September 2007

CRITICAL INFRASTRUCTURE PROTECTION

Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-1036, a report to congressional requesters

Why GAO Did This Study

Control systems—computer-based systems that monitor and control sensitive processes and physical functions—perform vital functions in many of our nation's critical infrastructures, including electric power, oil and gas, water treatment, and chemical production. The disruption of control systems could have a significant impact on public health and safety, which makes securing them a national priority. GAO was asked to (1) determine cyber threats, vulnerabilities, and the potential impact of attacks on critical infrastructure control systems; (2) determine the challenges to securing these systems; (3) identify private sector initiatives to strengthen the cybersecurity of control systems; and (4) assess the adequacy of public sector initiatives to strengthen the cybersecurity of control systems. To address these objectives, we met with federal and private sector officials to identify risks, initiatives, and challenges. We also compared agency plans to best practices for securing critical infrastructures.

What GAO Recommends

GAO is making recommendations to the Department of Homeland Security (DHS) to develop a strategy for coordinating control systems security efforts and to enhance information sharing with relevant stakeholders. DHS officials did not agree or disagree with GAO's recommendations, but stated that they would take them under advisement.

www.gao.gov/cgi-bin/getrpt?GAO-07-1036.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Dave Powner at (202) 512-9286 or at pownerd@gao.gov.

What GAO Found

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. Threats can be intentional or unintentional, targeted or nontargeted, and can come from a variety of sources. Control systems are more vulnerable to cyber attacks than in the past for several reasons, including their increased connectivity to other systems and the Internet. Further, as demonstrated by past attacks and incidents involving control systems, the impact on a critical infrastructure could be substantial. For example, in 2003, a computer virus was blamed for shutting down train signaling systems throughout the East Coast and in 2006, a foreign hacker was reported to have planted malicious software capable of affecting a water filtering plant's treatment operations.

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 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.

Multiple private sector entities such as trade associations and standards setting organizations are working to help secure control systems. Their efforts include developing standards, providing guidance to members, and hosting workshops on control systems security. For example, the electricity industry has recently developed standards for cybersecurity of control systems and a gas trade association is developing guidance for members to use encryption to secure control systems.

Federal agencies also have multiple initiatives under way to help secure critical infrastructure control systems, but more remains to be done to coordinate these efforts and to address specific shortfalls. Over the past few years, federal agencies—including the Department of Homeland Security, the Department of Energy, and the Federal Energy Regulatory Commission (FERC)—have initiated efforts to improve the security of critical infrastructure control systems. However, there is as yet no overall strategy to coordinate the various activities across federal agencies and the private sector. Further, DHS lacks processes needed to address specific weaknesses in sharing information on control system vulnerabilities. Until public and private sector security efforts are coordinated by an overarching strategy and specific information sharing shortfalls are addressed, there is an increased risk that multiple organizations will conduct duplicative work and miss opportunities to fulfill their critical missions.