How to Obtain the Document

The procurement language is available and may be downloaded at the Multi-State Sharing and Analysis Center (MS-ISAC) website (http://www.msisac.org/scada/). Once at the Website users should click on hyper link text, "Cyber Security Procurement Language for Control Systems."

Cyber Security Procurement Language for Control Systems

There has been significant involvement by the Department of Homeland Security, the Department of Energy, National Laboratories, State Agencies, Private Industry, and Vendors in support of this effort. If you would like more information or would like to get involved with enhancing the cyber security requirements of control systems specifications, visit http://www.msisac.org/scada/registration/

Getting Involved

If you are interested in learning more about the Department of Homeland Security Control Systems Security Program (CSSP) and its efforts related to control systems security, visit the CSSP web site: http://www.us-cert.gov/control_systems/

Or contact us at cssp@dhs.gov

Homeland Security

Building Security into Control Systems

Cyber Security Procurement Language for Control Systems

Homeland Security

Cyber Security Procurement Language for Control Systems

The "Cyber Security Procurement Language for Control Systems" is a document that summarizes security principles that should be considered when designing and procuring control systems products (software, systems, and networks) and provides example language to incorporate into specifications, which addresses these concerns. The guidance is offered as a resource for informative use—it is not intended as a policy or standard. This document is a “tool kit” designed to reduce cyber security risk in control systems by asking technology providers, through the procurement cycle, to assist in managing known vulnerabilities and weaknesses by delivering more secure systems. It initially targets high-value security risk reduction opportunities achieved through the procurement cycle.

Guidelines are also provided for requesting specifications from the vendor for associated equipment not directly provided by the vendor. The goal is to cover new control systems, legacy systems, and maintenance of control systems. The guide is written to make it easy for users to determine which guidelines are appropriate to use for their systems.

Control System Benefits

Control system security vulnerabilities often arise due to the customer not requesting or knowing which security attributes to request in the procurement process. By utilizing the Cyber Security Procurement Language for Control Systems document when a system is upgraded, or a control system is ordered, many cyber security vulnerabilities will be addressed and possibly prevented. The Cyber Security Procurement Language for Control Systems document enables asset owner to request security "built-in" rather than "bolted on."

Status of the Document

The "Cyber Security Procurement Language for Control Systems" is available in draft form. This document provides procurement guidance and contains security principles that should be considered when designing and procuring control systems. Example language is included to incorporate into control system procurement specifications, and future cyber security topics are identified that will be addressed in upcoming revisions to the document. Currently there are 17 topics addressed in the Cyber Security Procurement Language for Control Systems document. This includes:

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

Other topics will be considered for inclusion as requested by control system users.