# Cyber Security Procurement Language for Control Systems

Rita Wells

Idaho National Laboratory

Program Sponsor:

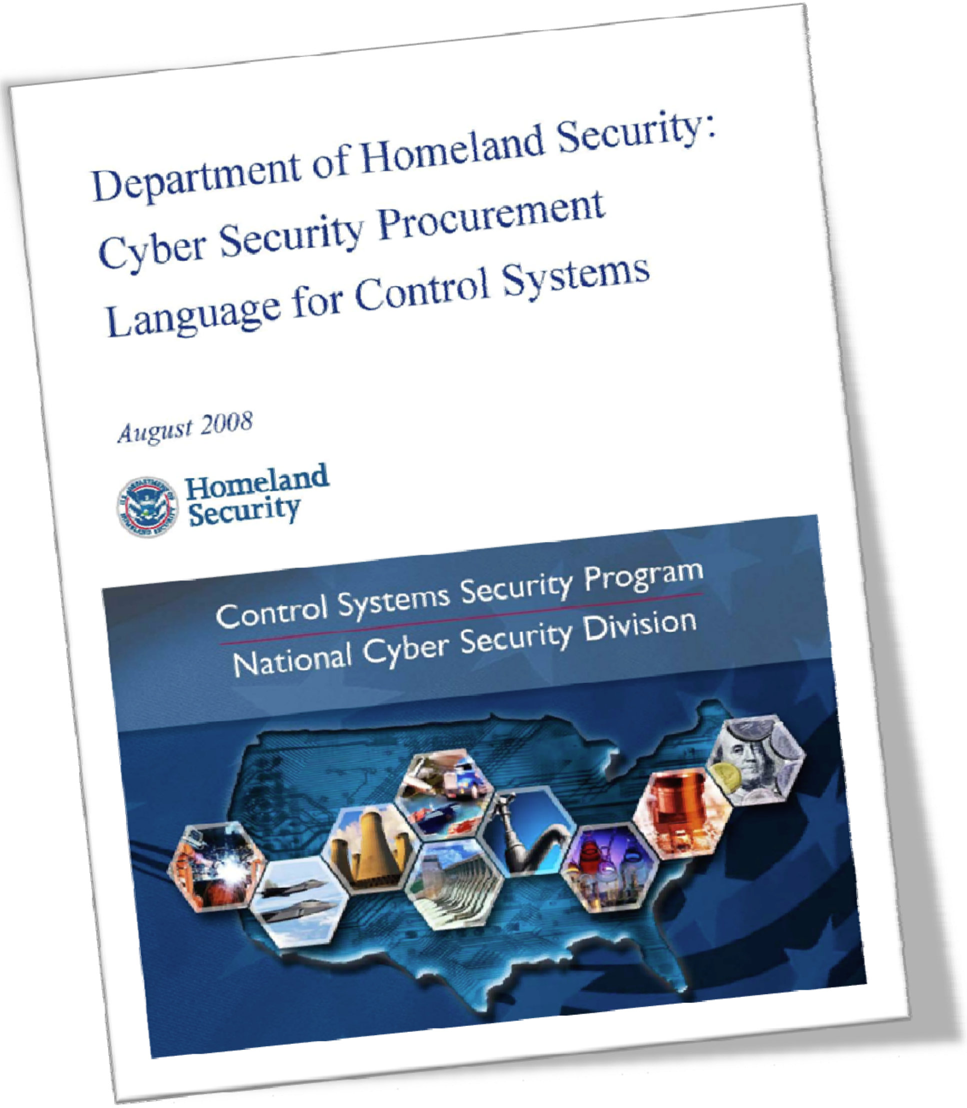
National Cyber Security Division

Control Systems Security Program

Homeland Security

# Agenda

- Background
- Foundation
- How to Use the Document
- Content



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

*August 2008*

Homeland Security

Control Systems Security Program

National Cyber Security Division

Homeland Security

# Background

**Sponsor**

- DHS Control Systems Security Program

**Contributors**

- Idaho National Laboratory
- New York State
- SANS

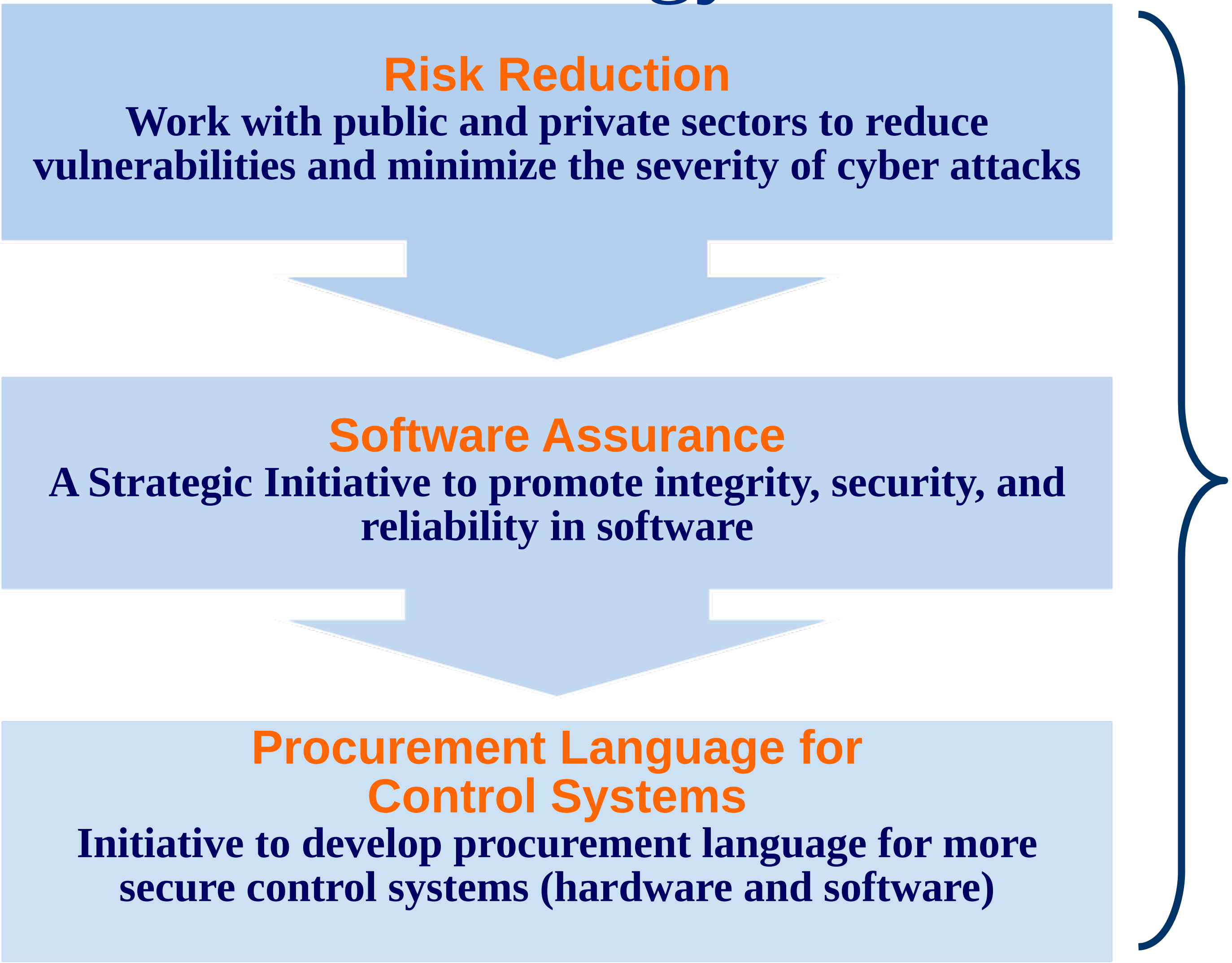
**Cyber Security Procurement Language Project Workgroup**

- 242 public and private sector entities from around the world representing asset owners, operators, vendors, and regulators.

**DHS Latest Release – August 2008**

**http://www.us-cert.gov/control_systems/pdf/SCADA_Procurement_DHS_Final_to_Issue_08-19-08.pdf**

# National Strategy



**Risk Reduction**

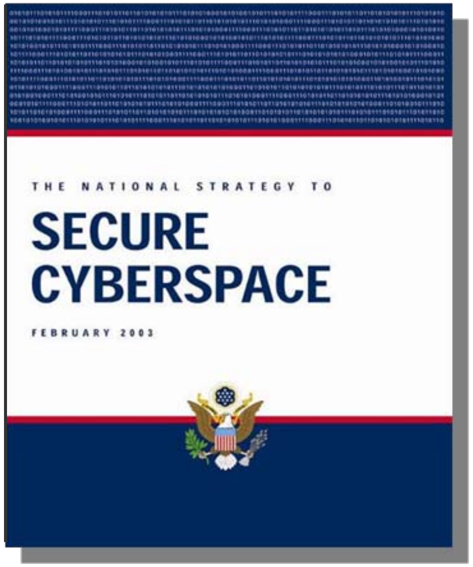
**Work with public and private sectors to reduce vulnerabilities and minimize the severity of cyber attacks**

**Software Assurance**

**A Strategic Initiative to promote integrity, security, and reliability in software**

**Procurement Language for Control Systems**

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



THE NATIONAL STRATEGY TO

SECURE CYBERSPACE

FEBRUARY 2003

# Project Goal & Scope

## Goal

- Develop common procurement requirements and contractual language that the owners can use to ensure control systems they are purchasing or maintaining have the best available security integrated into the operational lifecycle.

## Scope

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

# Foundation

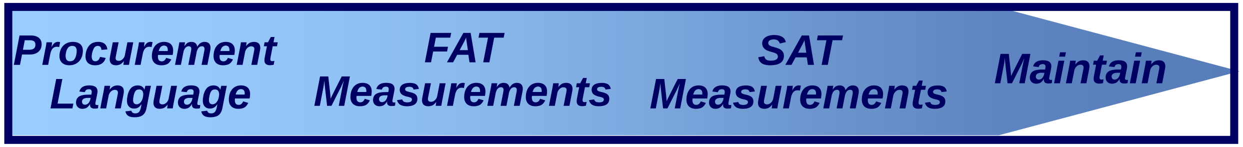
***Analyzed 57 Assessments:***

- Assessments sponsored by DHS National Cyber Security Division, Department Of Energy-Office of Electricity Delivery and Energy Reliability (DOE-OE), Industry, and Asset-owners
- Each assessment ranges from 275-900 hours utilizing cyber security researchers, control system experts, and network engineers
- Assessment breakdown:
  - 31 at the Idaho National Laboratory
  - 19 on-site
  - 7 component
- Assessments identified common vulnerabilities and unique defensive architectures

Homeland Security

# 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



Procurement Language

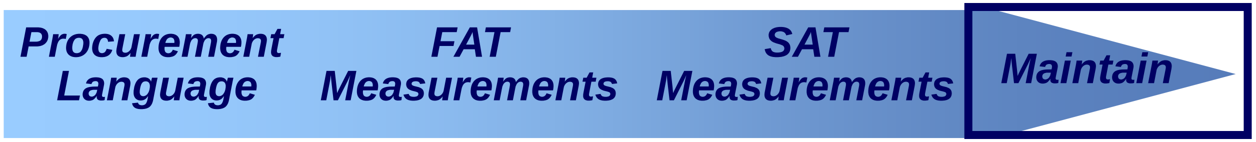
FAT Measurements

SAT Measurements

Maintain

# 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:

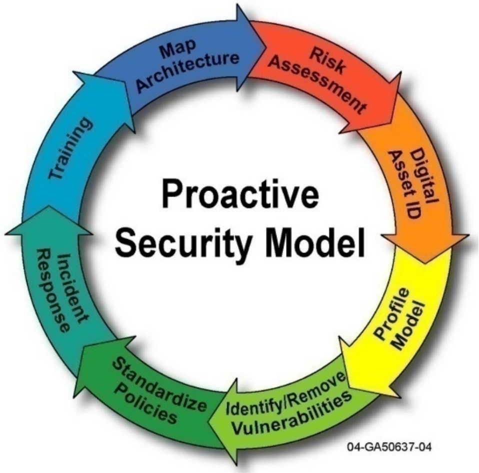
Changing the Security Culture

## Understand your company’s past experience:

- Need for an ongoing security program (not a one time project)
- Provide adequate resources for security
- Strong security culture or outsource
- Maintain adequate security staff for support

## Modify, Customize, Tailor

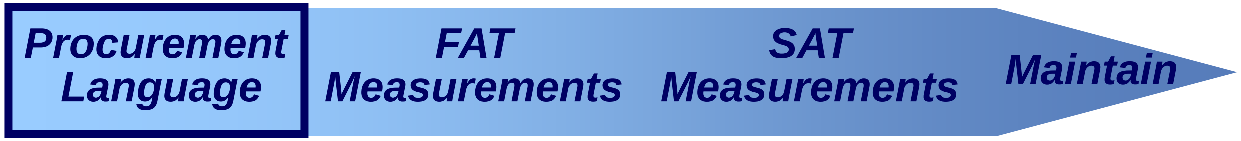
- Organizations need to engineer system and understand the architecture, functional requirements, and operational constraints
- Can not ***“cut and paste”*** document as a whole



# How to Use:

## Functional Architecture Procurement Language

- Provides a tool kit for “buyers”
- Provides security requirements for inclusion into Request For Proposal
- Provides common language
- Supports Bid Reviews (gauge responsiveness)
- Provides the details necessary to support Statement Of Work development and Design Creation & Review



Procurement Language

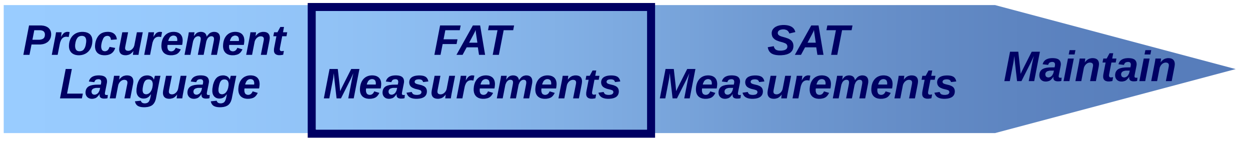
FAT Measurements

SAT Measurements

Maintain

# Factory Acceptance Test Measurements

- Provides measurement requirements
- Provides language to include in Factory Acceptance Testing requirements and specifications
- Provides a process to validate requirements
- Provides for security testing in an isolated environment
- Provides the vendor an opportunity to verify that the requested product meets the security requirements prior to installation



**Procurement Language**

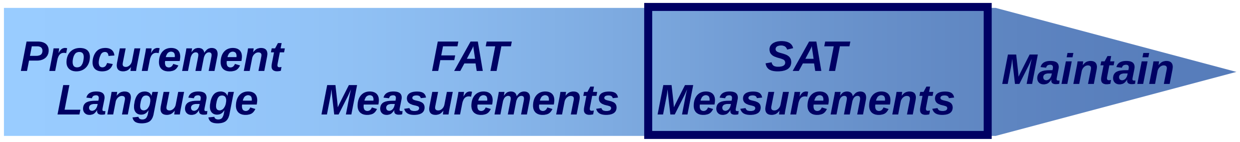
**FAT Measurements**

**SAT Measurements**

**Maintain**

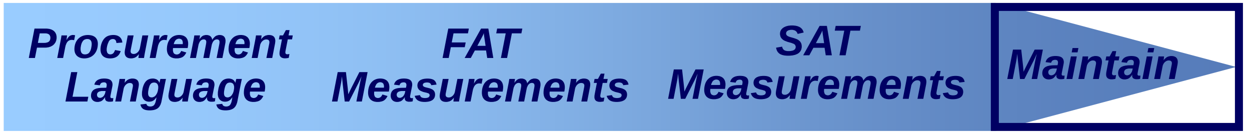
# Site Acceptance Test Measurements

- Provides measurement requirements
- Provides language to include in Site Acceptance Testing requirements and specifications
- Provides a process to validate the risk mitigation requirements during implementation
- Provides acknowledgement of security integration
- Provides a documented security process from the procurement provider to the operator and maintainer



# Maintenance Language & Operating Guidance

- Provides measurement requirements
- Provides language to include in maintenance contracts
- Provides clear requirements to reduce the cyber risk to control systems during lifecycle
- Provides steps to ensure the benefits of the security requirements are maintained during operational lifecycle
- Provides an understanding of “why it was delivered that way”



Procurement Language

FAT Measurements

SAT Measurements

Maintain

# Procurement Language Topics

## System Hardening

- Removal of Unnecessary Services and Programs
- Host Intrusion Detection systems
- Changes for File Systems and OS Permissions
- Hardware Configuration
- Heartbeat Signals
- Installing OS, applications, and 3rd party software updates

## Perimeter Protection

- Firewalls
- Network Intrusion Detection System
- Canaries

## Account Management

- Disabling, Removing, or Modifying Well-Known or Guest Accounts
- Session Management
- Password/Authentication Policy and Management
- Account audit and Logging
- Role-based Access Control
- Single Sign-on
- Separation Agreement

## Coding Practices

- Coding for Security

## Flaw Remediation

- Notification and Documentation from Vendor
- Problem Reporting

# Procurement Language Topics

(Continued)

## Malware Detection and Protection

- Malware Detection and Protection

## Host Name Resolution

- Network Addressing and Name Resolution

## 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 Security

## Physical Security

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

## Network Partitioning

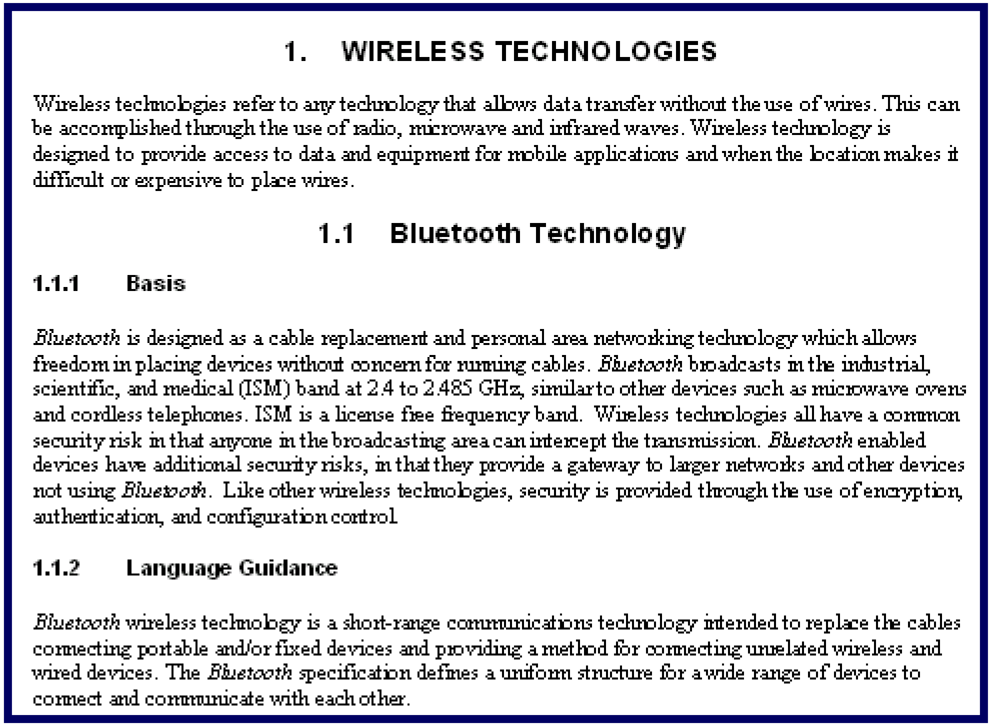
- Network Devices
- Network Architecture

Homeland Security

# DHS will Address Additional Topics

## For 2009

- **Fall - Online version will be available**
- **Spring - New Topic - Wireless**
  - Bluetooth
  - 802.11
  - ZigBee
  - RF
  - Cellular
  - WiMax
  - Wireless HART
  - Wireless Mesh



### 1. WIRELESS TECHNOLOGIES

Wireless technologies refer to any technology that allows data transfer without the use of wires. This can be accomplished through the use of radio, microwave and infrared waves. Wireless technology is designed to provide access to data and equipment for mobile applications and when the location makes it difficult or expensive to place wires.

### 1.1 Bluetooth Technology

**1.1.1 Basis**

*Bluetooth* is designed as a cable replacement and personal area networking technology which allows freedom in placing devices without concern for running cables. *Bluetooth* broadcasts in the industrial, scientific, and medical (ISM) band at 2.4 to 2.485 GHz, similar to other devices such as microwave ovens and cordless telephones. ISM is a license free frequency band. Wireless technologies all have a common security risk in that anyone in the broadcasting area can intercept the transmission. *Bluetooth* enabled devices have additional security risks, in that they provide a gateway to larger networks and other devices not using *Bluetooth*. Like other wireless technologies, security is provided through the use of encryption, authentication, and configuration control.

**1.1.2 Language Guidance**

*Bluetooth* wireless technology is a short-range communications technology intended to replace the cables connecting portable and/or fixed devices and providing a method for connecting unrelated wireless and wired devices. The *Bluetooth* specification defines a uniform structure for a wide range of devices to connect and communicate with each other.

# Organizations Leveraging the Procurement Language

- DOE-OE National SCADA Testbed (NSTB)
  - Spring 2009 Wireless specification for AMI
- International Community
- Control Systems Vendors
- Asset Owners/Operators

# Cyber Security: A Shared Responsibility

**Report general cyber incidents & vulnerabilities**

- www.us-cert.gov or soc@us-cert.gov
- 703-235-5111, 888-282-0870

**Sign up for cyber alerts**

- www.us-cert.gov

**Report Control Systems cyber incidents & vulnerabilities**

- ics-cert@dhs.gov
- 703-235-5111, 888-282-0870

**Learn more about Control Systems Security Program**

- www.us-cert.gov/control_systems
- cssp@dhs.gov

Homeland
Security

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland Security