Control Systems Security Program (CSSP)

Vishant Shah, Deputy Director

Control System Security Program

National Cyber Security Division (NCSD)

Homeland Security

Overview

- Control Systems Security Challenges
- NCSD's Control System Security Program
  - Recommended Procurement Language
  - Technology Assessments
  - Self Assessment Tool
- Areas for Study
  - Safety Systems
  - Managed Security Services

Homeland Security

Control Systems Security Challenges

Security Topic	Information Technology	Control Systems
Anti-virus & mobile-code counter measures	Common & widely used	Uncommon & difficult to deploy
Support technology lifetime	3-5 years	Up to 20 years
Outsourcing	Common & widely used	Rarely used
Application of patches	Regular/ scheduled	Slow (vendor specific)
Change management	Regular/ scheduled	Legacy based – unsuitable for modern security
Time critical content	Delays are generally accepted	Critical due to safety delays unacceptable
Availability	Delays are generally accepted	24x7 x 365 availability means delays unacceptable
Security awareness	Good in both private & public sector	Generally poor regarding cyber security
Security testing / audit	Scheduled & mandated	Occasional testing for outages
Physical security	Secure	Very good but often remote & unmanned

CSSP Strategic Overview

Goal

Reduce Cyber Risk to Critical Infrastructure Control Systems

Key Objectives

Provide Guidance
- *Outreach & Awareness*
- *Risk Reduction Products*
- *Technology Assessments*

Develop Partnerships
- *Government*
- *Industry*
- *Academia*
- *International*

Prepare & Respond
- *Situational Awareness*
- *Scenario Development*
- *Vulnerability & Threat*
- *Incident Analysis & Response*

Homeland Security

Risk Reduction Products

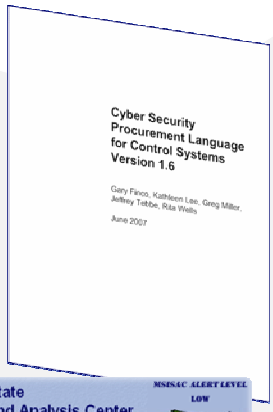
Cyber Security Procurement Language for Control Systems

Building Security into Control Systems

Provides sample or recommended language for control systems security requirements

- New SCADA / control systems
- Legacy systems
- Maintenance contracts

Website: http://www.msisac.org/scada/



Multi-State
Information Sharing and Analysis Center
MS-ISAC

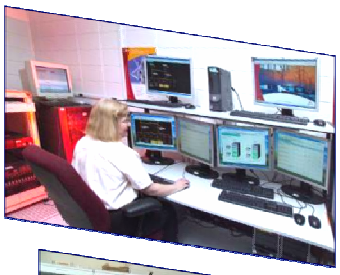
MSISAC ALERT LEVEL
LOW

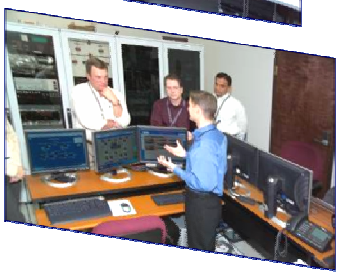
Homeland Security

Technology Assessments

Vendor Assessment Objectives

- Partnership created with the vendor
- Utilizing expertise at national laboratories to evaluate control systems
- Benefits:
  - Identify specific cyber security vulnerabilities
  - Work with vendors to develop effective mitigation strategies
  - Vendors provide patches & improved products to stakeholder community

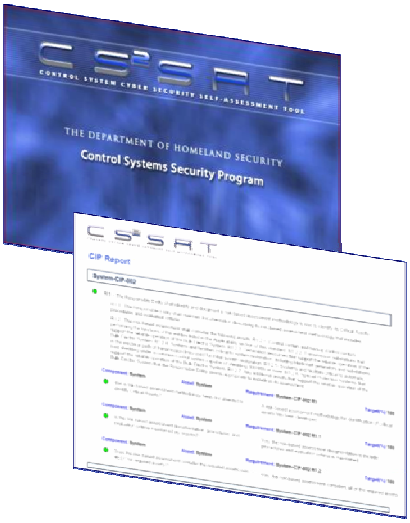




Homeland Security

Risk Reduction Products
Desktop Analysis Tool – CS2SAT

- Based on industry standards
- Capability:
  - Creates baseline security posture
  - Provides recommended solutions to improve security posture
  - Standards specific reports (e.g. NERC CIP, DOD 8500.2)



Homeland Security

Areas for Further Study

- Safety Instrumented Systems (SIS)
  - SIS provides a final fail safe to prevent catastrophic control systems failure
  - Should use the most trusted devices and software
- Managed Security Services
  - As with enterprise IT, control systems operators are beginning to use 3rd party services to provide management and monitoring of control systems security devices
  - Emphasis needs to be placed on who ultimately is providing the services (i.e., no third party outsourcing)

Homeland Security

Questions?

- Cyber security is a shared responsibility
  - Report cyber incidents and vulnerabilities at www.us-cert.gov, soc@us-cert.gov, 703-235-5110, or 888-282-0870
  - Sign up for cyber alerts at www.us-cert.gov
  - Learn more about CSSP at www.us-cert.gov/control_systems
- Contact information

  cssp@hq.dhs.gov

Homeland Security