analyses can pinpoint vulnerabilities that need to be eliminated so that they will not be exploited again. NIST states that intrusion detection is the process of monitoring events occurring in a computer system or network and analyzing the events for signs of intrusion, which it defines as an attempt to compromise the confidentiality, integrity, or availability of a computer or network. NIST guidance prescribes network and host-based intrusion detection systems²⁰ as a means of protecting systems from the threats that come with increasing network connectivity.

TVA had limited ability to effectively monitor its network with its intrusion detection system. Although a network intrusion detection system was deployed by TVA to monitor network traffic, it could not effectively monitor key computer assets. As a result, there is an increased risk that unauthorized access to TVA's networks may not be detected and mitigated in a timely manner.

²⁰An intrusion detection system detects inappropriate, incorrect, or anomalous activity that is aimed at disrupting the confidentiality, availability, or integrity of a protected network and its computer systems.

TVA Control System Networks and Devices Were Vulnerable to Disruption

TVA's control system networks and devices on these networks were vulnerable to disruption due to inadequate information security controls. Specifically, firewalls were either bypassed or inadequately configured, passwords were either weak or not used at all, logging of certain activity was limited, configuration management policies for control systems software were not consistently implemented, and servers and workstations lacked key patches and effective virus protection. The combination of these weaknesses with the weaknesses in the TVA corporate network identified in the previous section places TVA's control systems that operate its critical infrastructures at increased risk of unauthorized modification or disruption by both internal and external threats.

Firewalls Were Either Bypassed or Inadequately Configured

A firewall is a hardware or software component that protects given computers or networks from attacks by blocking network traffic. NIST guidance states that firewalls should be configured to provide adequate protection for the organization's networks and that the transmitted information between interconnected systems should be controlled and regulated.

TVA had implemented firewalls to segment control systems networks from the corporate network at all facilities we reviewed with connections between these two networks. However, firewalls at three of six facilities reviewed were either bypassed or inadequately configured. As a result, the hosts on higher security control system networks were at increased risk of compromise or disruption from the other lower security networks.

Passwords or Other Compensating Controls Were Not Effectively Implemented

Passwords are used to establish the validity of a user's claimed identity by requesting some kind of information that is known only by the user—a process known as authentication. The combination of identification, using, for example, a unique user account, and authentication, using, for example, a password, provides the basis for establishing individual accountability and for controlling access to the system. In cases where passwords cannot be implemented because of technological limitations or other concerns, such as impact on emergency response, NIST states that an organization should document controls that have been put in place to compensate for this weakness. TVA policy requires authentication of users except where security requirements or limitations in the hardware or software preclude it. In addition, agency policy requires users to establish complex passwords.

TVA did not have effective passwords or other documented compensating controls governing control systems we reviewed. According to agency

officials, in certain cases, passwords were not technologically possible to implement but in these cases, there were no documented compensating controls. Until the agency implements either effective password practices or documented compensating controls, it faces an increased risk of unauthorized access to its control systems.

Audit Controls Did Not Effectively Log Certain Activity on Control Systems

Determining what, when, and by whom specific actions are taken on a system is crucial to establishing individual accountability, monitoring compliance with security policies, and investigating security violations. Audit and monitoring involves the regular collection, review, and analysis of auditable events for indications of inappropriate or unusual activity and the appropriate investigation and reporting of such activity. Audit and monitoring can help security professionals routinely assess computer security, perform investigations during and after an attack, and even recognize an ongoing attack. Federal guidance states that organizations should develop formal audit policies and procedures. TVA guidance states that sufficient audit logs should be maintained that allow monitoring of key user activities.

While TVA had taken steps to establish audit logs for its transmission control centers, it had not established effective audit logs or compensating controls at other facilities we reviewed. According to agency officials, system limitations at these facilities have historically meant that multiple users shared a single account to access these control systems. Therefore, audit logs would not have served a useful purpose because activities could not be traced to a single user. Until TVA establishes detailed audit logs for its control systems at these facilities or compensating controls in cases where such logs are not feasible, it risks being unable to determine if malicious incidents are occurring and, after an event occurs, being able to determine who or what caused the incident.

Configuration Management Policies Were Not Consistently Implemented on TVA Control Systems

Federal guidance states that all applications and changes to those applications should go through a formal, documented process that identifies all changes to the baseline configuration. Also, procedures should ensure that no unauthorized software is installed. TVA has established configuration management policies and procedures for its information technology systems. Specifically, its policies define the roles and responsibilities of application owners and developers; require business units to implement procedural controls that define documentation and testing required for software changes; and establish procedures to ensure that all changes relating to infrastructure and applications be managed and controlled.

However, TVA did not consistently apply its configuration management policies and procedures to control systems. The transmission control system had a configuration management process, and the hardware at individual plants was governed by a configuration management process, including plant drawings that tracked individual pieces of equipment. However, there was no formal configuration management process for software that was part of the control systems at the hydroelectric and fossil facilities that we reviewed. As a result, increased risk exists that unapproved changes to control systems could be made.

Software Patches on Control Systems Were Not Current

Patch management, including up-to-date patch installation, helps to mitigate vulnerabilities associated with flaws in software code, which could be exploited to cause significant damage. According to NIST, agencies should identify, report, and correct their information system flaws. According to NIST, tracking patches allows organizations to identify which patches are installed on a system and provides confirmation that the appropriate patches have been applied. Moreover, TVA policy requires the agency to remediate these vulnerabilities in a timely manner.

TVA had not installed current versions of patches for key applications on computers on control systems networks. While TVA had an agencywide policy and procedure for patch management, these policies did not apply to individual plant-level control systems. According to the operators at two of the facilities we reviewed, they applied vendor-approved patches to control systems but did not track versions of patches on these machines. Failure to keep software patches up-to-date could allow unauthorized individuals to gain access to network resources or disrupt network operations.

Virus Protection Software Was Not Consistently Implemented

Virus and worm²¹ protection for information systems is a serious challenge. Computer attack tools and techniques are becoming increasingly sophisticated; viruses are spreading faster as a result of the increasing connectivity of today's networks; commercial off-the-shelf products can be easily exploited for attack by their users; and there is no single solution such as firewalls or encryption to protect systems. To combat viruses and worms specifically, entities should keep antivirus programs up-to-date. According to NIST, agencies should implement

²¹A virus is a program that contains hidden code that usually performs some unwanted function as a side effect. A worm is a program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.

malicious code protection that includes a capability for automatic updates so that virus definitions are kept up-to-date on servers, workstations, and mobile computing devices. Virus-scanning software should be provided at critical entry points, such as remote-access servers, and at each desktop system on the network.

Although TVA implemented antivirus software on its transmission control systems network, it did not consistently implement antivirus software on other control systems we reviewed. In one case, according to agency officials, the vendor that developed the control systems software would not support an antivirus application, and the agency did not have plans to require the vendor to address this weakness. In another case, antivirus software was implemented, but it was not up-to-date. In the event that using antivirus software is infeasible on a control system, the agency must document the controls, such as training or physical security, that would compensate for this deficiency. TVA had not done this. According to agency officials, such documentation is under way for its hydroelectric facilities, but not for other facilities. As a result, there is increased risk that the integrity of these networks and devices could be compromised.

Physical Security Controls Did Not Effectively Limit Access to Sensitive Control Systems

Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. These controls restrict physical access to computer resources, usually by limiting access to the buildings and rooms in which the resources are housed and by periodically reviewing the access granted in order to ensure that access continues to be appropriate. TVA policy requires that appropriate physical and environmental controls be implemented to provide security commensurate with the level of risk and magnitude of harm that would result from loss, misuse, unauthorized access, or modification of information or information systems. Further, NIST policy requires that federal organizations implement a variety of physical security controls to protect information and industrial control systems and the facilities in which they are located.

TVA had taken steps to provide physical security for its control systems. For example, it had issued electronic badges to agency personnel and contractors to help control access to many of its sensitive and restricted areas. TVA had also established law enforcement liaisons that help ensure additional backup security and facilitate the accurate flow of timely security information between appropriate government agencies. In addition, the agency had implemented physical security training for its employees to help achieve greater security awareness and accountability.

However, the agency had not effectively implemented physical security controls at various locations, as the following examples illustrate:

- Live network jacks connected to TVA's internal network at certain facilities we reviewed had not been adequately secured from access by the public.
- TVA did not adequately control or change its keys to industrial control rooms containing sensitive equipment at one facility we reviewed. For example, the agency could neither account for all keys issued at the facility, which relies on manual locks for the security of rooms containing sensitive computer and control equipment, nor could it determine when keys had last been changed.
- TVA did not have an effective visitor control program at one facility we reviewed. For example, the agency had not maintained a visitor log describing visitors' names, organizations, purpose of visits, forms of identification, or the names of the persons visited.
- Physical security policies and plans were either in draft form or were nonexistent.
- Rooms containing sensitive IT equipment had not been adequately environmentally protected. For example, sufficient emergency lighting was not available outside the control room at one facility we reviewed, a server room at the facility had no smoke detection capability, a control room at the facility contained a kitchen (a potential fire and water hazard), and a communications room had batteries collocated with sensitive communications gear.
- TVA had not always ensured that access to sensitive computing and industrial control systems resources had been granted to only those who needed it to perform their jobs at one facility we reviewed. About 75 percent of those who were issued facility badges had access to a facility computer room, but the vast majority of these badgeholders did not need access to the room. While TVA officials stated that all of those with access had been through the background investigation and training process required for all employees at the facility, an underlying principle for secure computer systems and data recommended by NIST is that users should be granted only those access rights and permissions needed to perform their official duties.

As a consequence of weaknesses such as these, increased risk exists that sensitive computing resources and data could be inadvertently or deliberately misused or destroyed.

Cumulative Effect of Inconsistencies and Weaknesses in Layered Network Defense Placed Critical Infrastructure Control Systems at Risk

Federal guidance and best practices in information security call for the use of multiple layers of defense to secure information resources. These multiple layers include the use of protection mechanisms and key network control points such as firewalls, routers, and intrusion detection systems to segment and control access to networks. Higher risk networks and devices, such as critical infrastructure control systems, may require additional security controls and should be on networks that are separate from lower risk devices.

TVA had deployed a layered defense model to control access between and among the corporate and control systems networks. For example, in all cases we examined, control systems were located on networks that had been segmented from business computing resources. The agency had also deployed protection mechanisms such as firewalls, router access control lists, virtual local area networking, and physical security controls at multiple locations throughout its network. For example, TVA's transmission control organization used layered networks with increasing levels of security to separate critical control devices from the corporate network.

However, these mechanisms and information security controls had been inconsistently applied. As a result, the effectiveness of the multiple layers of defense was limited. For example, while the transmission control organization network restricted access to control systems using multiple firewalls at outer and inner network boundaries, some plant systems had significantly fewer levels of security to reach control systems that impacted the same facilities. In addition, specific weaknesses in security configurations on key systems further reduced the overall effectiveness of security controls. The cumulative effect of these individual weaknesses and the interconnectedness of TVA critical infrastructure control systems places these systems at risk of compromise or disruption from internal and external threats.

Information Security Management Program Was Not Consistently Implemented across TVA's Critical Infrastructure

An underlying reason for TVA's information security control weaknesses is that it had not consistently implemented significant elements of its information security program. The effective implementation of an information security program includes implementing the key elements required under FISMA and the establishment of a continuing cycle of activity—which includes developing an inventory of systems, assessing risk, developing policies and procedures, developing security plans,²² testing and monitoring the effectiveness of controls, identifying and tracking remedial actions, and establishing appropriate training. TVA had not consistently implemented key elements of these activities. As a result of not fully developing and implementing its information security program, an increased potential for disruption or compromise of its control systems exists.

Inventory of Systems Was Not Complete or Accurate

FISMA requires that each agency develop, maintain, and annually update an inventory of major information systems operated by the agency or that are under its control. A complete and accurate inventory of major information systems is a key element of managing the agency's information technology resources, including the security of those resources. The inventory can be used to track agency systems for purposes such as periodic security testing and evaluation, patch management, contingency planning, and identifying system interconnections. TVA requires that the senior agency information security officer maintain an authoritative inventory of general support systems, major applications, major information systems, and minor applications.

TVA did not have a complete and accurate inventory of its control systems. In its fiscal year 2007 FISMA submission, TVA included in its inventory of major applications the transmission and the hydro automation control systems. Although TVA stated that the plant control systems at its nuclear and fossil facilities were minor applications, these applications had not been included in TVA's inventory of minor applications or accounted for as part of a consolidated general support system. These systems are essential to automated operation of generation facilities. At the conclusion of our review, agency officials stated they had developed a plan to develop a more complete and accurate system

²²FISMA requires that agencywide information security programs include subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate. These plans are commonly referred to as system security plans.

inventory by September 2008. Until TVA has a complete and accurate inventory of its control systems, it cannot ensure that the appropriate security controls have been implemented to protect these systems.

TVA Had Not Assessed Risk for Almost All of Its Control Systems

FISMA mandates that agencies assess the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of their information and information systems. The Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, and related NIST guidance provide a common framework for categorizing systems according to risk. The framework establishes three levels of potential impact on organizational operation, assets, or individuals should a breach of security occur—high (severe or catastrophic), moderate (serious), and low (limited)—and it is used to determine the impact for each of the FISMA-specified security objectives of confidentiality, integrity, and availability. Once determined, security categories are to be used in conjunction with vulnerability and threat information in determining minimum security requirements for the system and in assessing the risk to an organization. Risk assessments help ensure that the greatest risks have been identified and addressed, increase the understanding of risk, and provide support for needed controls. Office of Management and Budget (OMB) Circular A-130, appendix III, prescribes that risk be assessed when significant changes are made to major systems and applications in an agency's inventory or at least every 3 years. Consistent with NIST guidance, TVA policy states that risk assessments should be updated to reflect the results of security tests and evaluations.

TVA had not completed assigning risk levels or assessing the risk of its control systems. While TVA categorized the transmission and hydro automation control systems as high-impact systems using FIPS 199, its nuclear division and fossil business unit, which include its coal and combustion turbine facilities, had not assigned risk levels to their control systems. Further, although TVA had performed a risk assessment for the transmission control system, the risk assessment did not include the risks associated with the newly identified vulnerabilities identified during the latest security test and evaluation. TVA had not completed risk assessments for the control systems at their nuclear, hydroelectric, coal, and combustion turbine facilities. According to TVA officials, the agency plans to complete risk assessments by May 2008 at the nuclear facility and June 2008 at the hydroelectric facility. For the fossil facility and all remaining control systems throughout TVA, agency officials stated that they would complete the security categorization of these systems by the

end of September 2008. However, no date has been set for completion of risk assessments. Without assigned risk levels, TVA cannot make risk-based decisions on the security needs of their information and information systems. Moreover, until TVA assesses the risks of all its control systems, the agency cannot be assured that its control systems apply the appropriate level of controls to help prevent their unauthorized access, use, disclosure, disruption, modification, or destruction.

Security Policies Existed but Were Not Always Consistent and Did Not Clearly Define All Roles and Responsibilities

A key task in developing, documenting, and implementing an effective information security program is to establish and implement risk-based policies, procedures, and technical standards that cover security over an agency's computing environment. If properly implemented, policies and procedures can help to reduce the risk that could come from unauthorized access or disruption of services. Because security policies are the primary mechanism by which management communicates its views and requirements, it is important to document and implement them.

Several shortcomings existed in TVA's information security policies. First, the agency had not consistently applied information security policies to its control systems. Second, business unit security policies were not always consistent with overall agency information security policies. Third, cyber security responsibilities for interfaces between TVA's transmission control system and its fossil and hydroelectric generation units had not been documented. Fourth, TVA's patch management process was not in compliance with federal guidance. Finally, physical security standards for control system sites were in draft.

TVA Had Not Consistently Applied Information Security Policies to Control Systems

TVA had developed and documented policies, standards, and guidelines for information security; however, it had not consistently applied these policies to its control systems. Although neither FISMA nor TVA's agencywide IT security policy explicitly mentions control systems, our analysis of NIST guidance and the stated position of NIST officials is that the guidance does apply to industrial control systems, such as the systems that TVA uses to operate critical infrastructures. Furthermore, NIST has recently developed and released guidance to assist agencies in applying federal IT security requirements to control systems. As a result of not applying this guidance with the same level of rigor to its control systems, numerous shortfalls existed in TVA's information security management program for its control systems, including outdated risk assessments; incomplete system security categorizations, system security plans, and testing and evaluation activities; and an ineffective remediation process. TVA officials stated that they are in the process of applying current NIST

criteria to their control systems and plan to complete this process by the end of fiscal year 2008. Until TVA consistently applies federal IT security policies to its control systems and addresses identified weaknesses, its control systems will remain at risk of compromise and disruption.

Business Unit Policies Were Not Consistent with Overall Agency Policy

While two TVA business units had developed IT security policies to address anticipated cyber security guidance from their respective industries, these policies were not always consistent with agencywide IT security policy. According to TVA policy, business units may establish their own IT security policies but must still comply with agencywide IT security policy. For example, TVA's Nuclear Power Group had developed a cyber security policy and the Power Systems Operations business unit had developed two cyber security policies—one business unit policy that was in draft, and one approved policy developed by and applicable to the unit's Transmission and Reliability Organization. These policies addressed many of the same issues as TVA's agencywide IT security policy, including establishing roles and responsibilities, access controls, configuration management, training, and emergency planning and response. However, the policies were not always consistent with the agencywide IT security policy. For example, although both the Nuclear Power Group and the Transmission and Reliability Organization policies had been developed to establish requirements for cyber security of plant systems, neither policy directed system security officers to implement minimum baseline security controls to protect the confidentiality, integrity, and availability of these systems, as is required by agency policy, nor did they establish a link or reference to agencywide IT security policy or federal IT security requirements. Although the Power System Operations cyber security policy reiterated requirements outlined by FISMA and the TVA IT security policy, this policy remained in draft. The existence of inconsistent policies at different levels of TVA could hinder its ability to apply IT security requirements consistently across the agency. Without developing and implementing consistent policies, procedures, and standards across all agency divisions and groups, TVA has less assurance that its systems controlling critical infrastructure are protected from unauthorized access and cyber threats.

**Cyber Security Responsibilities
for Interfaces with
Transmission Organization
Were Not Defined**

NIST guidance states that organizations should authorize all connections from an information system to another information system through the use of system connection agreements.²³ Documentation should include security roles and responsibilities and any service level agreements, which should define the expectations of performance for each required security control, and remedy and response requirements for any identified instance of noncompliance.

The agreements established by TVA's Transmission and Reliability Organization with other TVA business units did not fully address information that should be included based on NIST guidance. For example, the control systems operated by the Transmission and Reliability Organization interface with power plant control systems operated by TVA's fossil and hydroelectric business units. Although the transmission organization had established agreements with the fossil and hydroelectric business units, these agreements made no mention of cyber security roles and responsibilities, performance expectations for security controls, and remedy and response requirements for noncompliance. TVA officials stated that the type of interface between the transmission control system and individual plant systems means that, in most cases, a cyber security incident on a plant control network would not impact the overall transmission control network. While the likelihood of direct transmission of malware such as a virus might be small, without clear documentation of information required in an intergroup agreement, TVA faces the risk that security controls may not be in place or work as intended at an individual plant, resulting in a situation where critical generation equipment may not be able to start, safely shut down, or otherwise be controlled by the transmission control system when necessary. This is particularly of concern because of the variation in cyber security controls that we observed between the overall transmission control system and the individual plants. Without clear documentation of cyber security-related roles and responsibilities, TVA faces the risk that security controls may not be in place or work as intended.

**Patch Management Policies
Were Not in Compliance with
NIST Guidance**

NIST guidance states that federal agencies should create a comprehensive patch management process.²⁴ The process should include

²³NIST, *Guide for Developing Security Plans for Federal Information Systems*, SP 800-18 (Gaithersburg, Md.: February 2006).

²⁴NIST, *Creating a Patch and Vulnerability Management Program*, SP 800-40 (Gaithersburg, Md.: November 2005).

-
- monitoring of security sources for vulnerability announcements;
 - an accurate inventory of the organization's IT resources, using commercially available automated inventory management tools whenever possible;
 - prioritization of the order in which the vulnerabilities are addressed with a focus on high-priority systems such as those essential for mission-critical operations; and
 - automated deployment of patches to IT devices using enterprise patch management tools.

TVA had not fully implemented such a comprehensive process. It had a patch management process, including staff whose primary responsibility is to monitor security sources for vulnerability announcements. However, the agency lacked an accurate inventory of its IT resources produced using an automated management tool. For example, agency staff did not have timely access to version numbers and build numbers of software applications in the agency, although officials stated this information could be obtained manually. In addition, the agency's patch management policy did not apply to individual plant-level control systems or network infrastructure devices such as routers and switches.

Furthermore, TVA's written guidance on patch management provided only limited guidance on how to prioritize vulnerabilities. For example, the guidance did not refer to the criticality of IT resources. In addition, as previously noted, the agency had not categorized the impact of many of its control systems. The guidance also did not specify situations for which it was acceptable to upgrade or downgrade a vulnerability's priority from that given by industry standard sources such as the vendor or third-party patch tracking services. As a result, patches that were identified as critical, meaning they should be applied immediately to vulnerable systems, were not applied in a timely manner. For example, agency staff had reduced the priority of three vulnerabilities identified as critical or important by the vendor or a patch tracking service and did not provide sufficient documentation of the basis for this decision. TVA also did not document many vulnerabilities on its systems. For a 15-month period, TVA documented its analysis of 351 reported vulnerabilities, while NIST's

National Vulnerability Database²⁵ reported about 2,000 vulnerabilities rated as high or medium-risk for the types of systems in operation at TVA for the same time period. Finally, the agency lacked an automated tool to assess the deployment of many types of application patches. As a result, certain systems were missing patches more than 6 months past TVA deadlines for patching. Without a fully effective patch management process, TVA faces an increased risk that critical systems may remain vulnerable to known vulnerabilities and be open to compromise or disruption.

Physical Security Policies Remained in Draft

NIST guidance states that organizations should develop formal documented physical security policies and procedures to facilitate the implementation of physical and environmental protection controls. However, TVA's physical security standards for protection of its assets, including sensitive computer and industrial control equipment, as well as employees, contractors, visitors, and the general public, had been drafted but not approved by management. These standards are intended to provide clear and consistent physical security policy for all nonnuclear facilities. According to TVA Police officials, most sites budget for and implement their own physical security guidance and measures. Finalized physical security standards agencywide would provide consistent guidelines for facilities to make risk-based decisions on implementing these recommendations. Consequently, TVA has less assurance that control systems will be consistently and effectively protected from inadvertent or deliberate misuse including damage or destruction.

Security Plans for Most Control Systems Had Not Been Completed

The objective of system security planning is to improve the protection of IT resources. A system security plan provides a complete and up-to-date overview of the system's security requirements and describes the controls that are in place—or planned—to meet those requirements. FISMA requires that agency information security programs include subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate. OMB Circular A-130 specifies that agencies develop and implement system security plans for major applications and for general support systems and that these plans address policies and procedures for providing management, operational, and technical controls. NIST guidance states

²⁵The National Vulnerability Database is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance.

that minor applications that are not connected to a general support system or major application should be described in a general support system plan that has either a common physical location or is supported by the same organization. Further, TVA policy states that minor applications should be briefly described in a general support system security plan. NIST guidance states that security plans should contain key information needed to select the appropriate security controls, such as the FIPS 199 category and the certification and accreditation status of the connected systems. Plans should also be updated to include the latest security test and evaluation and risk assessment results.

TVA had only developed a system security plan that covered two of the six facilities we reviewed, and this plan was incomplete and not up-to-date. The transmission control system security plan, which addressed systems at two transmission control centers, included many elements required by NIST, such as the description of the individuals responsible for security, and addressed management, operational, and technical controls. Although the plan listed interconnected systems, it did not completely address interconnectivity with other systems operated by other organizations. Specifically, it did not include essential information needed to select the appropriate security controls, such as the FIPS 199 category or the certification and accreditation status of the connected systems. Further, the plan was not updated to include the latest security test and evaluation or risk assessment results. According to agency officials, TVA is developing a system security plan for its hydroelectric automation control system as part of its certification and accreditation process. Agency officials stated that this plan will be completed by June 2008.

TVA nuclear and fossil facilities had not developed security plans for their control systems. Agency officials stated that they were planning to develop security plans and complete the certification and accreditation process for these control systems. The plan for the nuclear facility is scheduled to be completed by June 2008. For the fossil facility, TVA officials stated that they intend to complete a security plan and certification and accreditation activities based on the results of security categorizations that will be completed by September 2008. However, no time frame has been set for completion of the plan or accreditation. Until these activities are completed, TVA cannot ensure that the security requirements have been identified and that the appropriate controls will be in place to protect these critical control systems.

General Security Awareness Training Was Completed, but Training for Specific Roles Was Not Completed

FISMA mandates that federal employees and contractors who use agency information systems be provided with periodic training in information security awareness. FISMA also requires agencies to provide appropriate training on information security to personnel who have significant security responsibilities. This training, described in NIST guidance,²⁶ should inform personnel, including contractors and other users of information systems supporting the operations and assets of an agency, of information security risks associated with their activities and their roles and responsibilities to properly and effectively implement the practices that are designed to reduce these risks. Depending on an employee's specific security role, training could include specialized topics such as incident detection and response, physical security, or firewall configuration. TVA also has a policy that requires that all employees and others who have access to its corporate network to complete annual security awareness training. The policy requires that employees and contractors who do not complete the training within a set time frame have their network access suspended.

Although for fiscal year 2007 TVA reported that 98 percent of its employees and contractors completed its annual security awareness training, other shortfalls existed in TVA's training program. For example, the agency policy of suspending network access for employees who did not complete security awareness training did not apply to control system-specific networks, such as those at the nuclear, hydroelectric, and fossil facilities we reviewed. At these sites, there were no controls in place to enforce completion of the required training by employees using these control systems.

In addition, a substantial number of TVA employees who have significant security responsibilities did not complete role-based training in the last fiscal year, and the required training did not include specialized technical topics. In fiscal year 2007, TVA reported that only 25 percent of 197 applicable employees who had significant IT security responsibilities had completed role-based training, compared with 86 percent and 72 percent who reportedly received such training in fiscal years 2005 and 2006, respectively. According to agency officials, training had not been completed primarily due to a lack of staff to provide the training. Furthermore, the role-based training that was required was focused on

²⁶NIST, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, SP 800-16 (Gaithersburg, Md.: April 1998), and NIST, *Building an Information Technology Security Awareness and Training Program*, 800-50 (Gaithersburg, Md.: October 2003).

management and procedural issues. TVA had technical security training available to its information security staff, which comprised approximately 14 of the 197 employees who needed role-based training, but this training was not required. For these 14 staff, TVA reported a 100 percent completion rate for the technical training. At the end of our review, agency officials provided a plan to improve the number of employees completing role-based training and to examine adding technical training to training requirements. The plan is to be completed by July 2008. Until this plan is fully implemented, security lapses are more likely to occur and could contribute to information security weaknesses at TVA.

TVA Did Not Adequately Test and Evaluate the Effectiveness of Security Practices

A key element of an information security program is ongoing testing and evaluation to ensure that systems are in compliance with policies and that the policies and controls are both appropriate and effective. Testing and evaluation demonstrates management's commitment to the security program, reminds employees of their roles and responsibilities, and identifies areas of noncompliance and ineffectiveness requiring remediation. Starting in fiscal year 2007, OMB required agencies to discontinue using SP 800-26 and to use NIST SP 800-53A for the assessment of security controls effectiveness when performing periodic security testing and evaluation of their information systems.²⁷ In addition, TVA policy requires all minor applications to be assigned to a general support system or major application that is tested and evaluated as part of the certification and accreditation process performed every 3 years.

TVA did not properly test and evaluate all of its control systems. Although TVA had performed annual self-assessments of the two control systems designated as major applications (transmission and hydro automation control systems) in fiscal year 2007, it did so using outdated NIST guidance contained in SP 800-26, rather than the current guidance in SP 800-53A. Of these two control systems, TVA performed a complete test and evaluation of the security controls on one of the systems—the transmission control system—within the last 3 years. Although TVA officials at the nuclear and fossil facilities considered their plant-level control systems to be minor applications, they were not part of any general support system. As a result, TVA did not appropriately identify,

²⁷OMB, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, M-06-20 (Washington, D.C.: July 17, 2006).

test, or evaluate the effectiveness of the security controls in place for the control systems at these facilities. Without appropriate tests and evaluations of all its control systems, the agency has limited assurance that policies and controls are appropriate and working as intended. Additionally, increased risk exists that undetected vulnerabilities could be exploited to allow unauthorized access to these critical systems.

Most Remedial Action Plans Had Not Been Developed

A remedial action plan is a key component described in FISMA. Such a plan assists agencies in identifying, assessing, prioritizing, and monitoring progress in correcting security weaknesses that are found in information systems. In its annual FISMA guidance to agencies, OMB requires agencies' remedial action plans, also known as plans of action and milestones, to include, at a minimum, the resources necessary to correct an identified weakness, the original scheduled completion date, the status of the weakness as completed or ongoing, and key milestones with completion dates.²⁸ According to TVA policy, the agency should document weaknesses found during security assessments and document any planned remedial actions to correct any deficiencies.

TVA did not always address known significant deficiencies in its remedial action plans. The agency had developed a plan of action and milestones for its transmission control system; however, it did not do so for the control systems at the fossil, hydroelectric, or nuclear facilities. In addition, while the agency tracks weaknesses identified by the TVA Inspector General for its transmission control system, it did not include these weaknesses in its plan of action and milestones. Until the agency implements an effective remediation process for all control systems, it will not have assurance that the proper resources will be applied to known vulnerabilities or that those vulnerabilities will be properly mitigated.

Incident Response Procedures Had Not Been Finalized

Even strong controls may not block all intrusions and misuse, but organizations can reduce the risks associated with such events if they take steps to promptly detect, report, and respond to them before significant damage is done. In addition, analyzing security incidents allows organizations to gain a better understanding of the threats to their

²⁸See OMB, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*, M-03-19 (Washington, D.C.: Aug. 6, 2003) for OMB's 2003 FISMA reporting guidance.

information and the costs of their security-related problems. Such analyses can pinpoint vulnerabilities that need to be eliminated so that they will not be exploited again. Incident reports can be used to provide valuable input for risk assessments, can help in prioritizing security improvement efforts, and can illustrate risks and related trends for senior management. FISMA and NIST guidance require that agency information security programs include procedures for detecting, reporting, and responding to security incidents, including reporting them to the U.S. Computer Emergency Readiness Team (US-CERT). Furthermore, NIST guidance prescribes network and host-based intrusion detection systems as a means of protecting systems from the threats that come with increasing network connectivity.

TVA had developed incident detection, response, and reporting procedures. However, while the TVA organization responsible for operating its transmission control center had approved incident response and reporting procedures, the agencywide incident response and reporting procedure remained in draft form, although it is currently being used by TVA information security personnel. According to agency officials, the procedure is being revised and finalized to align with incident reporting guidelines developed by US-CERT. Until TVA finalizes these procedures, it cannot be assured that facilities are prepared to respond to and report incidents in an effective manner.

Contingency Planning Activities Were Completed but Were Not Fully Documented

Contingency planning includes developing and testing plans and activities so that when unexpected events occur, critical operations can continue without disruption or can be promptly resumed and that critical and sensitive data are protected. If contingency planning controls are inadequate, even relatively minor interruptions can result in a loss of system function and expensive recovery efforts. For some TVA control systems, system interruptions or malfunctions could result in loss of power, injuries, or loss of life. Given these severe implications, it is critical that an entity have in place (1) procedures for protecting information systems and minimizing the risk of unplanned interruptions and (2) a plan to recover critical operations should interruptions occur. To determine whether recovery plans will work as intended, they should be tested periodically in disaster-simulation exercises. FISMA requires that each federal agency implement an information security program that includes plans and procedures to ensure continuity of operations for information systems that support the operation and assets of the agency.

TVA had taken steps to address contingency planning for physical incidents such as fire, explosion, and natural disasters, and for other events such as cyber incidents. At the facilities we reviewed, staff performed regular drills and tests to address physical contingencies. According to agency officials, in many cases, these same drills are applicable to cyber incidents that could have physical consequences. In addition, the agency had developed backup²⁹ procedures for key information resources, including those that support its control systems. In TVA's transmission control centers, written backup procedures existed; however, in the hydroelectric, coal, and gas turbine facilities we reviewed, the backup procedures were not documented. Until TVA consistently documents backup procedures across all of its facilities, it has limited assurance that all TVA facilities will be able to respond appropriately in the event of a physical or cyber incident.

Conclusions

TVA's power generation and transmission critical infrastructures are important to the economy of the southeastern United States and the safety, security, and welfare of millions of people. Control systems are essential to the operation of these infrastructures; however, multiple information security weaknesses existed in both the agency's corporate network and individual control systems networks and devices. As a result, although TVA had implemented multiple layers of information security controls to protect its critical infrastructures, such as segmenting control systems networks from the corporate network, in many cases, these layers were not as effective as intended. An underlying cause for these weaknesses is that the agency had not consistently implemented its information security program throughout the agency. If TVA does not take sufficient steps to secure its control systems and implement an information security program, it risks not being able to respond properly to a major disruption that is the result of an intended or unintended cyber incident, which could affect the agency's operations and its customers.

²⁹Backup is the activity of copying files or databases so that they will be preserved in case of equipment failure or other catastrophe. Backup is usually a routine part of business operations.

Recommendations for Executive Action

To improve the implementation of information security program activities for the control systems governing TVA's critical infrastructures, we are recommending that the Chief Executive Officer of TVA take the following 19 actions:

- Establish a formal, documented configuration management process for changes to software governing control systems at TVA hydroelectric and fossil facilities.
- Establish a patch management policy for all control systems.
- Establish a complete and accurate inventory of agency information systems that includes each TVA control system either as a major application, or as a minor application to a general support system.
- Categorize and assess the risk of all control systems.
- Update the transmission control system risk assessment to include the risk associated with vulnerabilities identified during security testing and evaluations and self-assessments.
- Revise TVA information security policies and procedures to specifically mention their applicability to control systems.
- Ensure that any division-level information security policies and procedures established to address industry regulations or guidance are consistent with, refer to, and are fully integrated with TVA corporate security policy and federal guidance.
- Revise the intergroup agreements between TVA's Transmission and Reliability Organization and its fossil and hydroelectric business units to explicitly define cyber security roles and responsibilities.
- Revise TVA patch management policy to clarify its applicability to control systems and network infrastructure devices, provide guidance to prioritize vulnerabilities based on criticality of IT resources, and define situations where it would be appropriate to upgrade or downgrade a vulnerability's priority from that given by industry standard sources.
- Finalize draft TVA physical security standards.
- Complete system security plans that cover all control systems in accordance with NIST guidance and include all information required by

NIST in security plans, such as the FIPS 199 category and the certification and accreditation status of connected systems.

- Enforce a process to ensure that employees who do not complete required security awareness training cannot access control system-specific networks.
- Ensure that all designated employees complete role-based security training and that this training includes relevant technical topics.
- Develop and implement a TVA policy to ensure that periodic (at least annual) assessments of control effectiveness use NIST SP 800-53A for major applications and general support systems.
- Perform assessments of control effectiveness following the methodology in NIST SP 800-53A.
- Develop and implement remedial action plans for all control systems.
- Include the results of inspector general assessments in the remedial action plan for the transmission control system.
- Finalize the draft agencywide cyber incident response procedure.
- Document backup procedures at all control system facilities.

In a separate report designated “Limited Official Use Only,”³⁰ we are also making 73 recommendations to the Chief Executive Officer of TVA to address weaknesses in information security controls.

Agency Comments and Our Evaluation

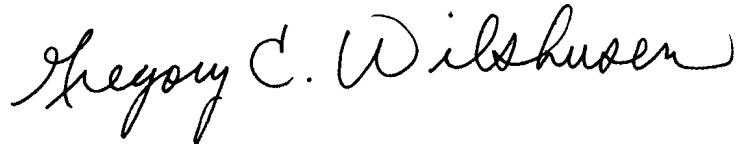
In written comments on a draft of this report, the Executive Vice President of Administrative Services for TVA agreed on the importance of protecting critical infrastructures and described several actions TVA has taken to strengthen information security for control systems, such as centralizing responsibility for cyber security within the agency. The Executive Vice President concurred with all 19 recommendations in this report and provided information on steps the agency was taking to implement the recommendations. A copy of the agency’s response is included in appendix II.

³⁰ GAO-08-459SU.

Additionally, in a meeting with GAO officials, TVA officials expressed concerns about the level of detail in this report. Based on that meeting and subsequent discussions with agency officials, we have modified the wording in this report to address the agency's concerns. The agency also provided technical comments that we have incorporated where appropriate.

We are sending copies of this report to OMB, the TVA Inspector General and other interested parties. 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>.

If you have any questions on matters discussed in this report, please contact Gregory Wilshusen at (202) 512-6244 or Nabajyoti Barkakati (202) 512-4499, or by e-mail at wilshuseng@gao.gov and barkakatin@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.



Gregory C. Wilshusen
Director, Information Security Issues



Nabajyoti Barkakati
Acting Chief Technologist

List of Requesters

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

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

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

Appendix I: Objective, Scope, and Methodology

The objective of our review was to determine if the Tennessee Valley Authority (TVA) has effectively implemented appropriate information security practices for the control systems used to operate its critical infrastructure. We conducted our review using our Federal Information System Controls Audit Manual,¹ a methodology for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized data. We focused our work on the control systems located at six TVA facilities. These facilities were selected to provide a cross-section of the variety of control systems by type of generation facility (coal, combustion turbine, hydroelectric, and nuclear) and function (generation and transmission).

To evaluate the effectiveness of TVA's information security practices, we conducted tests and observations using federal guidance, checklists, and vendor best practices for information security. Where federal requirements or guidelines, including National Institute of Standards and Technology (NIST) guidance, were applicable, we used them to assess the extent to which TVA had complied with specific requirements. Specifically, we used NIST guidance for the security of federal information systems.² For example, we

- analyzed the password hashing implementation used for identification and authentication;
- evaluated and reviewed the complexity and expiration of passwords on servers to determine if strong password management was enforced;
- examined user and application system authorizations to determine whether they had more permissions than necessary to perform their assigned functions;
- analyzed system configurations to determine whether sensitive data were being encrypted;
- observed whether system security software was configured to log successful system changes;

¹GAO, *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999).

²See, for example, NIST, *Recommended Security Controls for Federal Information Systems*, SP 800-53, Revision 2 (Gaithersburg, Md.: December 2007).

-
- inspected key servers, workstations, and network infrastructure devices to determine whether critical patches had been installed or were up-to-date;
 - tested and observed physical access controls to determine if computer facilities and resources were being protected from espionage, sabotage, damage, and theft; and
 - synthesized the information obtained about networks and applications to develop an accurate understanding of overall network and system architecture.

The Federal Information Security Management Act of 2002 (FISMA) establishes key elements of an effective agencywide information security program. We evaluated TVA's implementation of these key elements by

- reviewing TVA's system inventory to determine whether it contained an accurate and comprehensive list of control systems;
- analyzing risk assessments for key TVA systems to determine whether risks and threats were documented;
- examining security plans to determine if management, operational, and technical controls were in place or planned and whether these security plans were updated;
- analyzing TVA policies, procedures, practices, and standards to determine their effectiveness in providing guidance to personnel responsible for securing information and information systems;
- inspecting training records for personnel with significant responsibilities to determine if they received training commensurate with those responsibilities;
- analyzing test plans and test results for key TVA systems to determine whether management, operational, and technical controls were adequately tested at least annually and were based on risk;
- evaluating TVA's process to correct weaknesses and determining whether remedial action plans complied with federal guidance; and
- examining contingency plans for key TVA systems to determine whether those plans had been tested or updated.

To conduct our work, we reviewed and analyzed relevant documentation and held discussions with key security representatives, system administrators, and management officials to determine whether information system controls were in place, adequately designed, and operating effectively. We also reviewed previous reports issued by the TVA Inspector General's Office. We conducted this performance audit from March 2007 to April 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Tennessee Valley Authority

Tennessee Valley Authority, 400 West Summit Hill Drive, Knoxville, Tennessee 37902-1401

John E. Long, Jr.
Executive Vice President
Administrative Services

May 14, 2008

Mr. Gregory C. Wilshusen, Director
Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

RE: Revised GAO Draft Public Report -- GAO-08-526 TVA Control Systems Security

Dear Mr. Wilshusen:

We appreciate the opportunity to provide the comments of the Tennessee Valley Authority (TVA) on the subject revised draft of GAO's Public report, which was transmitted to us by GAO on May 13, 2008. These comments replace those comments TVA provided on May 7, 2008, on an earlier draft of the Public report.

TVA agrees with the central premise that preserving the security of our nation's critical infrastructures is essential to ensuring national and economic security and protecting public health and safety.

As a result of the field work on this performance audit which commenced in October 2007, and was completed in February 2008, GAO is making 19 recommendations to TVA in its revised draft Public report. TVA was in the process of addressing 17 of the 19 recommendation areas when the field work on this performance audit began in October 2007, including an Office of the Inspector General/Science Applications International Corporation audit for IT Security Organizational Effectiveness, for which planning began in July 2007, and an agency-wide physical access control project which began in October 2005.

TVA also commenced a number of actions in other recommendation areas while the audit was ongoing. In July 2007, TVA established a new structure for its Information Services organization and by December 2007 had approved plans to centralize all responsibility for IT security in a single, corporate-level function. The implementation of this transition for IT security was completed on February 7, 2008, with the announcement by TVA's Chief Executive Officer of the centralization of TVA-wide cyber security policy, administration, and oversight in a new corporate-level Enterprise IT Security organization.

A specific example of steps being taken by TVA during this same time period was the enlistment of a third-party consultant to perform uninformed and informed penetration

Appendix II: Comments from the Tennessee Valley Authority

Mr. Gregory C. Wilshusen
Page 2
May 14, 2008

testing of TVA's infrastructure to identify weaknesses and provide recommendations for remediation. As noted in the April 14, 2008 report to TVA from the third-party consultant, "the team was unable to gain access to any of the targeted Process Control Networks." During this testing, TVA did receive immediate alerts from our security perimeter monitoring service and also from some of our key internal monitoring systems. As a consequence of this testing, some weaknesses and areas were identified for improvement and enhancement to strengthen TVA's current defense-in-depth security posture. Remedial steps have already been taken to address those issues.

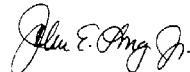
To memorialize the actions completed or already in process by TVA with respect to specific recommendation areas during the field audit period and to summarize TVA's ongoing action plans for all of the remaining GAO recommendations, please find enclosed Exhibit I, which addresses each of the 19 recommendations in the "Public" report.

We believe that our actions clearly demonstrate TVA's commitment to assuring the security of its critical infrastructures and related information and control systems.

As you are aware, TVA, GAO, and DHS representatives met on May 2 to discuss the certain changes that TVA had requested be made in the earlier version of the draft Public Report. In suggesting those changes, it was TVA's overarching concern that the public disclosure of certain references and examples would unintentionally encourage, and might actually facilitate, efforts by certain types of individuals to try to disrupt or sabotage TVA's critical infrastructure systems by specifically identifying TVA systems, applications, or areas.

Our review of the revised draft Public report provided to us on May 13 indicates that changes have been made by GAO which address TVA's most material concerns. TVA appreciates GAO's willingness to make those changes. If there are any questions, please contact Wayne R. Gildroy, Assistant General Counsel, at 865/632-7361.

Sincerely,



John E. Long, Jr.

Enclosure

Exhibit 1

EXHIBIT I

**TVA RESPONSES TO
GAO RECOMMENDATIONS
PUBLIC REPORT**

GAO Recommendations (Public Report)

1. Establish a formal, documented configuration management process for changes to software governing control systems at TVA's hydroelectric and fossil facilities.

TVA Response: Management agrees. Fossil Power Group (FPG) process development was scheduled prior to GAO field work. Development began during audit and will be complete by July 31, 2008. Procedures for conventional hydro plants for River Operations (RO) are in progress and will be complete by June 30, 2008. Additionally Nuclear Power Group (NPG) has a formal, documented configuration management process in accordance with NRC requirements.

2. Establish a patch management policy for all control systems.

TVA Response: Management agrees. TVA had a patch management policy in place for its corporate systems prior to the start of GAO's field work. This process was not consistently applied to control systems. As a result of TVA's centralization of all IT security as a corporate-level function on February 7, 2008, this policy has been extended to be agency-wide including control

Exhibit 1

systems. A cross organizational task team to evaluate the patch management process has been formed and objectives have been drafted. Appropriate actions will be implemented with a target completion date of December 31, 2008.

3. Establish a complete and accurate inventory of agency information systems as required by FISMA that includes each TVA control system either as a major application, or as a minor application to a general support system.

TVA Response: Management agrees. There was a system inventory effort established prior to GAO field work. This effort is being enhanced and will be complete May 30, 2008. A process will be established for assuring the maintenance of a complete and accurate inventory by May 30, 2008. Categorizations for control systems will be completed by September 30, 2008.

4. Categorize and assess the risk of all control systems.

TVA Response: Management agrees.

TVA has an established standard set of security steps. This process, which TVA already had in place prior to GAO field work, was not consistently applied to control systems. With the TVA CEO's February 7, 2008, announcement of the TVA-wide cyber security policy, administration, and oversight centralizing in a new corporate-level Enterprise IT Security organization, TVA will be completing the security categorizations for all control systems by September 30, 2008. Major applications and General Support Systems (GSS) will have appropriate system security plans, risk assessments, and security test and evaluation steps developed with a targeted completion date of September 30, 2009.

5. Update the transmission control system risk assessment to include the risk associated with vulnerabilities identified during security testing and evaluations and self assessments.

TVA Response: Management agrees. This was completed April 23, 2008.

Exhibit 1

6. Revise TVA information security policies and procedures to specifically mention their applicability to control systems.
TVA Response: Management agrees. Communication Practice 1, Business Practice 29, and Computer Security and Privacy Incident Response policy / procedure were issued May 5, 2008.
7. Ensure that any division-level information security policies and procedures established to address industry regulations or guidance are consistent with, refer to, and are fully integrated with TVA corporate security policy and federal guidance.
TVA Response: Management agrees. Power System Operations (PSO) procedures with references that were specifically mentioned in the report were issued May 2, 2008. Nuclear Power Group (NPG) procedures with references that were specifically mentioned in the report were issued April 30, 2008. Additionally, conventional hydro's are in progress and will be updated by June 30, 2008 and Raccoon Mountain by December 31, 2008.
8. Revise the intergroup agreements between TVA's Transmission and Reliability Organization and its fossil and hydroelectric business units to explicitly define cyber security roles and responsibilities.
TVA Response: Management agrees. Information Services Enterprise IT Security has responsibility for agency-wide cyber security management and administration on all TVA cyber assets. Revisions to agreements are in progress. The Transmission Reliability Organization (TRO) will complete an interconnection service agreement (ISA) with FPG, RO, and NPG to define cyber security roles and responsibilities by June 30, 2008. The ISA documents will reference the intergroup agreements and will be added to the intergroup agreements on their next revision. TRO will follow EITS guidance to ensure alignment with TVA-wide governance.
9. Revise TVA patch management policy to clarify its applicability to control systems and network infrastructure devices; provide guidance to prioritize vulnerabilities based on criticality of IT resources; and define situations where it would be appropriate to

Exhibit 1

upgrade or downgrade a vulnerability's priority from that given by industry standard sources.

TVA Response: Management agrees. TVA had a patch management policy in place for its corporate systems prior to the start of GAO's field work. This process was not consistently applied to control systems. As a result of TVA's centralization of all IT security as a corporate-level function on February 7, 2008, this policy has been extended to be agency-wide including control systems. A cross organizational task team to evaluate the patch management process has been formed and objectives have been drafted. Appropriate actions will be implemented with a target completion date of December 31, 2008.

10. Finalize draft TVA physical security standards.

TVA Response: Management agrees. TVA physical security standards will be issued May 9, 2008.

11. Complete system security plans that cover all control systems in accordance with NIST guidance and include all information required by NIST in security plans, such as the FIPS 199 category and the certification and accreditation status of connected systems.

TVA Response: Management agrees.

TVA has an established standard set of security steps. This process, which TVA already had in place prior to GAO field work, was not consistently applied to control systems. With the TVA CEO's February 7, 2008, announcement of the TVA-wide cyber security policy, administration, and oversight centralizing in a new corporate-level Enterprise IT Security organization, TVA will be completing the security categorizations for all control systems by September 30, 2008. Major applications and General Support Systems (GSS) will have appropriate system security plans, risk assessments, and security test and evaluation steps developed with a targeted completion date of September 30, 2009.

12. Enforce a process to ensure that employees who do not complete required security awareness training cannot access control system-specific networks.

Exhibit 1

TVA Response: Management agrees. A cross organizational task team to evaluate enforcement options has been formed and objectives have been drafted. Implementation of compensatory controls such as logs will be completed by September 30, 2008.

13. Ensure that all designated employees complete role-based security training and that this training includes relevant technical topics.

TVA Response: Management agrees. An improvement plan has been developed and is in progress. This plan will be implemented by July 31, 2008. This plan was previously provided to the GAO audit team.

14. Develop and implement a TVA policy to ensure that periodic (at least annual) assessments of control effectiveness use NIST SP 800-53A for major applications and general support systems.

TVA Response: Management agrees. IT Security Procedure - Security Test and Evaluation was issued on May 7, 2008.

15. Perform assessments of control effectiveness following the methodology in NIST SP 800-53A.

TVA Response: Management agrees.

TVA has an established standard set of security steps. This process, which TVA already had in place prior to GAO field work, was not consistently applied to control systems. With the TVA CEO's February 7, 2008, announcement of the TVA-wide cyber security policy, administration, and oversight centralizing in a new corporate-level Enterprise IT Security organization, TVA will be completing the security categorizations for all control systems by September 30, 2008. Major applications and General Support Systems (GSS) will have appropriate system security plans, risk assessments, and security test and evaluation steps developed with a targeted completion date of September 30, 2009.

16. Develop and implement remedial action plans for all control systems.

TVA Response: Management agrees.

Exhibit 1

TVA has an established standard set of security steps. This process, which TVA already had in place prior to GAO field work, was not consistently applied to control systems. With the TVA CEO's February 7, 2008, announcement of the TVA-wide cyber security policy, administration, and oversight centralizing in a new corporate-level Enterprise IT Security organization, TVA will be completing the security categorizations for all control systems by September 30, 2008. Major applications and General Support Systems (GSS) will have appropriate system security plans, risk assessments, and security test and evaluation steps developed with a targeted completion date of September 30, 2009.

17. Include the results of inspector general assessments in the remedial action plan for the transmission control system.

TVA Response: Management agrees. Results were added and closed out on the remedial action plan by TRO on April 25, 2008.

18. Finalize the draft agency-wide cyber incident response procedure.

TVA Response: Management agrees. The Computer Security and Privacy Incident Response policy / procedure was issued May 5, 2008.

19. Document backup procedures at all control system facilities.

TVA Response: Management agrees. RO procedures are in progress and will be completed by June 30, 2008 for conventional hydro. Raccoon Mountain will be completed by December 31, 2008. NPG to complete by September 30, 2008. FPG backup procedures will be complete by August 31, 2008.

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen, (202) 512-6244, wilshuseng@gao.gov
Nabajyoti Barkakati, (202) 512-4499, barkakatin@gao.gov

Staff Acknowledgments

In addition to the individuals named above, Nancy DeFrancesco and Lon Chin, Assistant Directors; Angela Bell; Bruce Cain; Mark Canter; Heather Collins; West Coile; Kirk Daubenspeck; Neil Doherty; Vijay D'Souza; Nancy Glover; Sairah Ijaz; Myong Kim; Stephanie Lee; Lee McCracken; Duc Ngo; Sylvia Shanks; John Spence; and Chris Warweg made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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