SANS SCADA Summit

Cheri McGuire, Acting Director

National Cyber Security Division

U.S. Department of Homeland Security

Homeland Security

National Cyber Security Division Control Systems Efforts

Goal

Reduce Cyber Risk to Critical Infrastructure Control Systems

Key Objectives

Provide Guidance

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

Foster Partnerships

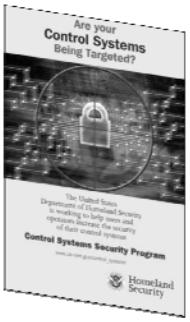
- *Government*
- *Industry*
- *Academia*
- *International*

Prepare & Respond

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

Homeland Security

Provide Guidance



Risk Reduction Products

- Self-assessment tool (CS2SAT)
- Recommended practices
- Cyber Security Procurement Language for Control Systems
- Catalog of Control System Security: Recommendations for Standards Developers

Technology Assessments

- Provide vendors and asset owners with recommendations on how to better secure their products and/or sites

Outreach & Awareness

- Training Courses
- International collaboration and information sharing
- Website (www.us-cert.gov/control_systems)

Homeland Security

3

Foster Partnerships

Industry

- Process Control System Forum (PCSF) (www.pcsforum.org)
- Control Systems Cyber Security Vendors Forum
- Sector Coordinating Councils
- Industry associations
- SANS

Government

- Federal, state (MS-ISAC), local, and international

Academia

- Curriculum for university courses
- I3P projects

International

- International standards support
- Coordinating efforts with allies (e.g., Australia, Canada, UK, New Zealand)

Homeland Security

4

Prepare & Respond

Situational Awareness

- Weekly and quarterly analysis of Common Vulnerabilities & Exposures, requests for information, special topical reports for US-CERT

Incident Analysis & Response

- Website (www.us-cert.gov/control_systems) for incident, vulnerability, and threat reporting, as well as informational sharing
- Operational response analysts integrated with the US-CERT Security Operations Center
- Engagement in national exercises, including Cyber Storm II

Scenario Development

- Postulate cyber attacks on control systems

Vulnerability Analysis

- Assess malware and vulnerabilities for potential impacts on critical infrastructure control systems

5

DHS Control Systems Security Products & Training

- Control Systems Cyber Security Self Assessment Tool (CS2SAT) (http://www.us-cert.gov/control_systems/pdf/CS2SAT.pdf)
- Control Systems Recommended Security Practices (http://csrp.inl.gov/)
- Catalog of Control Systems Security: Recommendations for Standards Developers (http://www.us-cert.gov/control_systems)
- Cyber Security Procurement Language for Control Systems (http://www.msisac.org/scada)
- Securing your SCADA and Industrial Control Systems Pocket Guide - Joint DHS & TSWG recommended practices guide covers administrative controls, architecture design and security technology (http://bookstore.gpo.gov)
- Web-based training: “Cyber Security for Control Systems Engineers & Operators" and “OPSEC for Control Systems” (http://www.us-cert.gov/control_systems/cstraining.html)

6


Homeland
Security
Homeland
Security