

Control Systems Security Program Industry Interest Group PCSF – June 7, 2006 La Jolla, CA

Jeff Hahn, Idaho National Laboratory

Control Systems Security Program

National Cyber Security Division



**Homeland
Security**

Agenda

- 1:00 Welcome – introductions
- 1:10 Purpose of IIG
- 1:15 CSSP Overview
- 1:25 Developing Awareness Products
- 2:00 Increasing Stakeholder Awareness
- 2:20 Training and Education
- 2:40 Working with Industry & Government
- 3:00 End – THANKS!



Purpose of Industry Interest Group

- Enable the DHS Control Systems Security Program to be grounded with industry.
 - Program direction
 - Tools
 - Products
 - Outreach & Awareness



Primary CSSP Objective

Reduce risk of cyber attacks to control systems within critical infrastructure by coordinating government and industry efforts to identify and mitigate cyber vulnerabilities



Homeland
Security

Overview

Primary Objective

Reduce Risk of Cyber Attacks to Control Systems

Program Goals

**Enhance
Incident Response
Capabilities**

**Assess
Vulnerabilities
& Risks**

**Enhance
Industry
Practices**

**Enhance
Security
Awareness**

**Recommend
R&D Needs**

Integrated Tasks

Reduction in Cyber Related Risk



**Homeland
Security**

Assess Vulnerabilities & Risk

Unacceptable Risk



Vulnerability Assessments
Vendors & Owner Operators

Risk Analysis to Optimize Security for Least Cost

Reduce Risk

Acceptable Risk



US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Incident Response
Control Systems Section

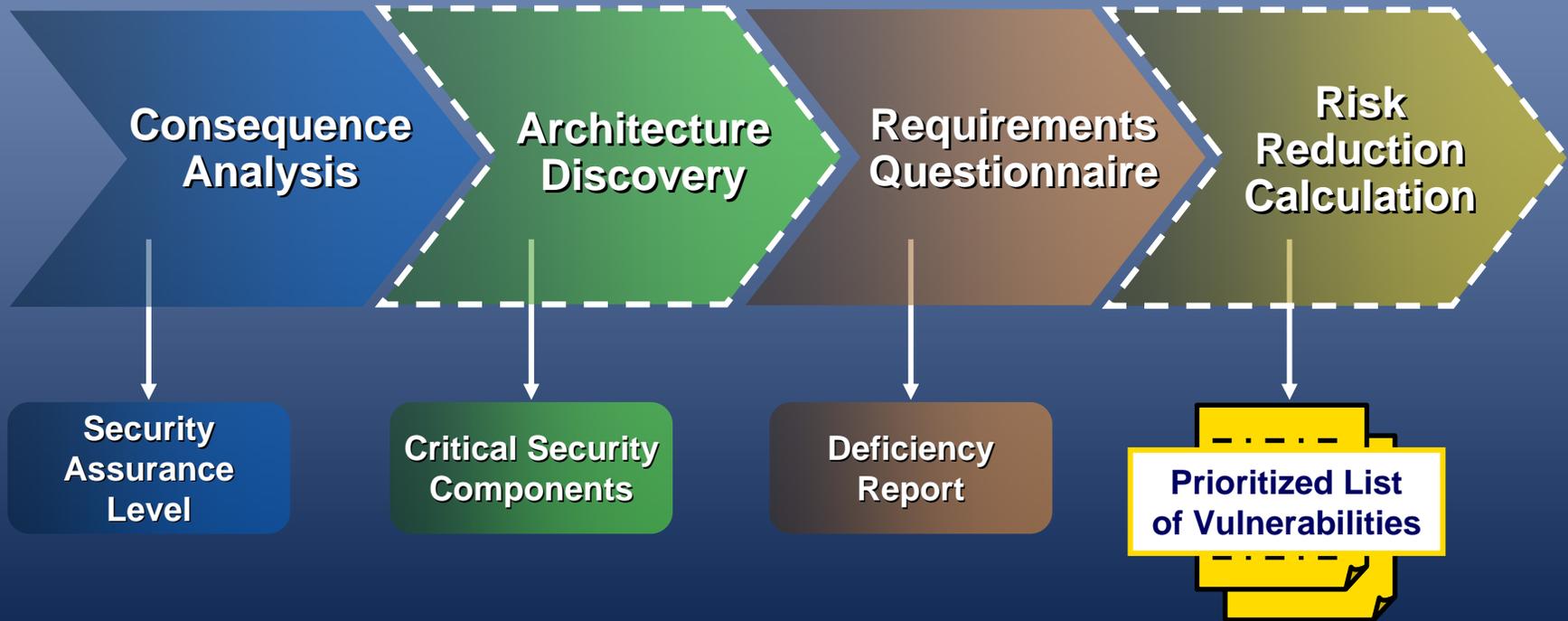


Homeland Security

Enhance Industry Practices

Four Independent Elements

--- = In Development



Recommended Practice Committee

- Committee was organized on March 1, 2006
- Members:
 - Dale Peterson, Digital Bond (Chair)
 - Keith Stouffer, NIST
 - Brian Singer, ISA
 - Jeff Dagle, PNNL
 - Eric Byres, Wurldtech Analytics Inc.
 - Michael Assante, INL
 - Julio Rodriguez, INL/NCSD



Digital Bond

A Network Security Practice



Homeland
Security

Recommended Practice Goals:

- Secured Architecture for Control Systems
- Central Location for all recommended Practices
- Monthly releases of recommended Practices
- All practices vetted with Industry – SME's



Activities To-Date:

- Glossary/Index of practices developed
- Committee will review and identify practices to link to the Recommended Practices website
- Four practices currently under development:
 - Implementation of Security Systems Architecture-Defense in Depth Strategies
 - OPSEC for Control Systems
 - Building a Security Culture
 - Wireless for Control Systems
- Website development

Enhance Security Awareness

- **Develop Awareness Products**
- Increase Stakeholder Awareness
- Training and Education
- Work with Industry & Government

www.us-cert.gov/control_systems



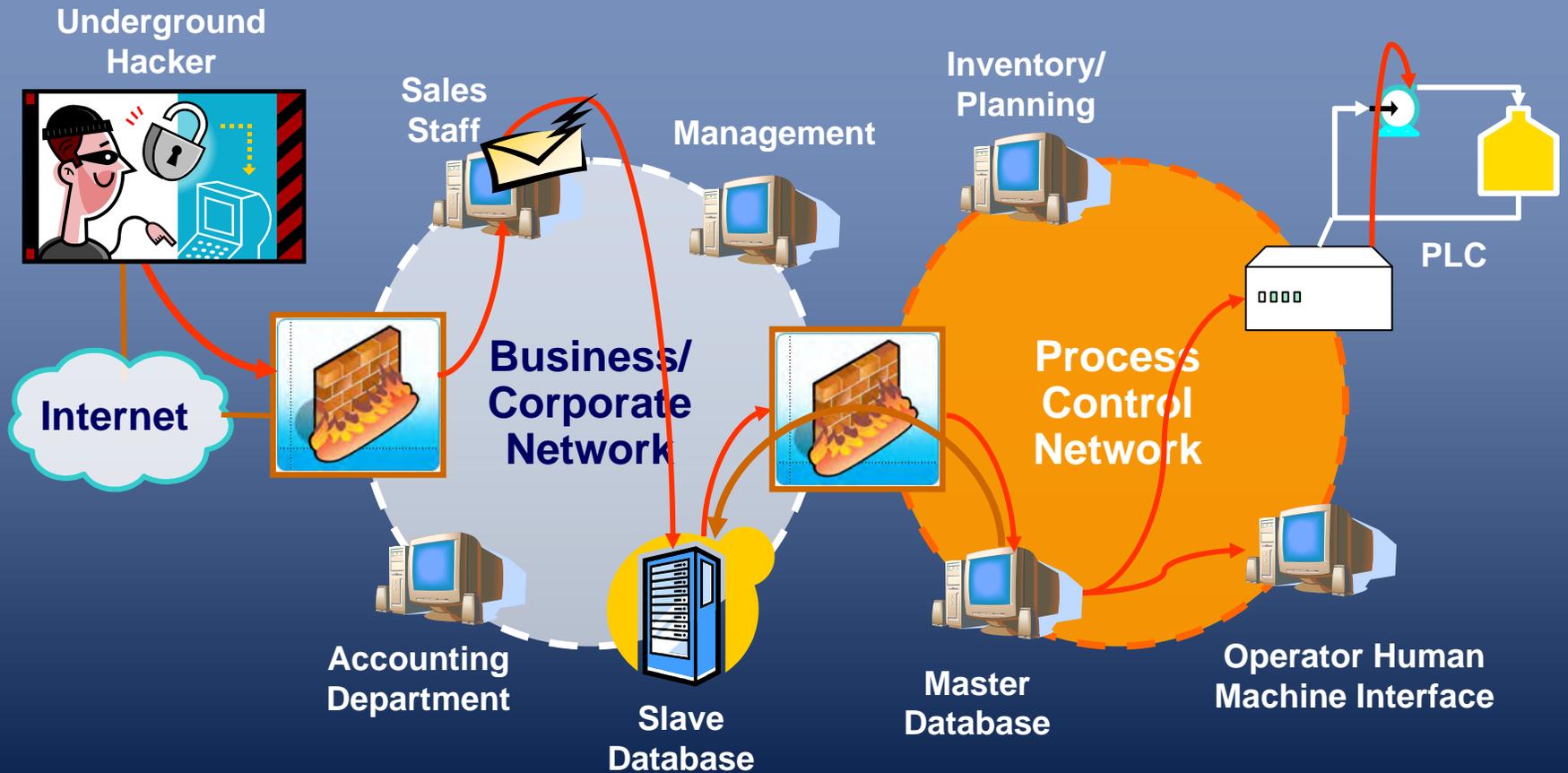
Homeland
Security

Develop Awareness Products

- Chemical Sector Awareness and Demonstration Video
 - Using during CSSP presentations and training
 - Available to members of ACC
- Electrical Utility Awareness and Demonstration Video
 - Developed and being considered for approval by DHS.
- Other Sector Specific Videos
 - Showing Cyber Attack Scenario
 - Providing ideas for mitigations
 - Increasing awareness
- Recommendations?



Attack Process Demonstration





Homeland
Security

Video Demo



Homeland
Security

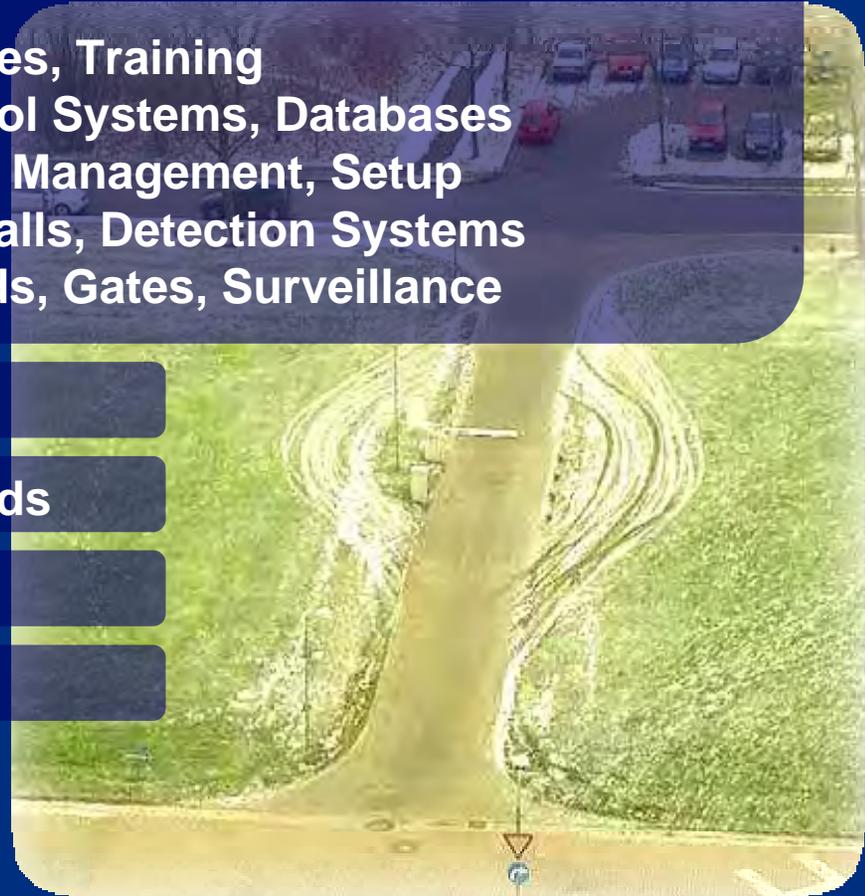
Recommendations

Layers of Defense

- Human:
- Applications:
- Operating Systems:
- Networks:
- Physical:

Policies, Training
Control Systems, Databases
Patch Management, Setup
Firewalls, Detection Systems
Guards, Gates, Surveillance

- Identify Security Requirements
- Map Requirements to Security Standards
- Applying Appropriate Solutions
- Work with US CERT



Enhance Security Awareness

- Develop Awareness Products
- **Increase Stakeholder Awareness**
- Training and Education
- Work with Industry & Government

www.us-cert.gov/control_systems



Homeland
Security

Increase Stakeholder Awareness

- Industry Association Conferences
 - Participating in conference expo's
 - Providing training (1 hr, 4 hr and 8 hr) during conference sessions and as pre-conference tutorials.
- Working with industry
 - Standards organizations
 - Special efforts (e.g., Recommended Practices, Procurement Guide)
- Web Site
 - www.us-cert.gov/control_systems
 - Updated and improved frequently
- Recommendations?



Enhance Security Awareness

- Develop Awareness Products
- Increase Stakeholder Awareness
- **Training and Education**
- Work with Industry & Government

www.us-cert.gov/control_systems



Homeland
Security

Training & Education

- Training Courses available
 - Cyber Security, Who Needs It? (1 hr)
 - Control Systems Security for Managers (1 hr)
 - Solutions for Process Control Security (4 hrs)
 - Process Control Security for IT (4 hrs)
 - Introductory SCADA Security (4 hrs)
 - Intermediate Control Systems Security (8 hrs)
 - Intermediate SCADA Security (8 hrs)
- Education
 - Curriculum Development - Brian Lopez, LLNL
- Recommendations?



Control Systems Security Program Industry Interest Group PCSF – June 7, 2006 La Jolla, CA

Brian Lopez (blopez@llnl.gov, 925 422 5839)

Lawrence Livermore National Laboratory (LLNL)

Control Systems Security Program (CSSP)

National Cyber Security Division (NCSD)



**Homeland
Security**

CSSP Education & Training Strategy

- Three Thrust Areas
 - Academic
 - Students & Professors engaged with CIP issues and careers
 - Across all relevant disciplines (engineering, computer science, public policy, management, etc)
 - Awareness
 - Industry Leaders, Managers, System Designers
 - Government Officials and Agencies
 - General Public
 - Operational
 - System Operators



CSSP Education & Training Strategy

Three Goals

1. Encourage and enhance teaching of control system security at the college and university level (inherently multi-disciplinary).
2. Promote general awareness, interest, and knowledge of the need for and means to achieve security in the control systems.
3. Enhance the availability and quality of operational control system security training.



**Homeland
Security**

Targeted Outcomes

- Increased number of professionals engaged in cyber security of control systems within the critical infrastructure community.
- Increased awareness of control system security issues and solutions.
- Increased skills and skill development programs for operators of critical infrastructure control systems.
- Increased private sector partnerships.
- Develop the demand within the private sector for professionals with academic degrees and credentials in control system cyber security.
- Other ideas?



Example: Curriculum Development

- Target: Decision-makers Across Disciplines
- Expected Outcomes:
 - Understand basic concepts underlying the technical functions, vulnerabilities, and means of protection of control systems
 - Understand the drivers that lead to new and increasing levels of vulnerability
 - Be equipped to intelligently address policy development and decision making:
 - Industry: Advise leaders on relevant CIP issues, the value of control systems security, and practical strategies for doing so.
 - Government: Advise leaders on the relevant CIP issues and appropriate policies and programs to mitigate those issues.



Example Course Topics

- Critical infrastructures – What are they? Why critical?
 - Infrastructure facilities and services
 - Private vs public ownership
 - Criticality of services in times of disaster
 - Technical vulnerability examples (control system case studies)
 - Use of critical infrastructure as a weapon by terrorists
 - Interdependence (including shared control system vulnerabilities between sectors)
- Policy context:
 - Laws, Commissions, PDDs, role of DHS and other agencies
 - Role and structure of government (federal, state, city) in critical infrastructure security
 - Role of technical community – vendors, universities, national laboratories
 - Critical infrastructure as part of “all hazards” approach



Example Course Topics (cont.)

Technical problems and solutions

- Science and technology applied to reducing vulnerabilities
- Case studies
 - SCADA systems used in electric power industry
 - SCADA systems in chemical plants
 - Cyber threats and vulnerabilities; cyber attack as force multiplier
- Systems thinking and systems problems; testing and red-teaming

Managing high reliability organizations

- Experience from existing organizations
- Principals of management when facing terrorism, other disasters
- Business cases for investment in robustness and resilience

Creating a market for disaster preparedness investments

- Private risk management for terrorist attacks
- Role of insurance and re-insurance industries

Creating trust: information sharing, public-private partnerships

- Institutional proposals and solutions
- International issues
- Public-private collaboration – beyond regulation and subsidies



Very Interdisciplinary Team

- Engineering, Computer Science and Systems Analysis Departments
 - Control Systems critical to infrastructures
 - Underlying IT systems critical to all infrastructures
 - Systems Analysis Tools and Techniques
- Risk Management
 - Tools for vulnerability assessment and risk management
- Economics
 - Networked industries
 - Security externalities
- Business Analysis
 - Business Case Development
 - Insurance, reinsurance, and other options
- Management theory
 - Collaborative (public-private) governance
 - Managing robust and resilient industries



Project Leadership

Lewis Branscomb

- Harvard JFK School / University of California San Diego
- NSF, NIST, NAS, etc
- Author: *Making Our Nation Safer: the Role of Science and Technology in Countering Terrorism*

Philip Auerswald

- George Mason University
- Director, Center for Science & Technology Policy
- Editor: Book forthcoming this summer from Cambridge University Press focused on Critical Infrastructure Protection from multiple disciplines

Brian Lopez

- Lawrence Livermore National Laboratory
- Leader, Vulnerability & Risk Assessment Program (VRAP)
- Decade of experience leading vulnerability assessments against critical infrastructure, book forthcoming, lectured on vulnerability assessment and critical infrastructure issues at UC-Berkeley, Univ. of Washington, Microsoft.



Schedule - Distribution - Contact

Schedule

- Draft of the Curriculum: End of Summer
- Final Version: Christmas

Distribution

- Entire curriculum including reading lists and all supporting materials will be freely available and distributed via web site.

Contact

- Brian Lopez
 - Email: blopez@lhn.gov
 - Phone: 925 422 5839



Enhance Security Awareness

- Develop Awareness Products
- Increase Stakeholder Awareness
- Training and Education
- Work with Industry & Government

www.us-cert.gov/control_systems



Work with Industry and Government

- Industry
 - PCSF Industry Interest Group
 - Procurement Guide
 - Recommended Practices
 - Vendor Assessments
 - Validating Self-Assessment Tool
- Government
 - Holding government agency coordination meetings (2 this year – so far)
 - Sharing information forum.
- Recommendations?



For additional Information

Jeffrey.Hahn@inl.gov

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

Control System Security Program

Thank You



Homeland
Security



Homeland
Security