



**Process Control Systems
Industry Conference**

Raising the Bar On Build-In Cyber Security

Rita Wells

Idaho National Laboratory

August 27, 2008

Cyber Security Procurement Language for Control Systems

Background

Foundation

Use: When, How

Content

Future Direction

Department of Homeland
Security: Cyber Security
Procurement Language for
Control Systems

August 2008



Control Systems Security Program
National Cyber Security Division



Background: Procurement Language for Control Systems



**Homeland
Security**

Main Contributors:

Department of Homeland Security – NCSD/CSSP

Department of Energy – NSTB

Idaho National Laboratory

Asset Owners, Vendors

New York State

SANS



U.S. Department of Energy
Office of Electricity Delivery
and Energy Reliability



Idaho National Laboratory



Multi-State
Information Sharing and Analysis Center
MS-ISAC

MSISAC ALERT LEVEL
LOW



Latest Release

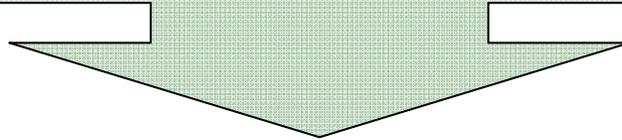
August 2008 – Version 2.0

http://www.us-cert.gov/control_systems



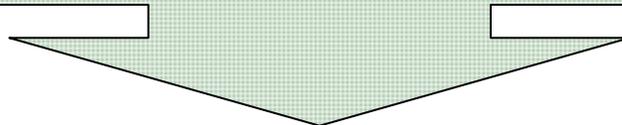
Risk Reduction

Work with public and private sectors to reduce vulnerabilities and minimize the severity of cyber attacks



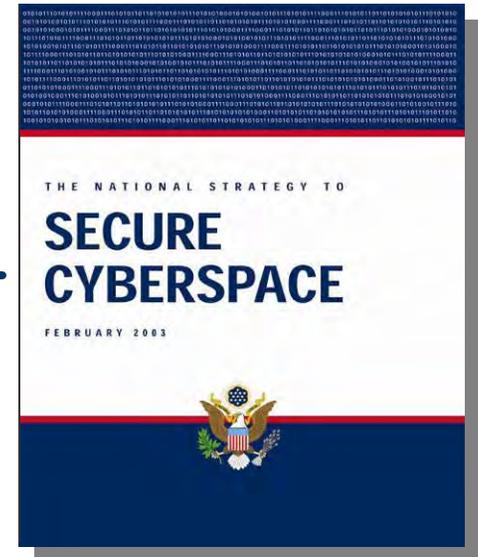
Software Assurance

A Strategic Initiative to Promote Integrity, Security, and Reliability in Software



Procurement Specification for Control Systems

Initiative to develop procurement language for control systems (hardware and software)



Project Goal & Scope

Goal

Develop common procurement requirements and contractual language that the owners can use to ensure control systems they are buying or maintaining have the best available security

Scope

- ◆ *New control systems*
- ◆ *Maintenance of systems*
- ◆ *Legacy systems*
- ◆ *Information and personnel security*

Foundation

Analyzed 54 Assessments:

Assessments funded by DHS, DOE, Industry, and Asset-owners

Each assessment ranges from 275-800 hours of cyber security researcher and additional efforts for control system and network engineers

20 in-lab and 18 on-site assessments

Identified common vulnerabilities

Also identified unique defensive architectures



When to Use: New Systems

- ▶ *Request for Proposal*
- ▶ *Proposal Submittal*
- ▶ *Bid Review*
- ▶ *Contract Award*
- ▶ *Statement of Work*
- ▶ *Design Review*
- ▶ *Document Review*
- ▶ *Factory Acceptance Testing*
- ▶ *Site Acceptance Testing*
- ▶ *Maintenance*



When to Use: Legacy Systems

Negotiating a new maintenance contract

Applying Upgrades

Accepting Updates

Applying security add-ons

*Procurement
Language*

*FAT
Measurements*

*SAT
Measurements*

Maintain

How to Use: Security Culture

Not a cut and paste

Still need to engineer system and understand the architecture, functional requirements and operational constraints

Does your company have past experience:

Need for an ongoing security program (not a one time project)

Strong security culture or outsource?

Accustom to providing adequate funding for security

Have adequate security staff for support



How to use: Functional Architecture Procurement Language

Aggressive project designed to provide a “buyers” tool kit

Provide security requirements for inclusion into RFPs

Use common, grounded and valuable language

Support Bid Reviews (gauge responsiveness)

*Provide the detail required to support SOW development
and Design Creation & Review*

Starting with greatest risk that can be addressed



Factory Acceptance Test Measurements

Linked to the procurement requirement

Provides language to include in Factory Acceptance Testing requirements and specifications

Designed to validate the requirement has been met

Allows for rigorous security testing in an isolated environment

Gives the vendor the opportunity to verify the product meets the security requirements prior to installation in the field.



Site Acceptance Test Measurements

Linked to the procurement requirement

Provides language to include in Site Acceptance Testing requirements and specifications

Designed to validate the risk reducing requirement is not lost during implementation in the Asset Owners environment

Important step that requires an understanding of “why it was delivered that way”

First hand-off from the procurement / provider team to the actual operator and maintainer



Maintenance Language & Operating Guidance

Linked to the procurement requirement

Provides language to include in maintenance contracts

Designed to further reduce the risk to control systems during their life-time

Critical step to ensure the benefits of the security requirements are not lost during the technologies operational lifespan

Requires an understanding of “why it was delivered that way”



Procurement Language Topics - continued

End Devices

- Intelligent electronic Devices
- Remote Terminal Units
- Programmable Logic Controllers
- Sensors, Actuators and Meters

Remote Access

- Dial up Modems
- Dedicated Line Modems
- TCP/IP
- Web-based Interfaces
- Virtual Private Networks
- Serial Communications

Physical Security

- Access of Cyber Components
- Perimeter Access
- Manual Override Control
- Intra-perimeter Communications

Network Partitioning

- Network Devices
- Network Architecture

**Department of Homeland
Security: Cyber Security
Procurement Language for
Control Systems**

August 2008



Control Systems Security Program
National Cyber Security Division



A Page From the Tool Kit: Format

Procurement Topic

Security Risk or Basis Description

Language Guidance

Procurement Language

Factory Acceptance Test Measurements

Site Acceptance Test Measurements

Maintenance and Operations Guidance

References or Standards

Dependencies

11.4 Intra-perimeter Communications

Mechanisms within the perimeter may rely on intra-perimeter communication to ensure secure operation. The communication medium may consist of a physical, electrical (fly-by-wire), or wireless connection.

11.4.1 Basis

Intra-perimeter communications are commonly overlooked for security concerns. Access to the intra-perimeter communication medium constitutes access to the function or device itself with the potential for exploit and damage. The communication path must be physically secured to the same level as the components.

11.4.2 Language Guidance

The length and complexity of the communication channel to be protected should be minimized. The communication channel and access ports should also be hidden from view, out of reach, and/or behind layers of perimeter security if possible. A conduit may be placed around the communication medium to provide additional resistance to tampering. Wireless communication should not be detectable or accessible outside the perimeter.

11.4.3 Procurement Language

The Vendor shall verify and provide documentation that physical communication channels are secured from physical intrusion.

The Vendor shall verify and provide documentation that the range of the wireless communications is limited to within the perimeter.

The Vendor shall verify and provide documentation that communication channels are as direct as possible.

11.4.4 FAT Measures

The Vendor shall verify and provide documentation that the range of the wireless communications is limited to the required area.

The Vendor shall verify and provide documentation that the physical intrusion of communication channels is detectable.

11.4.5 SAT Measures

The Vendor shall verify and provide documentation that the range of the wireless communications is limited to within the perimeter.

The Vendor shall verify and provide documentation that the physical intrusion of communication

Vendors

Audience is for asset owners or buyers of systems

Support the vendors by addressing technology security problems they deal with as buyers of components

- Important trend: Control System company is an integration & software effort

Provide value to vendors which will pass on to asset owners, start the security dialog in a common language



International Outreach

Pressure from multiple markets

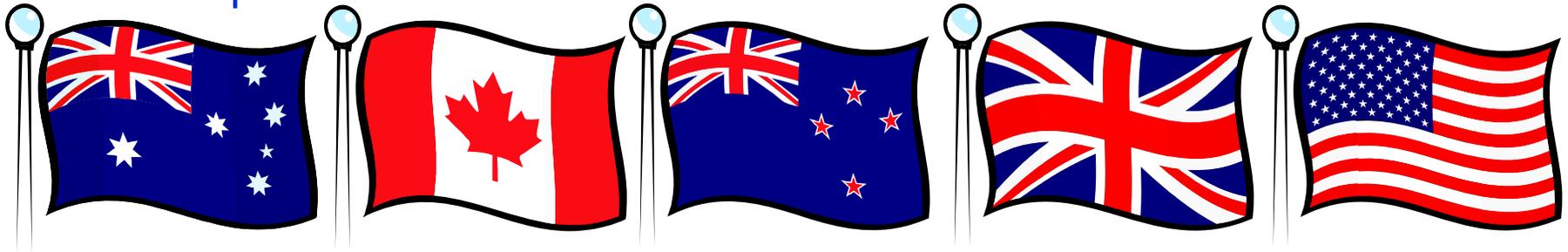
Europe & Asia

International participation & interest

15 countries

UK & Australia taking leadership role

European Union discussions



Participant Creation

Develop an “Open Contribution” framework

Shift drafting from drafting team to participants

Need to set up quality review process and rules

190+ asset owner members

Multiple stakeholder communities

Allow other programs to support (CPNI, AUS Gov, etc.)

Sectors take ownership to apply sections needed unique to architectures

System Integrators use as baseline

Vendors use as discussion points

Discussion

Gary J. Finco
Idaho National Laboratory
gary.finco@inl.gov
208-526 7048

Rita Wells
Idaho National Laboratory
rita.wells@inl.gov
208-526 3179