October 17, 2007

CRITICAL INFRASTRUCTURE PROTECTION

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

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-08-119T, 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

Control systems—computer-based systems that monitor and control sensitive processes—perform vital functions in many of our nation's critical infrastructures such as electric power generation, transmission, and distribution; oil and gas refining; and water treatment and distribution. 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 testify on portions of its report on control systems security being released today. This testimony summarizes the cyber threats, vulnerabilities, and the potential impact of attacks on control systems; identifies private sector initiatives; and assesses the adequacy of public sector initiatives to strengthen the cyber security of control systems. To address these objectives, GAO met with federal and private sector officials to identify risks, initiatives, and challenges. GAO also compared agency plans to best practices for securing critical infrastructures.

What GAO Recommends

In its report, GAO recommends that DHS improve coordination of control systems activities and information sharing (see table). DHS neither agreed nor disagreed with these recommendations, but stated that it would take them under advisement. The agency also discussed new initiatives to develop plans and processes that are consistent with GAO recommendations.

To view the full product, including the scope and methodology, click on GAO-08-119T. For more information, contact Gregory C. Wilshusen at wilshuseng@gao.gov or at (202) 512-6244.

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 2006, a foreign hacker was reported to have planted malicious software capable of affecting a water filtering plant's water treatment operations. Also in 2006, excessive traffic on a nuclear power plant's control system network caused two circulation pumps to fail, forcing the unit to be shut down manually.

Multiple private sector entities such as trade associations and standards setting organizations are working to help secure control systems. Their efforts include developing standards and providing guidance to members. For example, the electricity industry has recently developed standards for cyber security 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 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, the Department of Homeland Security (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, there is an increased risk that multiple organizations will conduct duplicative work. In addition, until information-sharing weaknesses are addressed, DHS risks not being able to effectively carry out its responsibility for sharing information on vulnerabilities with the private and public sectors.

GAO Recommendations to DHS

- Develop a strategy to guide efforts for securing control systems, including agencies' responsibilities, as well as overall goals, milestones, and performance measures.
- Establish a rapid and secure process for sharing sensitive control system vulnerability information with critical infrastructure control system stakeholders, including vendors, owners, and operators.