US Standards Strategy

2006 International Control Systems Security and Standards Coordination Workshop

August 10, 2006

Portland OR

Keith Stouffer
National Institute of Standards and Technology

Standards Strategy

- Federal strategy
- Private sector strategy

Federal Strategy

- Coordination and collaboration between federal stakeholders
  - Federal agencies that own/operate control systems
  - DHS NCSD and S&T
  - FERC
  - DOE
  - NIST

Federal Strategy Challenges

- Federal agencies required to apply NIST SP 800-53 (general IT security requirements) to their control systems
- Federal agencies that own/operates control systems could potentially have to meet 2 standards (NIST SP800-53 and NERC CIP standards)

Federal Strategy

- Hold workshop to discuss the development of security requirements and baseline security controls for federally owned/operated industrial/process control systems (ICS) based on NIST SP800-53
- Develop a guidance document (NIST SP800-82) on how to secure control systems
- Develop bi-directional mapping and gap analysis between NIST SP800-53 and the NERC CIP standard to discover and propose modifications to remove any conflicts

Federal ICS Workshop

- Workshop 4/19-20, 2006 at NIST to discuss the development of security requirements and baseline security controls for federally owned/operated industrial/process control systems based on NIST SP800-53
- Attended by Federal stakeholders
  - Bonneville Power Administration
  - Southwestern Power Administration
  - Western Area Power Administration
  - DOI – Bureau of Reclamation
  - DOE
  - DOE Labs (Argonne, Sandia, Idaho)
  - FERC
  - DHS

ICS Workshop Goals

- Develop draft material for an Appendix or Supplemental Guidance material that addresses the application of 800-53 to ICS
- Review the 800-53 controls (requirements) to
  - Determine which controls are causing challenges when applied to ICS
  - Discuss why a specific control is causing a challenge
  - Develop guidance on the application (or non application) of that control to ICS
  - Determine if there are any compensating controls that could be applied to address the specific control that can't technically be met.

Result - SP800-53 Appendix I

- **Industrial Control Systems: Interim Guidance on the Application of Security Controls**
- Provides initial recommendations for organizations that own and operate industrial control systems:
  - Use Section 3.3 of Special Publication 800-53, *Tailoring the Initial Baseline*, to modify or adjust the recommended security control baselines when certain conditions exist that require that flexibility.
  - Develop appropriate rationale and justification as described in the compensating control section of 800-53 to meet the intent of a control that can't technically be met.

http://csrc.nist.gov/publications/drafts.html#sp800-53-Rev1

NIST Special Publication (SP) 800 series documents

- Special Publications in the 800 series are documents of general interest to the computer security community
- Established in 1990 to provide a separate identity for information technology security publications.
- Reports on research, guidance, and outreach efforts in computer security, and collaborative activities with industry, government, and academic organizations

NIST SP800-82

- **Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security**
- Purpose
  - Provide guidance for establishing secure SCADA and Industrial Control Systems, including the security of legacy systems
- Content
  - Overview of Industrial Control Systems (ICS)
  - ICS Vulnerabilities and Threats
  - ICS Security Program Development and Deployment
  - Network Architecture
  - ICS in the Federal Information Security Management Act (FISMA) Paradigm
  - ICS Security Controls
- Initial public draft - end August 2006

http://csrc.nist.gov/publications/drafts.html

SP800-53/NERC CIP Mappings

- Developed a bi-directional mapping and gap analysis between NIST SP800-53 and the NERC CIP standard to discover and propose modifications to remove any conflicts
- Initial results show that if the agency meets the requirements in NIST SP800-53, they will generally meet the NERC CIP requirements

Private Sector Strategy

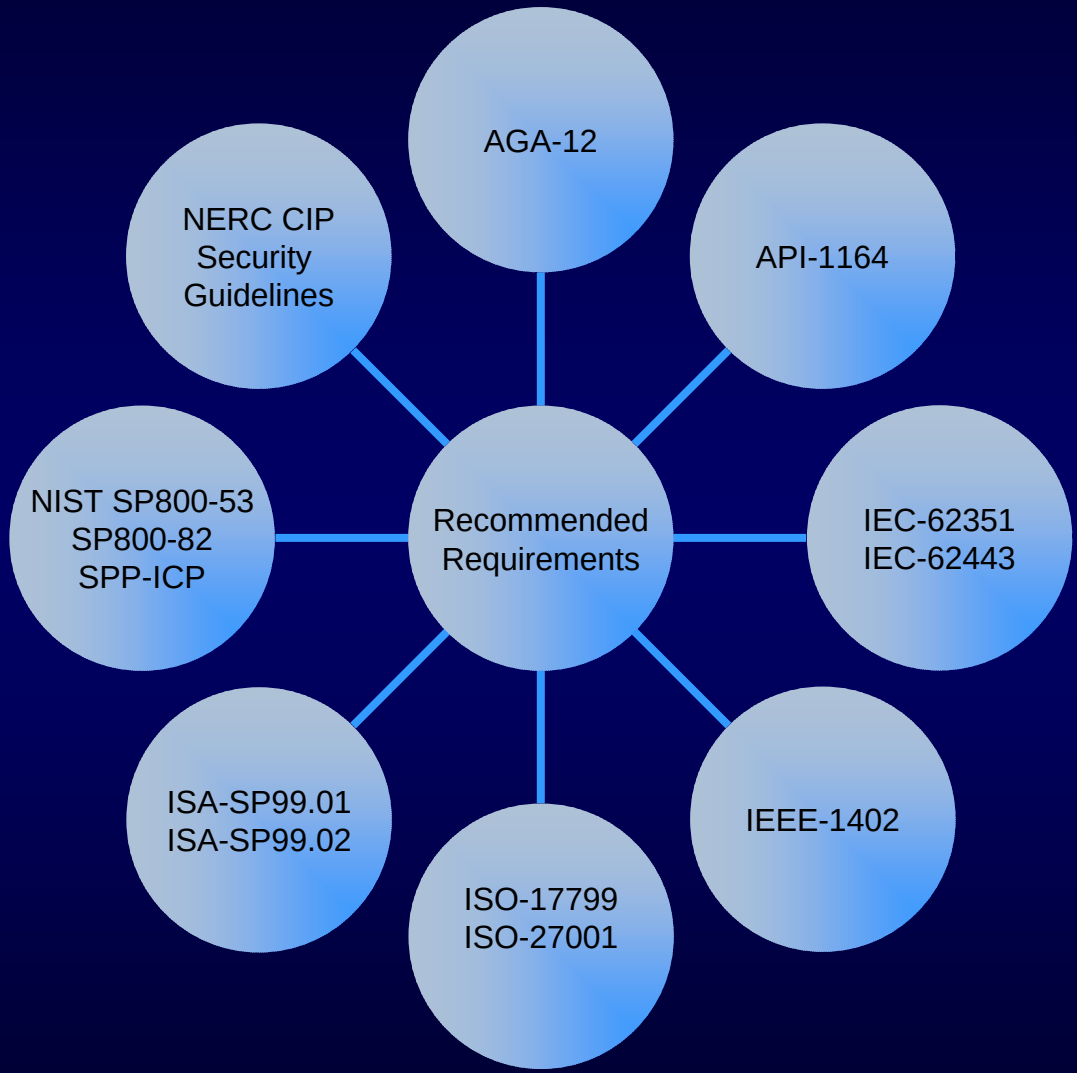
- **Standards for the ICS industry, if widely implemented, will raise the level of control systems security**
- **Greatest chance for industry acceptance and adoption is to have security requirements published in industry standards**
  - **ISA SP99 *Manufacturing and Control System Security* standard**
  - **IEC 62443 *Security for industrial process measurement and control –Network and system security* standard**

Recommended Requirements Document

- A baseline recommended cyber security requirements document is being drafted by the DHS CSSP Standards Awareness Team that identifies requirements that can be used by all sectors in the development of control system cyber security standards, recommended practices, etc.

- Starting point/reference document for organizations developing control system cyber security standards

Recommended Requirement Sources



ISA SP99

- Developing an ANSI Standard for Industrial Control System Security
  - Part 1 – Models and Terminology
  - Part 2 – Establishing a Manufacturing and Control Systems Program

    Part 3 – Operating a Manufacturing and Control Systems Program
  - Part 4 – Specific Security Requirements for Manufacturing and Control Systems
    - Recommended Requirements document will be vetted as a normative reference to develop the standard
    - The DHS CSSP Standards Awareness Team is planning to provide technical editing services to accelerate the development of this standard when WG4 is ready

http://www.isa.org/MSTemplate.cfm?MicrosoftID=988&CommitteeID=6821

Process Control Systems Forum (PCSF) Security Requirements Interest Group

- Newly formed Security Requirements Interest Group will be used to help accelerate and increase the visibility of the ISA-SP99 Part 4 effort
- Provide URL to the ISA-SP99 Part 4 effort to gather additional participation
- Publish the Recommended Requirements document so that it can be used by any organization in their preparation of standards or recommended practices
- Recommended Requirements document will not be vetted within this group, but within the specific organizations that are using the document (ISA SP99, IEC, etc.)

https://www.pcsforum.org/groups/78/

Summary

- **NIST SP800-53, Revision 1 - Appendix I**

  http://csrc.nist.gov/publications/drafts.html#sp800-53-Rev1
  - Provides Interim Guidance on the Application of 800-53 Security Controls to ICS

- **NIST SP800-82**

  http://csrc.nist.gov/publications/drafts.html
  - Provides Guidance for establishing secure SCADA and Industrial Control Systems
  - Initial Public Draft – end of August 2006

- **Recommended Requirements Document**
  - Identifies a harmonized set of requirements that can be used by all sectors in the development of control system cyber security standards.

- **ISA SP99**

  http://www.isa.org/MSTemplate.cfm?MicrosoftID=988&CommitteeID=6821
  - Developing an ANSI Standard for Industrial Control System Security

- **PCSF Security Requirements Interest Group**

  https://www.pcsforum.org/groups/78/
  - Vehicle to accelerate the development of security requirements standards

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

FISMA Project Leader

Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

Administrative Support

Peggy Himes
(301) 975-2489
peggy.himes@nist.gov

Senior Information Security Researchers and Technical Support

Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

Dr. Stu Katzke
(301) 975-4768
skatzke@nist.gov

Pat Toth
(301) 975-5140
patricia.toth@nist.gov

Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Matt Scholl
(301) 975-2941
matthew.scholl@nist.gov

Information and Feedback
Web: csrc.nist.gov/sec-cert
Comments: sec-cert@nist.gov

MEL/ISD Industrial Control Systems Co-Project Leader: **Keith Stouffer;**
(301) 975-3877; keith.stouffer@nist.gov