

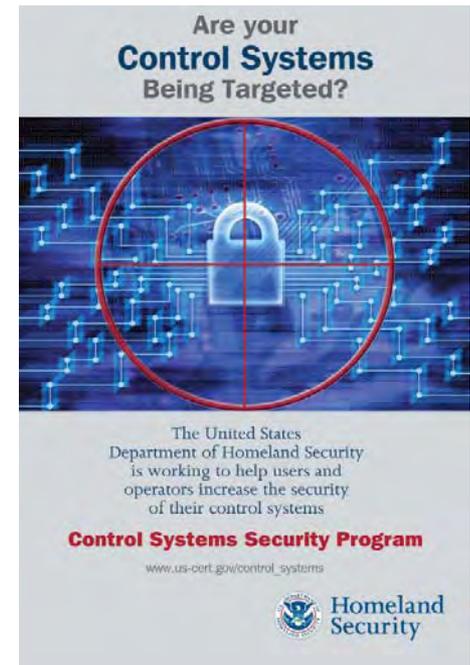
Control Systems Security Program Recommended Practices

**Trent D. Nelson, Idaho National Laboratory
Control Systems Security Program
PCSF March 6-8, 2007**

DHS Control Systems Security Program

- The sponsor for this effort is the Department of Homeland Security (DHS) Control Systems Security Program (CSSSP)
- The goal of the CSSSP is to

“Reduce Cyber Risk to Critical Infrastructure Control Systems by providing guidance and building partnerships”



Recommended Practices

Objective:

Identify and recommend practical and actionable security practices that have been vetted by control systems security experts, the government, and industry to describe security solutions which can be applied to reduce cyber risk to control systems.

Key aspects:

- Central location (www.us-cert.gov/control_systems)
- Industry clearinghouse and development for recommended practices
- Oversight Committee
- All practices vetted with Industry and government experts
- Industries accepted best practices by the control systems community is officially recognized by CSSP

Recommended Practices Update

- ◆ **NCSA announced the development of the Recommended Practices Website at PCSF 2006**
- ◆ **The Website went Live on June 1, 2006**
- ◆ **Website Content:**
 - Overview of Vulnerabilities
 - Cyber Threats
 - Standards and References
 - 103 best practices and security guides
 - http://www.us-cert.gov/control_systems/csstandards.html
 - Training
 - Secure Architecture Design
 - Recommended Practices

Recommended Practices Standards and References

Category List:

- **Cyber Security Policy Planning and Preparation**
- **Establishing Network Segmentation, Firewalls, and DMZs**
- **Patch, Password, and Configuration Management**
- **Control Systems Cyber Security Training**
- **Establishing and Conducting Asset, Vulnerability, and Risk Assessments**
- **Control System Security Procurement Requirements Specification**
- **Placement and Use of IDSs and IPDSs**
- **Authentication, Authorization, and Access Control**
- **Securing Wireless Connections**
- **Use of VPNs and Encryption in Securing Communications**
- **Establishing a Secure Topology and Architecture**
- **Applying and Complying with Security Standards**
- **Ensuring Security when Modernizing and Upgrading**

Recommended Practices Focus Areas:

- Awareness & Training
 - Centre for the Protection of National Infrastructure (CPNI) – National Infrastructure Security Co-ordination Centre (NISCC) Good Practice Guide – Improve Awareness and Skill
- System Administration & Mitigations
 - Mitigations for Security Vulnerabilities found in Control System Networks
 - Site-Scripting Mitigation (Vulnerability Bulletin)
 - Wireless for Control Systems (IEEE802.11i)
 - Wireless for Control Systems (IEEE802.15.4 – Zigbee)

Recommended Practices Focus Areas: (Cont.)

- ◆ Incident Response
 - CPNI Good Practice Guide – Establish response capabilities
- ◆ Policies, Plans & Procedures
 - Building Security Culture/OPSEC
 - CPNI Good Practice Guide – Establish ongoing governance
- ◆ Development and Acquisition
 - SANS/INL Procurement Language (Link)
 - CPNI Good Practice Guide – Engage projects

Recommended Practices Focus Areas: (Cont.)

- ◆ Systems Lifecycle Maintenance Support
 - CPNI Good Practice Guide – Manage third party risks
- ◆ Secure Architecture
 - Control Systems Cyber Security: Defense in Depth Strategies
 - CPNI Good Practice Guide – Firewall Development
 - CPNI Good Practice Guide – Implement secure architecture
- ◆ Configuration Management
- ◆ Systems Risk Management
 - CPNI Good Practice Guide – Understanding the business risk

Development & Review Process

Recommended Practices Oversight Committee (RPOC):

- Guides recommended practice prioritization and development
- Accuracy of content
- Standards validation

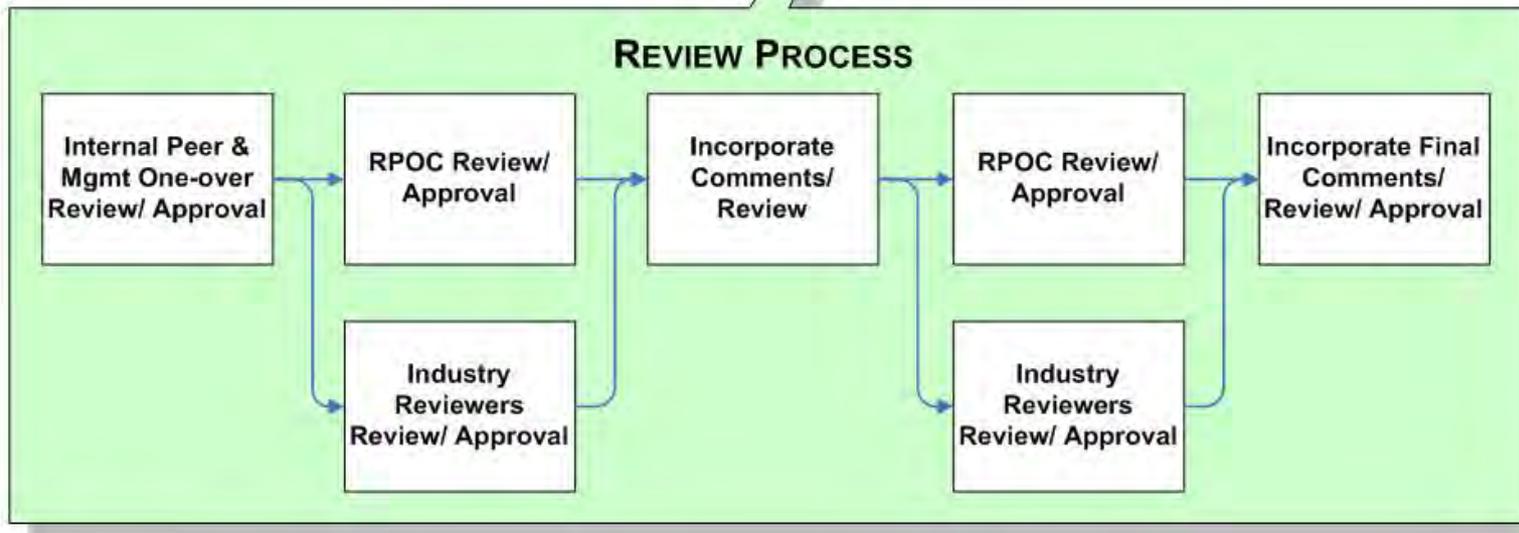
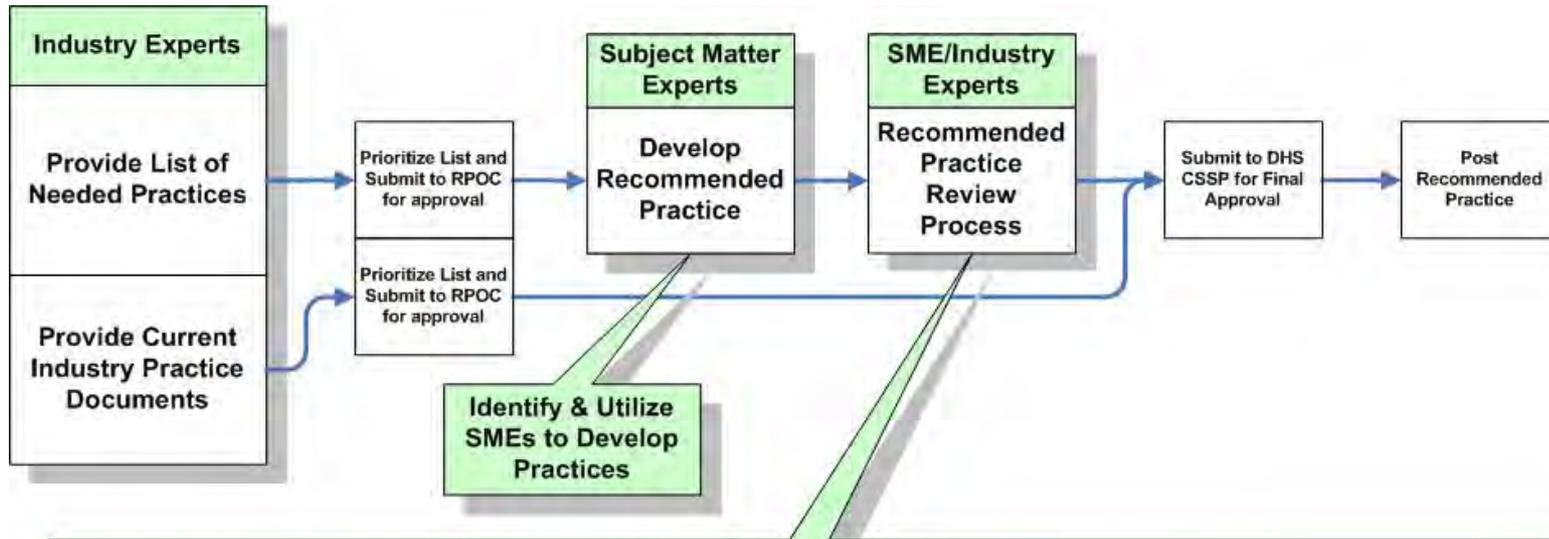


Vetting Process:

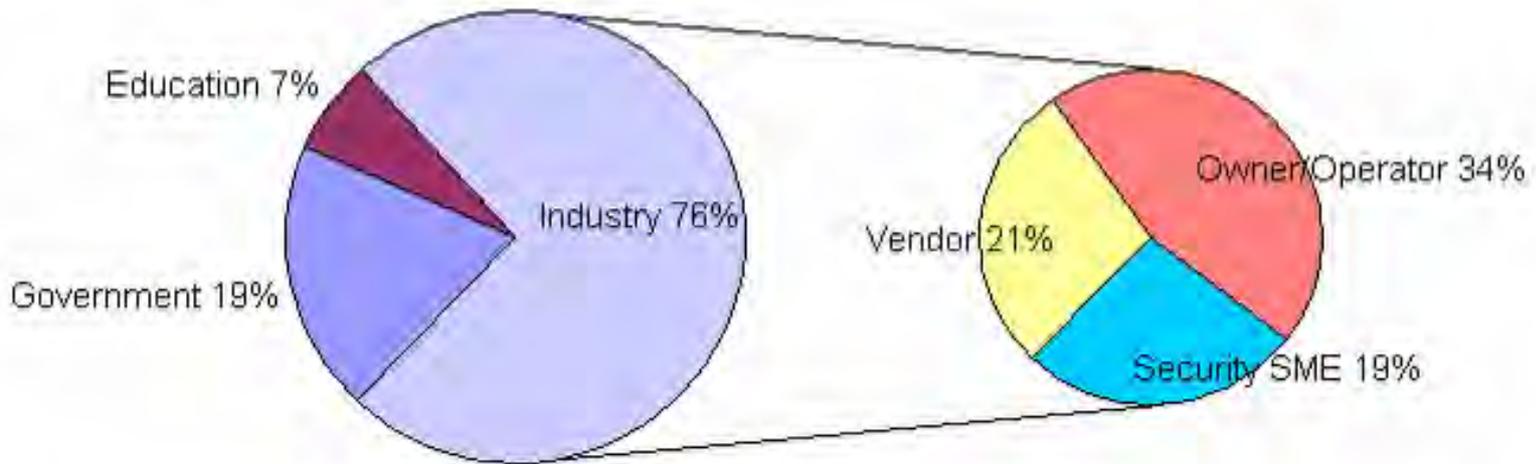
- Peer reviews
- RPOC & Industry reviews
- CSSP Program



Recommended Practice Review Process



72 Industry Reviews

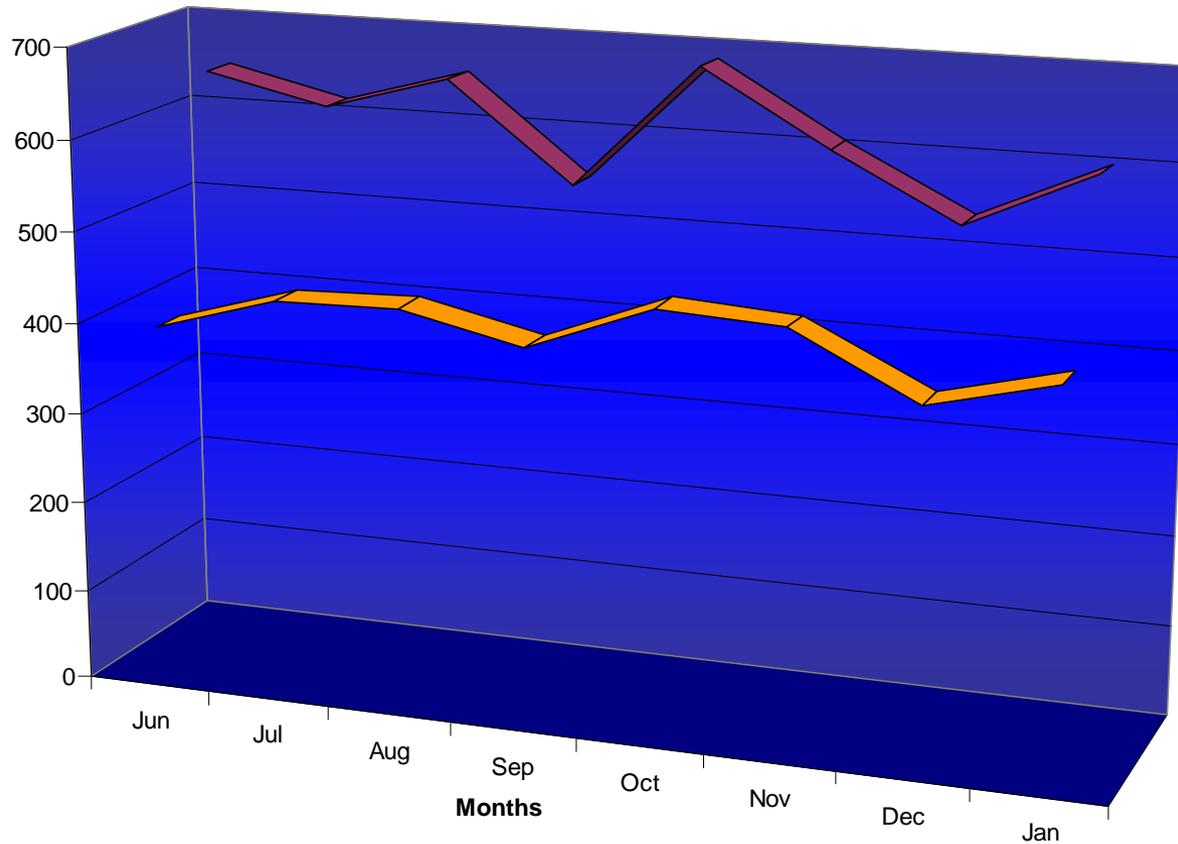


■ Government
 ■ Education
 ■ Industry
 ■ Vendor
 ■ Owner/Operator
 ■ Security SME

Government	Education	Industry	Industry		
			Vendor	Owner/Operators	Security SME
14	5	53	15	24	14

Website Demo

Recommended Practices Website Statistics



	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan
Unique Visitors	392	432	436	407	460	452	384	418
number of visits	647	617	655	550	686	607	538	602

Unique Visitors number of visits

RP Focus Areas for 2007

- ◆ System Administration & Mitigations
 - Wireless for Control Systems (IEEE802.15.4 – Zigbee)
 - ICCP Communications Protocol
- ◆ Configuration Management
 - CM and Security
- ◆ Policies, Plans & Procedures
 - Procedural infrastructure required for CS Security

RP Focus Areas for 2007 (Cont.)

- ◆ Incident Response
 - Response, Investigation and Backup Capabilities
- ◆ Access Control
 - User Management

Are your
Control Systems
Being Targeted?



The United States
Department of Homeland Security
is working to help users and
operators increase the security
of their control systems

Control Systems Security Program

www.us-cert.gov/control_systems



**Homeland
Security**

For additional information on the
Control Systems Security Program

www.us-cert.gov/control_systems

Or email us at cssp@dhs.gov