How to Obtain the Document

The *Cyber Security Procurement Language for Control Systems* may be downloaded from the ICS-CERT Web site.

Contributors

CSSP also acknowledges the significant involvement and support from New York Office of Cyber Security and Critical Infrastructure and the SANS Institute to the development of the *Cyber Security Procurement Language for Control Systems*.

Department of Homeland Security

The Homeland Security Act of 2002 provides the basis for the Department of Homeland Security's (DHS) responsibilities in the protection of the Nation's Critical Infrastructure/Key Resources (CI/KR). The DHS National Cyber Security Division (NCSD) works collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets. To protect the cyber infrastructure, NCSD has identified two overarching objectives: to build and maintain an effective national cyberspace response system and to implement a cyber risk management program for protection of critical infrastructure.

To lead this effort, NCSD established the CSSP to guide a cohesive effort between government and industry to reduce the cyber risk to industrial control systems. CSSP does this by providing guidance, preparing informational products and bulletins, building partnerships, and analyzing and responding to incidents.

Learning More

If you are interested in learning more about CSSP and its efforts related to control systems security, visit the Web site.

Contact Information Email:

ics-cert@hq.dhs.gov

Homeland Security

Cyber Security Procurement Language for Control Systems

Building Security into Control Systems

Homeland Security

Cyber Security Procurement Language for Control Systems

The *Cyber Security Procurement Language for Control Systems* summarizes security principles that should be considered when developing system specifications and procuring control systems products (software, systems, and networks) and provides example language to incorporate into procurement specifications. The guidance is offered as a resource for informative use—it is not intended as a policy or standard. This document serves as a "tool kit" designed to reduce cyber security risks in control systems through the procurement cycle to assist with the management of known vulnerabilities and weaknesses by delivering more secure systems. The *Cyber Security Procurement Language for Control Systems* targets high-value security risk reduction opportunities that can be achieved through the procurement cycle.

The *Cyber Security Procurement Language for Control Systems* document includes guidelines for specifying vendor requirements for a more secure configuration. The tool kit includes a collection of security requirements that map directly to vulnerabilities that have been observed in current and legacy control systems and that can be mitigated by technology providers and organizations through effective management of the technology across its operational lifespan.

Scope of the Document

The *Cyber Security Procurement Language for Control Systems* was developed by the Department of Homeland Security (DHS) Control System Security Program (CSSP). This document provides procurement guidance and contains security principles that should be considered when procuring control systems. Example language is included to incorporate into control system procurement specifications.

The *Cyber Security Procurement Language for Control Systems* includes topics such as:

- System Hardening
- Perimeter Protection
- Account Management
- Coding Practices
- Flaw Remediation
- Malware Detection & Protection
- Host Name Resolution

Other topics may be considered for inclusion in future versions, as recommended by stakeholders.

Control System Benefits

Control system security vulnerabilities can be inadvertently introduced when customers do not specify appropriate security attributes in the procurement process. By using the *Cyber Security Procurement Language for Control Systems* guidance when a control system is purchased or upgraded, customers can address and prevent many cyber security vulnerabilities. The *Cyber Security Procurement Language for Control Systems* document enables asset owners to request security "built-in" rather than "bolted on."