May 21, 2008

INFORMATION SECURITY

TVA Needs to Enhance Security of Critical Infrastructure Control Systems and Networks

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-08-775T, a testimony before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

The control systems that regulate the nation's critical infrastructures face risks of cyber threats, system vulnerabilities, and potential attacks. Securing these systems is therefore vital to ensuring national security, economic well-being, and public health and safety. While most critical infrastructures are privately owned, the Tennessee Valley Authority (TVA), a federal corporation and the nation's largest public power company, provides power and other services to a large swath of the American Southeast.

GAO was asked to testify on its public report being released today on the security controls in place over TVA's critical infrastructure control systems. In doing this work, GAO examined the security practices in place at TVA facilities; analyzed the agency's information security policies, plans, and procedures in light of federal law and guidance; and interviewed agency officials responsible for overseeing TVA's control systems and their security.

What GAO Recommends

In public and limited distribution reports being issued today, GAO is recommending that TVA take steps to improve implementation of the agency's information security program and to correct specific security weaknesses identified at TVA facilities.

In comments on drafts of GAO's reports, TVA provided information on steps it is taking to implement these recommendations.

To view the full product, including the scope and methodology, click on GAO-08-775T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

TVA had not fully implemented appropriate security practices to secure the control systems used to operate its critical infrastructures at facilities GAO reviewed. Multiple weaknesses within the TVA corporate network left it vulnerable to potential compromise of the confidentiality, integrity, and availability of network devices and the information transmitted by the network. For example, almost all of the workstations and servers that GAO examined on the corporate network lacked key security patches or had inadequate security settings. Furthermore, TVA did not adequately secure its control system networks and devices on these networks, leaving the control systems vulnerable to disruption by unauthorized individuals. Network interconnections provided opportunities for weaknesses on one network to potentially affect systems on other networks. For example, weaknesses in the separation of network segments could allow an individual who gained access to a computing device connected to a less secure portion of the network to compromise systems in a more secure portion of the network, such as the control systems. In addition, physical security at multiple locations that GAO reviewed did not sufficiently protect the control systems. For example, live network jacks connected to TVA's internal network at certain facilities GAO reviewed had not been adequately secured from unauthorized access. As a result, TVA's control systems were at increased risk of unauthorized modification or disruption by both internal and external threats.

An underlying reason for these weaknesses was that TVA had not consistently implemented significant elements of its information security program. For example, the agency lacked a complete and accurate inventory of its control systems and had not categorized all of its control systems according to risk, limiting assurance that these systems are adequately protected. In addition, TVA's patch management process lacked a mechanism to effectively prioritize vulnerabilities. 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.

Numerous opportunities exist for TVA to improve the security of its control systems. For example, TVA can strengthen logical access controls, improve physical security, and fully implement its information security program. If TVA does not take sufficient steps to secure its control systems and fully 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.