May 2008

INFORMATION SECURITY

TVA Needs to Address Weaknesses in Control Systems and Networks

GAO Accountability • Integrity • Reliability

Highlights

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.

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.