# Control Systems Security Program (CSSP)

**Rob Hoffman, INL**

**Control Systems Security Program**

**National Cyber Security Division (NCSD)**

Homeland Security

# Briefing Overview

- Control Systems Security Challenges
- Strategic Overview
- Measures for Success
- Summary
- Questions

Homeland Security

# Control Systems Security Challenges

| Security Topic | Information Technology | Control Systems |
|---|---|---|
| Support technology lifetime | 3-5 years | Up to 20 years |
| Application of patches | Regular/ scheduled | Slow (vendor specific) |
| 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 Standards | Established and Mature | Immature and developing |

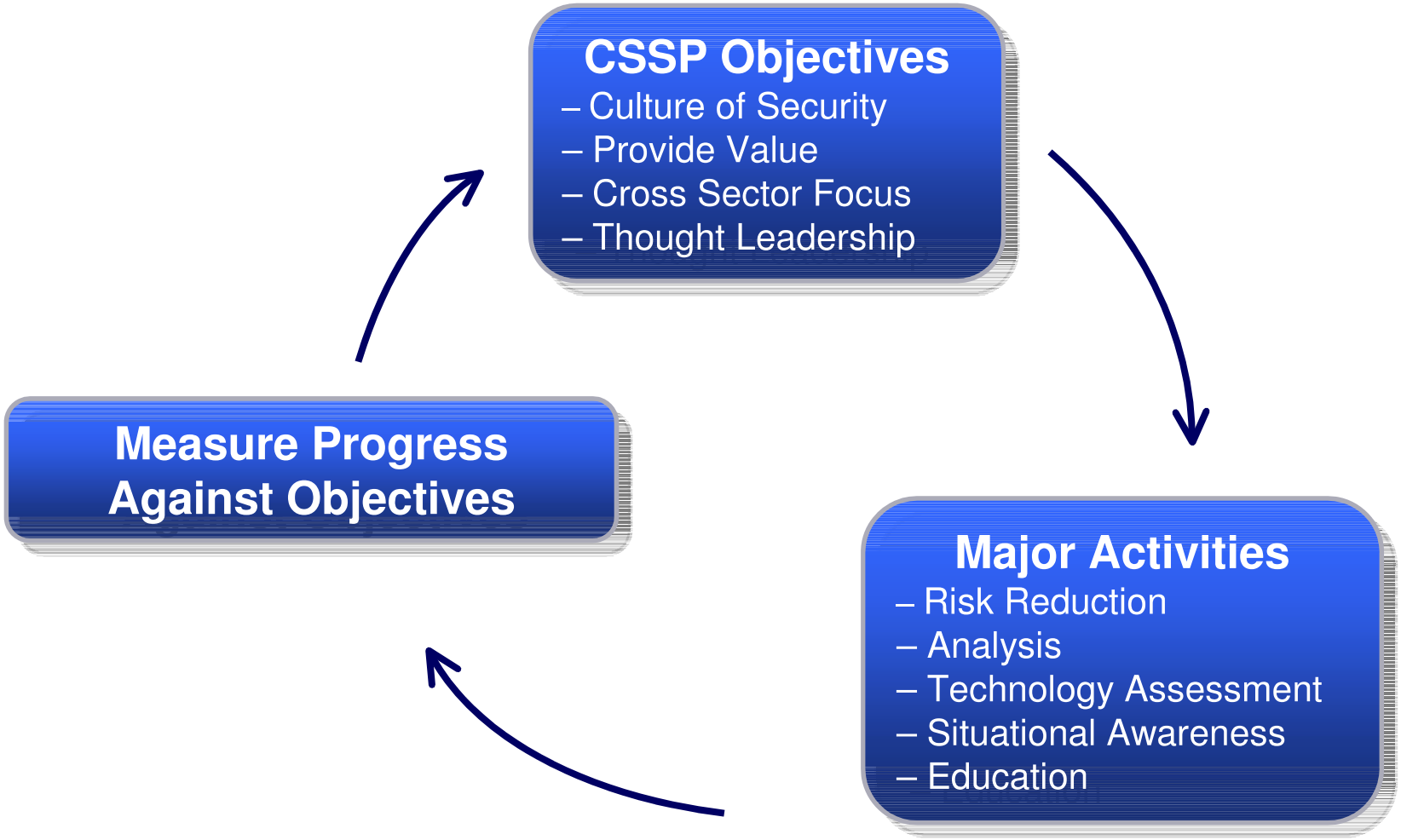
# CSSP Mission and Objectives

**To strengthen the control system security posture by coordinating across government, private sector and international organizations to reduce the risk**

- **Build a culture of reliability, security and resilience**
- **Demonstrate value**
- **Address cross sector security interdependencies**
- **Provide thought leadership**

Homeland Security

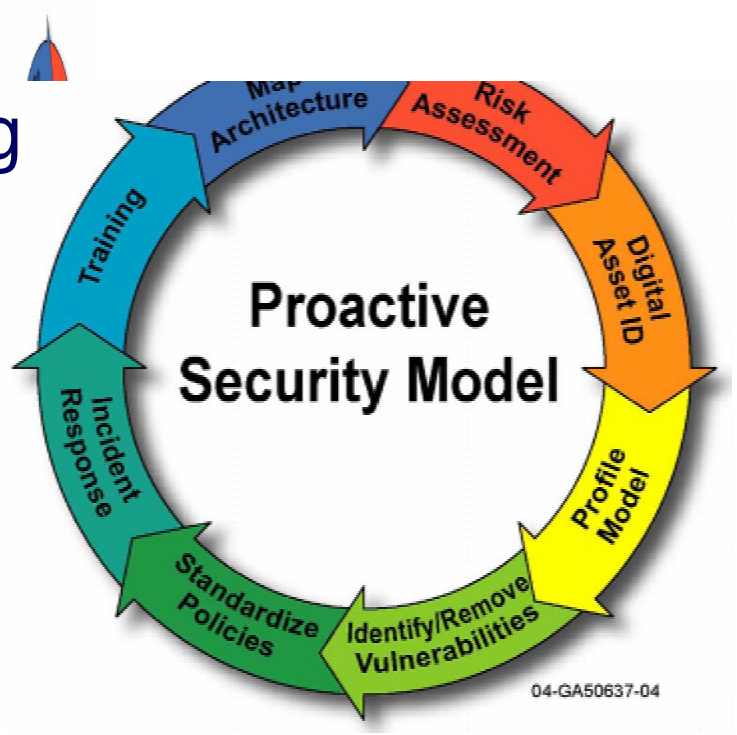
# CSSP Strategic Overview




Homeland Security

# Culture of Reliability, Security and Resilience

- Enhance collaboration
- Improve information sharing
- Develop products that enable asset owners to mitigate consequences is a secure and cost effective manner
- Support operational risk management




Homeland Security

# Risk Reduction Products
## *CSSP Products*

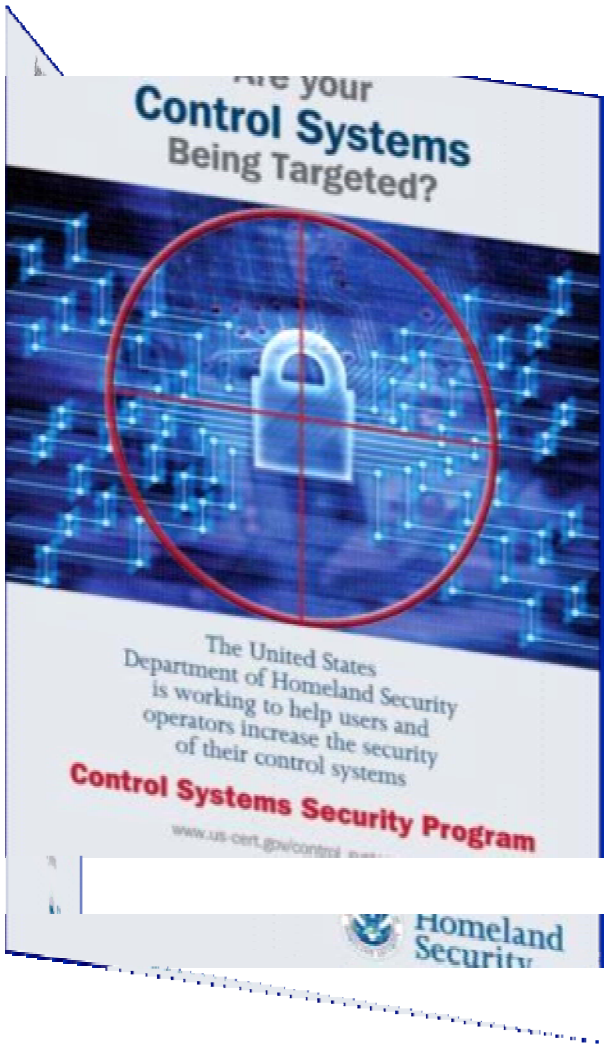
- **Control Systems Cyber Security Self Assessment Tool** (http://www.us-cert.gov/control_systems/pdf/CS2SAT.pdf)
- **Cyber Security Procurement Language for Control Systems**
- **Catalog of Control System Security: Recommendations for Standards Developers** (http://www.us-cert.gov/control_systems)
- **Securing Your SCADA and Industrial Control Systems Pocket Guide** (http://bookstore.gpo.gov)
- **US-CERT control systems related Vulnerability notices** (http://www.us-cert.gov/control_systems/csdocument.html#vuls)
- **Control systems recommended practices** (http://csrp.inl.gov/)
- **Control systems security awareness and mitigation training classes** (http://www.us-cert.gov/control_systems/cstraining.html)

**http://www.US-CERT.gov/control_systems**

Homeland Security

# Outreach & Awareness

- Sponsor Process Control Systems Forum (PCSF) to reach control system stakeholder community
- Enhance security awareness
- Provide training to increase knowledge & skills
- Developing curriculum
- Information sharing




Homeland Security

www.us-cert.gov/control_systems

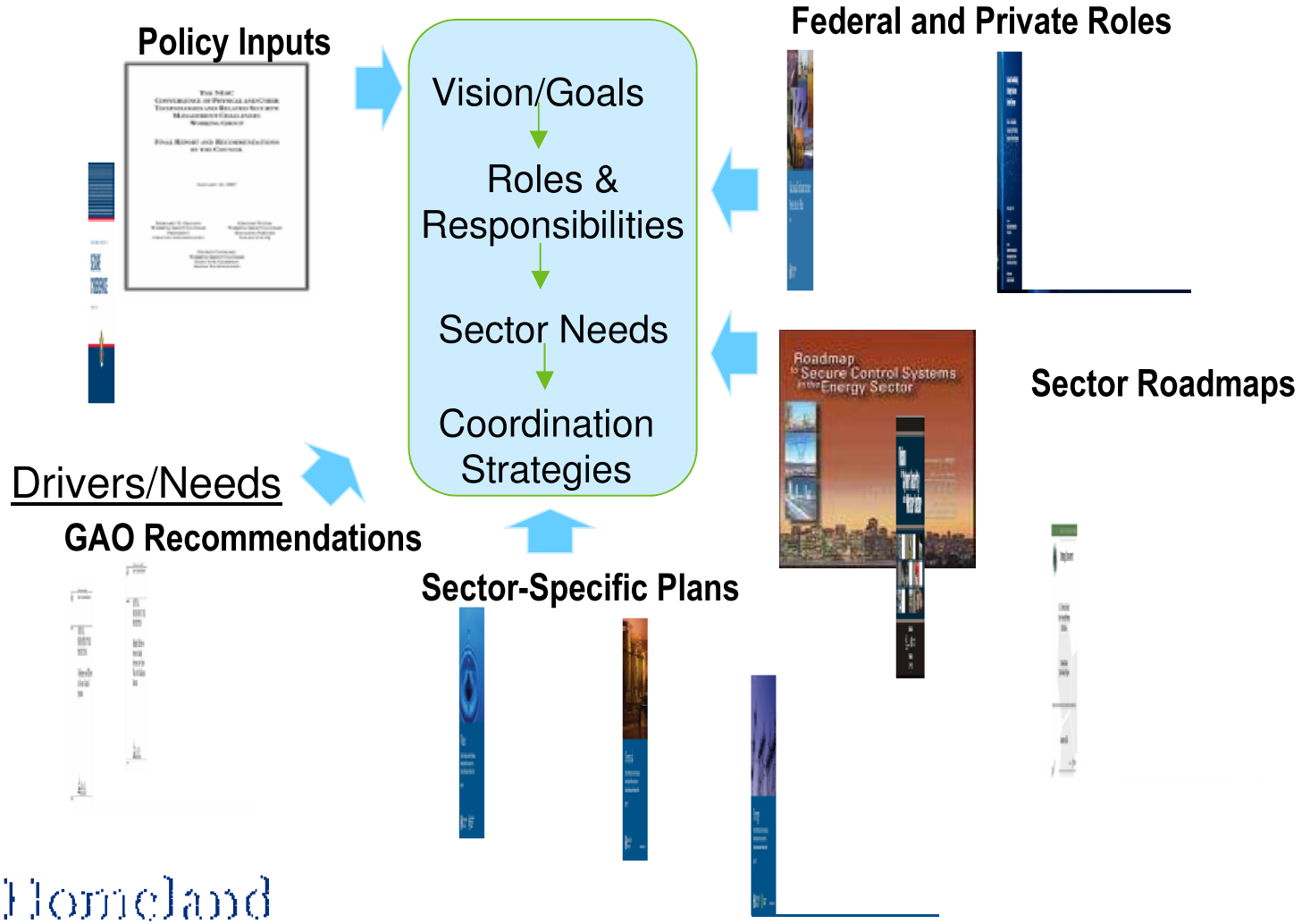
# Briefings & Training
## *Web-Based Courses*

- Cyber Security for Control Systems Engineers & Operators
- OPSEC for Control Systems


Homeland Security

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

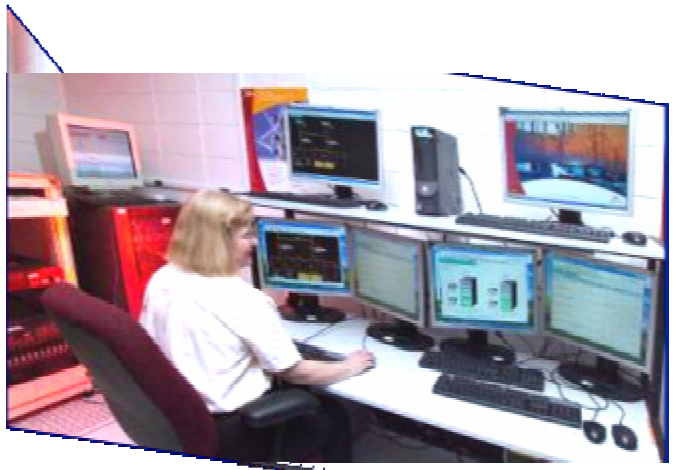
# Enhance Coordination:
## *Public Private Coordination Strategy*

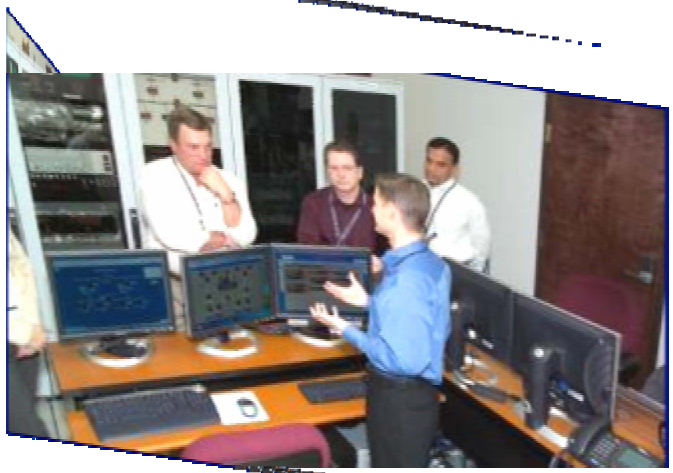



Homeland Security

# Technology Assessments
## *Vendor Assessment Objectives*

- Control Systems Vendor Partnership
- Utilizing expertise at Control Systems Security Center (CSSC)
- Benefits:
  - Identify specific cyber security vulnerabilities
  - Mitigate vulnerability in partnership with vendors
  - Deliver cyber security solutions to end users through patches and products





Homeland Security

# Vulnerability Analysis
## *Information Sharing*

- Control System Vulnerability reports may be submitted via US-CERT Web Site and entered into National Vulnerability Database (NVD)
- CSSP Web site 'Vulnerability Notes'
  - 14 vulnerability Notes published between May 2006 – February 2008
  - Vulnerabilities patched by vendors
  - CSSC analysis shared across all sectors through products and trainings
- PCII is an information-protection tool that facilitates private sector information sharing with the government

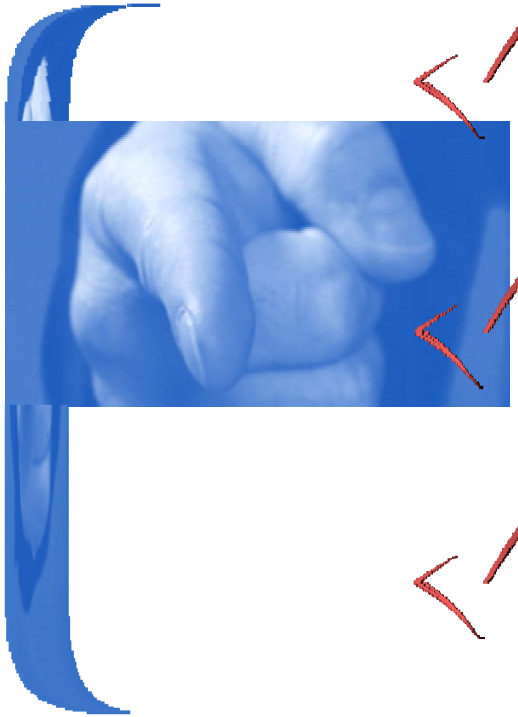
Homeland Security

# Situational Awareness

- ***Report Incident & Vulnerabilies*** to the US-CERT at (www.us-cert.gov/control_systems)
- ***Information Provided*** through bulletins and white papers
- ***Vulnerability Reports*** provided to control systems stakeholders through a secure website
- ***Conduct technical analysis*** of malware's affects on control systems

Homeland Security

# Scenario Development
## *Advance Vulnerability Discovery*



*Identifying cyber attacks capable of achieving physical damage*

*Combining cyber vulnerabilities with specific tactics, techniques & procedures to achieve maximum consequence*

*Requires industry experience to identify control system risks*

Homeland Security

# Measure Progress

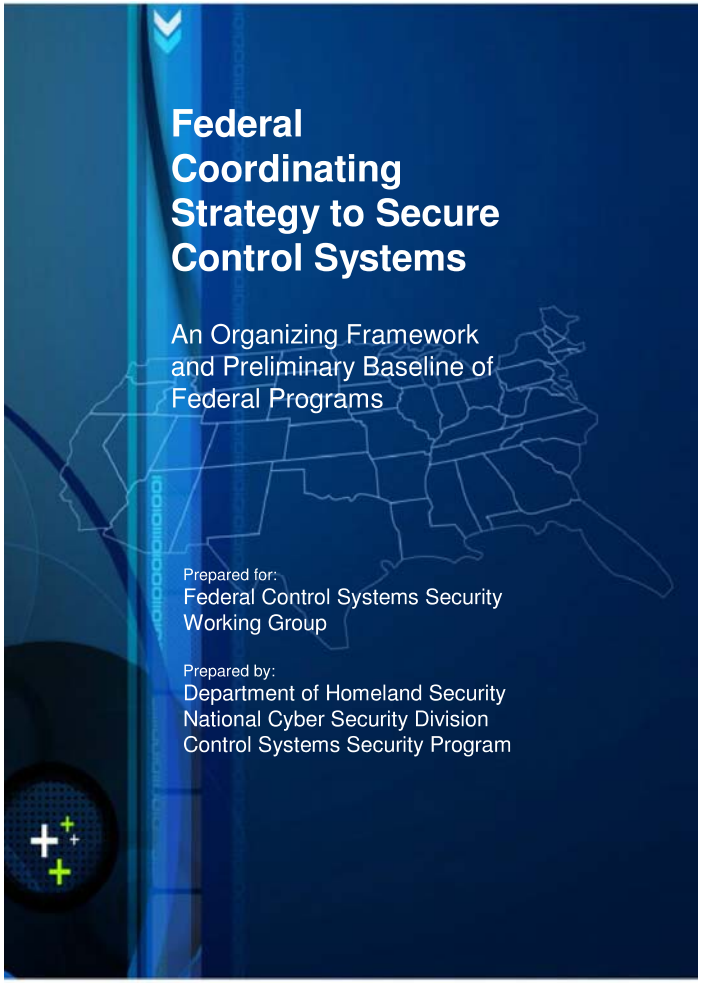
## *Examples of Control System Security Metrics*

| Security Ideal | Metric |
|---|---|
| 1. Security Group (SG) knows current system perfectly | Rogue change days |
| | Component test count |
| 2. Attack Group (AG) knows nothing about the system | Minimum password strength |
| 3. System is inaccessible to AGs | Reachability count |
| 4. The system has no vulnerabilities | Vulnerability exposure |
| 5. The system can't be damaged | Worst case loss |
| 6. SG detects any compromise instantly | Detection mechanism count |
| 7. SG can restore system integrity instantly | Restoration time |

Homeland Security

# Develop Partnerships – Government
## *Federal Control Systems Security Working Group*

- Coordinate efforts to improve control systems security
- Identify and leveraging activities
- Support a federal strategy for control systems security




Homeland Security

# Develop Partnerships – Industry

## *Control System Cyber Security Vendor's Forum*

# Develop Partnerships – Public
## *Process Control Systems Forum (PCSF)*

- ***Mission: To accelerate the design, development, & deployment of more secure control & legacy systems***
  - Participants include national & international stakeholders from government, academia, industry users, owner/operators, systems integrators, & the vendor community
  - For more information: www.pcsforum.org

PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

Homeland Security

# Develop Partnerships – Academia
## *Curriculum Development*

- Critical Infrastructure & Control System Security Curriculum
  - Masters level course on policy & management
  - To be released – Soon!

***Developing:***

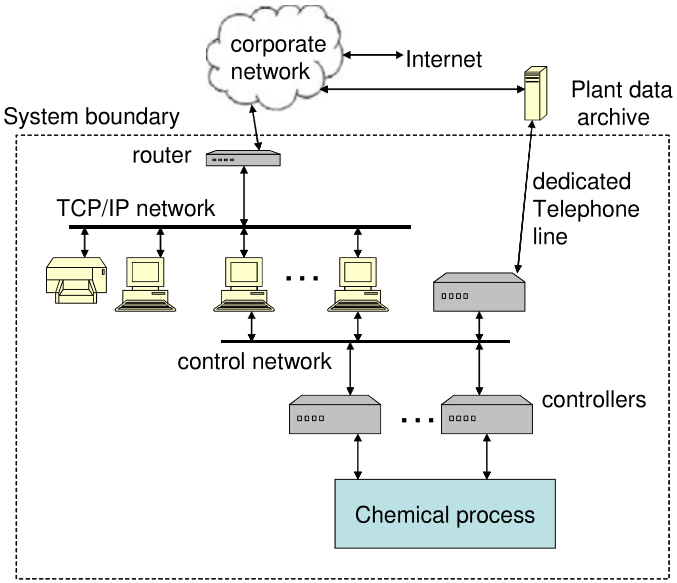
- Technical course on control system security

Homeland Security

# Measures of Success

***Metrics are Being Gathered & Identified to Qualify Programmatic Success***

- Program metrics
  - Measuring impact
- Control system security metrics
  - Aid assessment of control-system security exposure
- Sector metrics
  - Sector level risk measurement




Homeland Security

# Summary

- Products that provide Value
- Control Systems security awareness
- Increase stakeholder knowledge & skills
- Build culture of awareness

- Coordinate efforts
- Develop partnership relationships with stakeholders
- Access and inform Academia
- Leverage activities

- Provide awareness and solutions
- US-CERT Control Systems SMEs
- Vulnerability analysis
- Leadership

Homeland Security

# Cyber Security is a Shared Responsibility

- Report cyber incidents & 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 or email: CSSP@dhs.gov

- Contact information:
  - National Cyber Security Division
  - Seán P. McGurk, Director – Control Systems Security Program
  - Sean.McGurk@dhs.gov

Homeland Security

Homeland Security

# Backup Slides

# Demonstrate Value

- Capture Stakeholder Metrics
  - Products that are:
    - Measurable
    - Sustainable and
    - Scaleable to the CIKR
- Support collaboration and information sharing (national and international)


Homeland Security

# Cross Sector Security Interdependencies

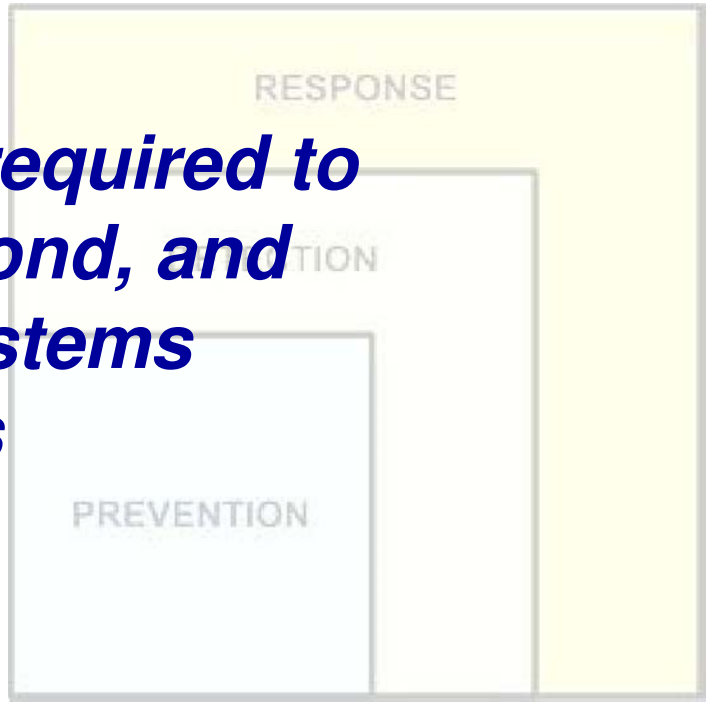
- Control systems security is not sector specific
- Connectivity crosses geographic boundaries
- Sectors are not operationally isolated


Homeland Security

# Provide Thought Leadership

- Establish control systems security principles
- Analyze the impact of technology
- Understand operational trends that affect control systems

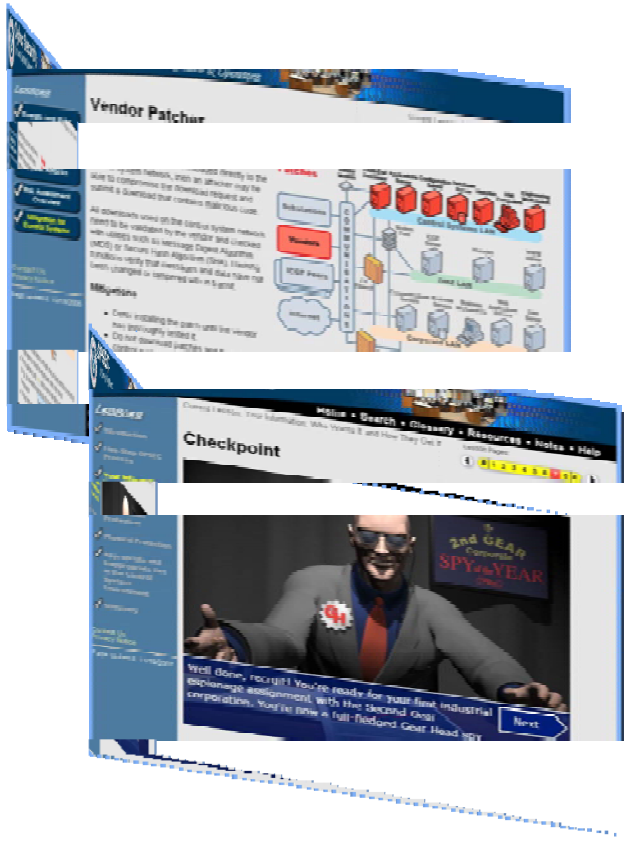
***Security principles are required to predict, prevent, respond, and mitigate control systems vulnerabilities***




Homeland Security

# Briefings & Training

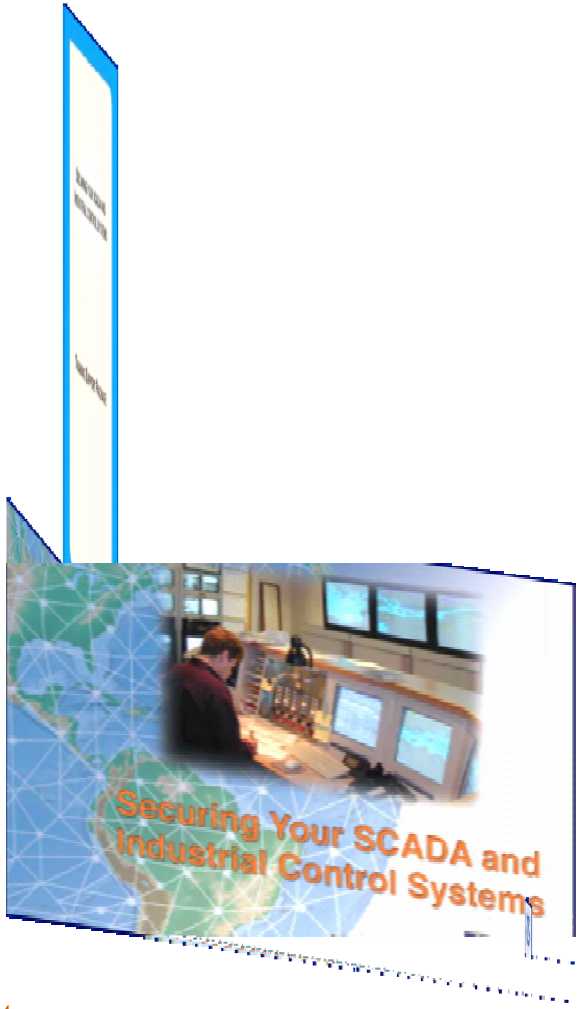
- Web Based Training
  - Cyber Security for Control Systems Engineers & Operators
  - OPSEC for Control Systems
- Instructor Led Courses
  - Cyber Security Who Needs It?
  - Control Systems Security for Managers
  - Solutions for Process Control Security
  - Introduction to Control Systems Security
    For the IT Professional
  - Intermediate Control Systems Security
  - Cyber Security Advanced Training and Workshop




Homeland Security

# Briefings & Training
## *Control Systems Security Pocket Guide*

- Securing your SCADA & Industrial Control Systems Pocket Guide - Joint DHS & TSWG recommended practices guide
- Covers administrative controls, architecture design & security technology
- Training Support Package Available

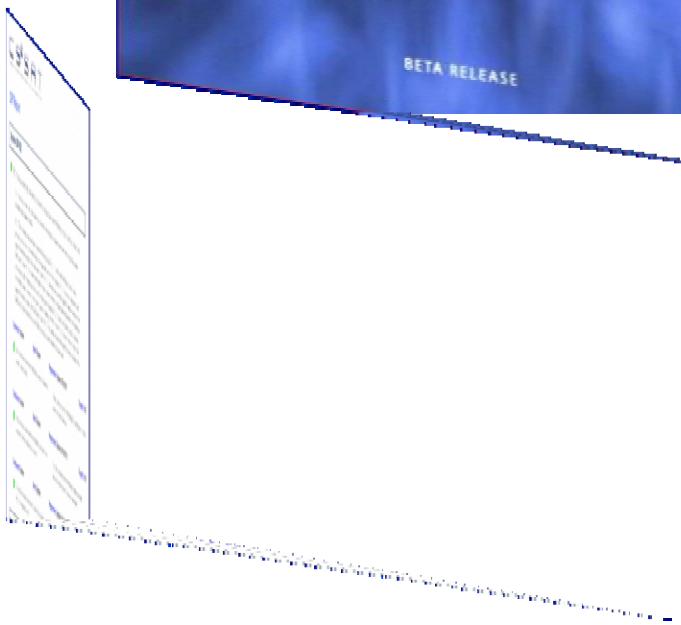



Homeland Security

http://bookstore.gpo.gov

# Risk Reduction Products
## *Self-Assessment 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)
- Availability:
  - To industry through licensed distributors (fee based)
  - To federal government through DHS (free)

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

Homeland Security

# Risk Reduction Products

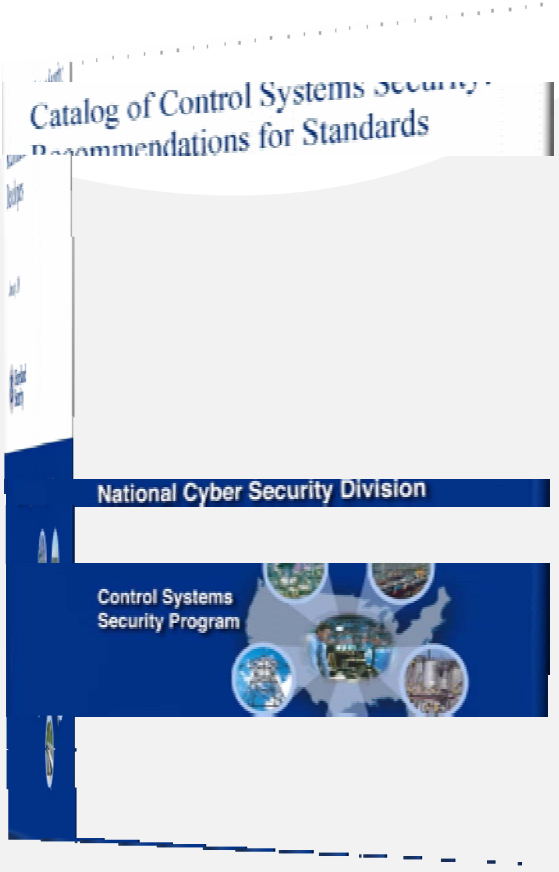
## *Catalog of Control Systems Security: Recommendations for Standards Developers*

### Supporting Standards Development

Provide guidance for cyber security requirements specific to control systems

Enable a common security language across all industry sectors (harmonization of standards)

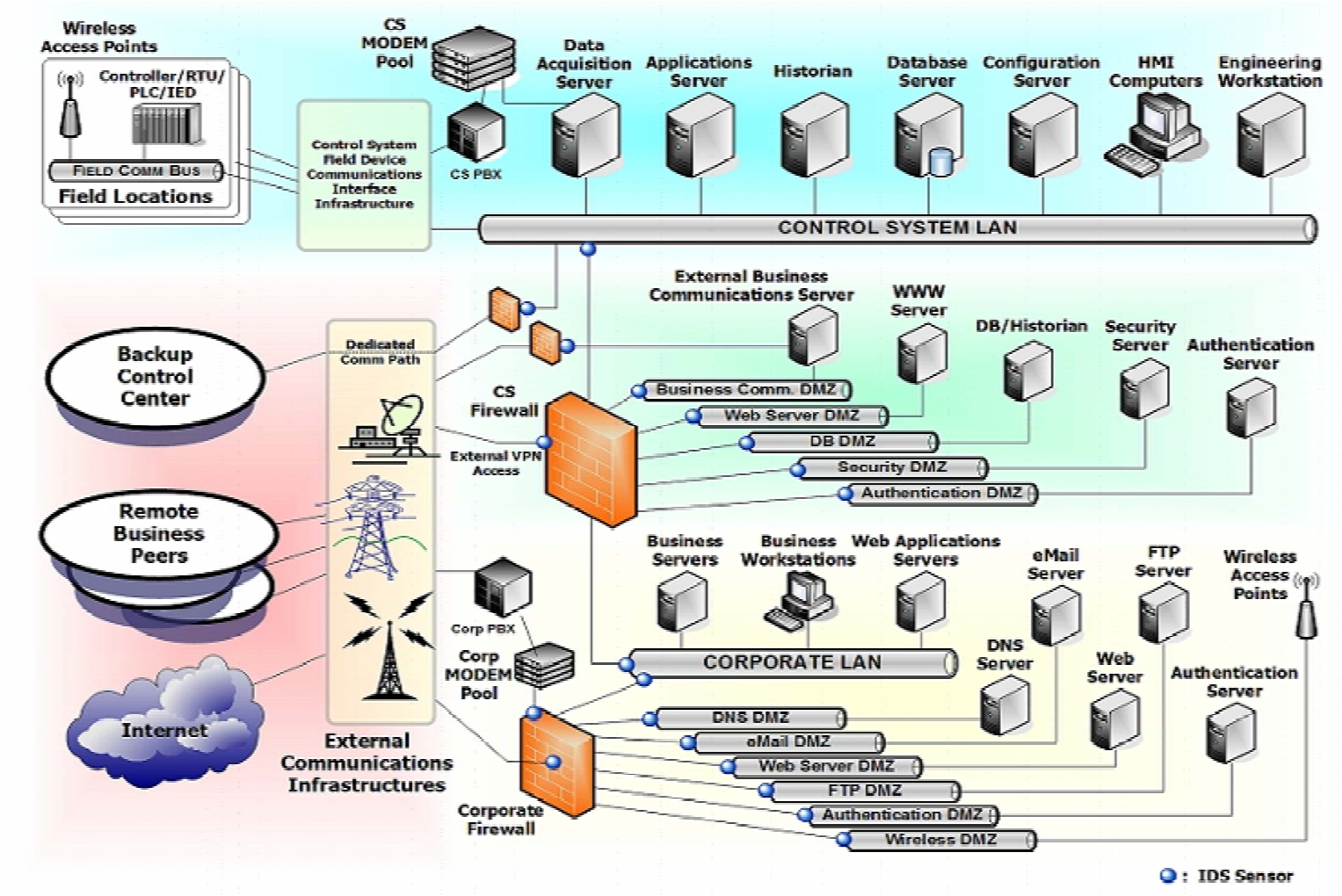
Support standards bodies and industry associations to implement sound security practices in current standards




Homeland Security

# Risk Reduction Products

## *Recommended Practices – e.g. Reference Architecture*




Homeland Security

# Incident Analysis & Response

- **Support to US-CERT:**
  - Maintain situational awareness
  - Provide expertise during control system incidents
  - Support mitigation recommendations for vulnerabilities and during incidents

Homeland Security

# Scenario Development

## *An Example -*


Homeland Security

# Develop Partnerships – Academia

## *Institute for Information Infrastructure Protection*

Leveraging knowledge & technologies developed under the I3P for control systems. For more information: www.thei3p.org

- Survivability & Recovery of Process Control Systems:
- Reduce the opportunity for an attack to be mounted against critical components
- Increase the likelihood of detection in case of attack
- Ensure that operators can rapidly recover

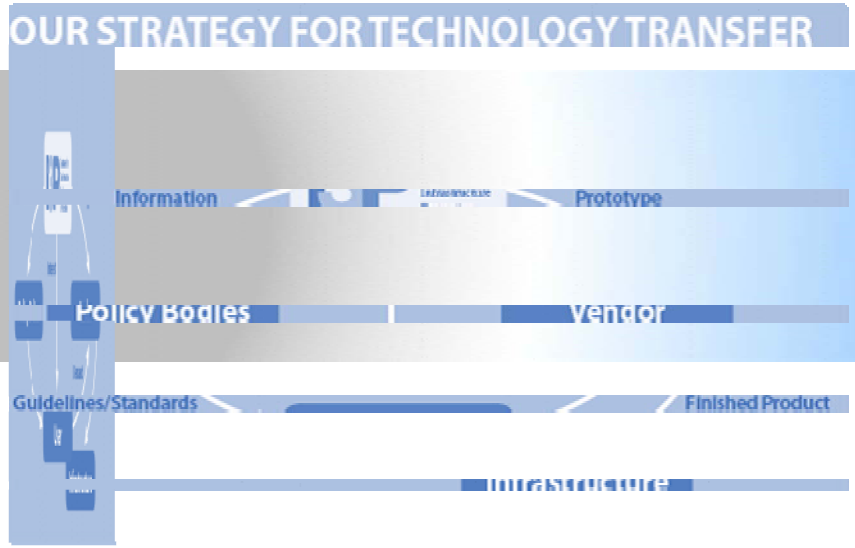
Homeland Security

# Develop Partnerships – Academia

## *Institute for Information Infrastructure Protection*

- Tools for Operators & Vendors:
  - RiskMAP - Tool to build a business case for security investment
  - DEADBOLT - Source code checking tool
  - SHARP - Security-Hardened Attack Resistant Platform
  - SecSS – Situational awareness tool for MODBUS networks
  - APT – Access policy tool for enforcing firewall policies

***Our Strategy for Technology Transfer***




Homeland Security