CRITICAL INFRASTRUCTURE PROTECTION

Challenges and Efforts to Secure Control Systems

What GAO Found

In addition to general cyber threats, which have been steadily increasing, several factors have contributed to the escalation of the risks of cyber attacks against control systems. These include the adoption of standardized technologies with known vulnerabilities and the increased connectivity of control systems to other systems. Typical control system components are illustrated in the graphic below. Control systems can be vulnerable to a variety of attacks, examples of which have already occurred. Successful attacks on control systems could have devastating consequences, such as endangering public health and safety.

Securing control systems poses significant challenges, including limited specialized security technologies and lack of economic justification. The government, academia, and private industry have initiated efforts to strengthen the cybersecurity of control systems. The President’s National Strategy to Secure Cyberspace establishes a role for DHS to coordinate with these entities to improve the cybersecurity of control systems. While some coordination is occurring, DHS’s coordination of these efforts could accelerate the development and implementation of more secure systems. Without effective coordination of these efforts, there is a risk of delaying the development and implementation of more secure systems to manage our critical infrastructures.

Typical Components of a Control System

![Diagram of a control system with various components including enterprise network, control system, supervisory control and monitoring station, redundant application servers, engineering workstation, human-machine interface (HMI), communications network, remote/local stations, sensors, control equipment, and handheld devices.](source: GAO (analyst), Art Explosion (clipart))