# Industrial Control System (ICS) Security: *An Overview of Emerging Standards, Guidelines, and Implementation Activities.*

Joe Weiss, PE, CISM
Executive Consultant
KEMA, Inc.
(408) 253-7934
joe.weiss@kema.com

Stuart Katzke, Ph.D.
Senior Research Scientist
National Institute of Standards and Technology
(301) 975-4768
skatzke@nist.gov

# Session Presentations

- Private sector industrial control system security standards, guidelines, and countermeasure implementation activities; Joe Weiss
- Applying NIST SP 800-53, Revision 1 to industrial control systems; Stu Katzke

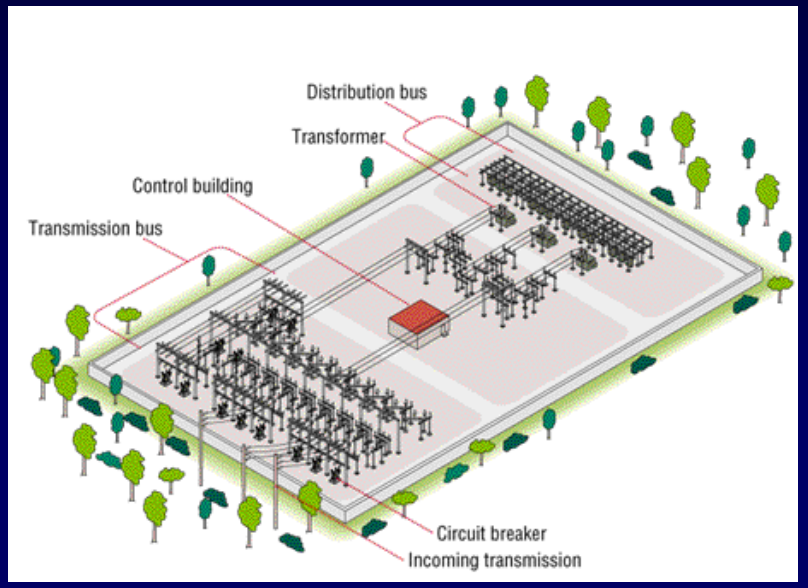
# Private sector industrial control system security standards, guidelines, and countermeasure implementation activities

Joe Weiss, PE, CISM
Executive Consultant
KEMA, Inc.
(408) 253-7934
joe.weiss@kema.com

# Industrial Control Systems - ICS

- What are ICS
  - SCADA, DCS, PLCs, Intelligent Field devices
- Used in all process control and manufacturing processes including electric, water, oil/gas, chemicals, auto manufacturing, etc

# SCADA




SCADA is used extensively in the electricity sector. Other SCADA applications include gas and oil pipelines, water utilities, transportation networks, and applications requiring remote monitoring and control. Similar to real-time process controls found in buildings and factory automation.

**CONTROL**

•Generator Set Points
•Transmission Lines
•Substation Equipment

**DATA**

•Critical Operational Data
•Performance Metering
•Events and Alarms

## Communication Methods

- Directly wired
- Power line carrier
- Microwave
- Radio (spread spectrum)
- Fiber optic

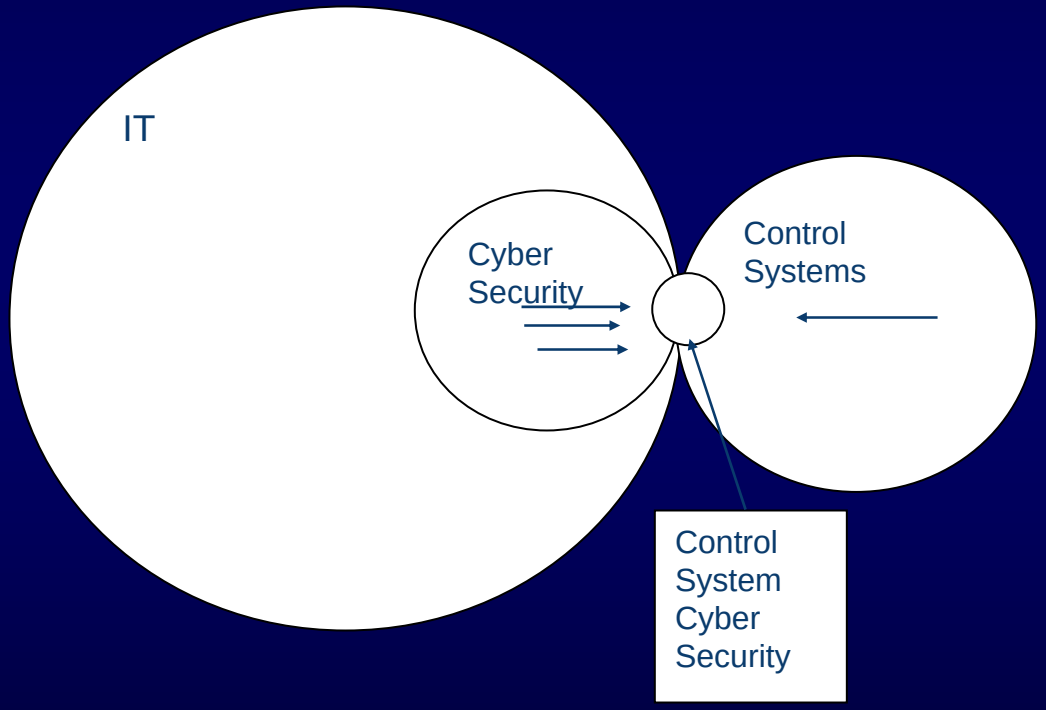
## Control Center

Provides network status, enables remote control, optimizes system performance, facilitates emergency operations, dispatching repair crews and coordination with other utilities.

# What Makes ICS Different than IT

- Deterministic systems with VERY high reliability constraints
  - Follow AIC rather than CIA
- Generally utilize a combination of COTS (Windows, etc) and proprietary RTOS
- Often are resource and bandwidth constrained
  - Block encryption generally does not work

# Why Are There So Few Experts



# ICS Security Myths

- Firewalls make you secure
- VPNs make you secure
- Encryption makes you secure
- IDSs can identify possible control system attacks
- Messaging can be one-way
- Field devices can’t be hacked
- You can keep hackers out
- You are secure if hackers can’t get in
- More and better widgets can solve security problems
- …

# Common ICS Vulnerabilities

- Ports and services open to outside
- Operating systems not “patched” with current releases
- Dial-up modems
- Improperly configured equipment (firewall does not guarantee protection)
- Improperly installed/configured software (e.g., default passwords)
- Inadequate physical protection
- Vulnerabilities related to “systems of systems” (component integration)

# Need for Private Sector ICS Standards

- IT security standards are not fully adequate
  - Need unique standards for field devices with proprietary RTOS
  - Need to be coordinated with IT
- Private industry ICS security requirements are different than for IT and DOD
  - Performance more important than security
- Lack of metrics and design requirements for industrial ICS

# Example Differences Between IT and ICS

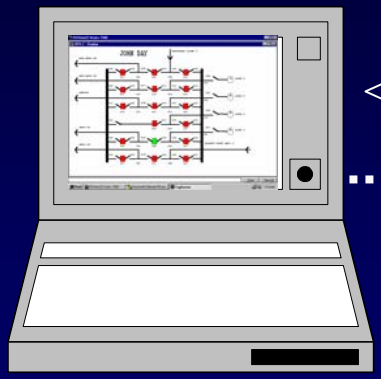
- Passwords
  - Unique, complex, changed frequently
- Patching
  - Timely with automated tools
- Administrator
  - Central administrator

- Passwords
  - Role-based, alpha, unchanged
- Patching
  - May not be timely, no automation
- Administrator
  - Control system engineer

# ICS Impacts

- More than 80 known cases (intentional and unintentional)
- All industries
  - Electric (T&D, fossil, hydro, and nuclear)
  - Oil/gas
  - Water
  - Chemicals
  - Manufacturing
  - Railroads
- Damage ranging from trivial to equipment damage and death

# Bench-Scale Vulnerability Demonstrations



SCADA Protocol (DNP 3.0)

Operator Interface

Protocol Analyzer
(Intruder)


Field Device
- Remote Terminal Unit (RTU)
- Intelligent Electronic Device (IED)
- Programmable Logic Controller (PLC)

Scenarios
- Denial of service
- Operator spoofing
- Direct manipulation of field devices
- Combinations of above

*Vulnerability implications vary significantly depending on the scenario and application*

# Very Few Publicly Identified Cases of Control System Cyber Events (Two attached are not public)

•**Event**: Unintentional substation communication failure caused by intentional Welchia worm traffic from unpatched system
•**Impact**: Shutdown of 30-40% of all communication traffic from the distribution SCADA to the Control Center
•**Lessons learned:** Use up-to-date patches and software & implement effective cyber security program/ protocols

•**Event**: Unsecured GIS mapping system (no firewall) enabled Internet-based targeted attack, resulting in loss of SCADA system
•**Impact**: SCADA servers and mapping system unavailable for two weeks
•**Lessons learned**: Isolate SCADA system from corporate LAN, install firewall between the DSL router and corporate LAN, install firewalls between frame relay and neighbors to isolate all non business-related ports

- More than 80 cases across multiple industries
- Impacts range from trivial to equipment damage to death
- Anecdotal evidence suggests other cases go unreported, for fear of vulnerability exposure, business liability

# Private Sector ICS Standards Activities

- Standards efforts ongoing internationally and by industry
- More than 40 standards and industry organizations world-wide
  - Need effective coordination
  - NIST 800-53 can help provide a common basis

# Typical ICS Standards

- By Industry
  - NERC (electric) , NRC (nuclear), IEC TC57 (electric), AGA (gas), AWWA (water), etc.
- Generic
  - ISA SP99, IEC TC65, ISO-17799

# ISA SP99

- Developing an Standard for Industrial Control System Security
  - Part 1 – Terminology, Concepts and Models
  - Part 2 – Establishing an Industrial Automation and Control Systems Program
  - Part 3 – Operating an Industrial Automation and Control Systems Program
  - Part 4 – Security Requirements for Industrial Automation and Control Systems

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

# Why the Need to Extend NIST SP 800-53

- NIST SP 800-53 was developed for the traditional IT environment
- It assumes ICSs are information systems
- When organizations attempted to utilize SP 800-53 to protect ICSs, it led to difficulties in implementing SP 800-53 countermeasures because of ICS-unique needs

# Applying NIST Special Publication (SP) 800-53 to Industrial Control Systems

Stuart Katzke, Ph.D.
Senior Research Scientist
National Institute of Standards and Technology
(301) 975-4768
skatzke@nist.gov

# FISMA Legislation

***Overview***

"Each federal agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source…"

**-- Federal Information Security Management Act of 2002**

# NIST Publications

- Federal Information Processing Standards (FIPS)
- Special Publication (SP) 800 Series documents

# Federal Information Processing Standards (FIPS)

- Approved by the Secretary of Commerce
- Compulsory and binding standards for federal agencies non-national security information systems
- Voluntary adoption by federal national security community and private sector
- Since FISMA requires that federal agencies comply with these standards, agencies may not waive their use for non-national security information systems

# 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 guidance, research, and outreach efforts in computer security, and collaborative activities with industry, government, and academic organizations
- Agencies must follow NIST 800 series guidance documents; but
- 800 series documents generally allow agencies some latitude in their application

# The Risk Framework

***Starting Point***

**FIPS 199 / SP 800-60**

**Security Categorization**

Define criticality /sensitivity of information system according to potential impact of loss

**FIPS 200 / SP 800-53**

**Security Control Selection**

Select minimum (baseline) security controls to protect the information system; apply tailoring guidance as appropriate

**FIPS 200 / SP 800-53 / SP 800-30**

**Security Control Refinement**

Use risk assessment results to supplement the tailored security control baseline as needed to ensure adequate security and due diligence

**SP 800-18**

**Security Control Documentation**

Document in the security plan, the security requirements for the information system and the security controls planned or in place

**SP 800-70**

**Security Control Implementation**

Implement security controls; apply security configuration settings

**SP 800-53A**

**Security Control Assessment**

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements)

**SP 800-37**

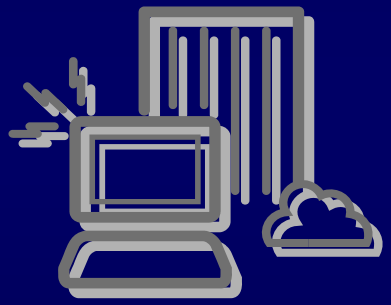
**System Authorization**

Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system operation

**SP 800-37 / SP 8800-53A**

**Security Control Monitoring**

Continuously track changes to the information system that may affect security controls and reassess control effectiveness



# Federal Agency Challenges

- Federal agencies required to apply NIST SP 800-53 *Recommended Security Controls for Federal Information Systems* (general IT security requirements) to their control systems
- Federal agencies that own/operates control systems could potentially have to meet 2 standards (NIST SP 800-53 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 SP 800-53
- Develop bi-directional mapping and gap analysis between NIST SP 800-53 and the NERC CIP standard to discover and propose modifications to remove any conflicts
- Develop an “ICS” interpretation of SP 800-53 that would also comply with the management, operational and technical controls in the NERC CIP.

# Federal Strategy (continued)

- Develop a guidance document (NIST SP 800-82) on how to secure industrial control systems
- Work with government and industry ICS community to foster convergence of ICS security requirements
  - DHS, DoE, FERC, DoI, ICS agencies (BPA, SWPA, WAPA)
  - Industry standards groups
    - NERC
    - ISA SP99 *Industrial Automation and Control System Security* standard
    - IEC 62443 *Security for industrial process measurement and control –Network and system security* standard

# Federal ICS Workshop

- Workshop April 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 SP 800-53
- 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.

# ICS Workshop Results

- Initial results incorporated in SP 800-53, Rev 1, July 2006
  - **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
- Continuing work to be reflected in future revisions to SP 800-53
- http://csrc.nist.gov/publications/drafts.html#sp800-53-Rev1

# Comparing SP 800-53 Controls and NERC CIP Standards

- Comparing control sets from different organizations/ frameworks is difficult and subject to interpretation
- NERC CIP standards generally correspond to controls in one or more of the SP 800-53 control families
  - Most NERC CIP requirements* correspond to controls in SP 800-53.
  - NERC CIP measures* correspond to assessments of the security controls in SP 800-53 described in SP 800-53A *Guide for Assessing the Security Controls in Federal Information Systems*.
  - NERC CIP compliance* best corresponds to SP 800-37 *Guide for the Security Certification and Accreditation of Federal Information Systems*



* *Requirements, measures,* and *compliance* are reserved words defined in the NERC CIP

# Mapping Table Extract

| | | | CIP-002 | | | | CIP-003 | | | | | | CIP-004 | | | | CIP-005 | | | | | CIP-006 | | | | | | CIP-007 | | | | | | | | | CIP-008 | | CIP-009 | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | R1. Critical Asset Identification | R2. Critical Asset Identification | R3. Critical Cyber Asset Identification | R4. Annual Approval | R1. Cyber Security Policy | R2. Leadership | R3. Exceptions | R4. Information Protection | R5. Access Control | R6. Change Control and Confign Mgmt | R1. Awareness | R2. Training | R3. Personnel Risk Assessment | R4. Access | R1. Electronic Security Perimeter | R2. Electronic Access Controls | R3. Monitoring Electronic Access | R4. Cyber Vulnerability Assessment | R5. Documentation Review and | R1. Physical Security Plan | R2. Physical Access Controls | R3. Monitoring Physical Access | R4.Logging Physical Access | R5. Access Log Retention | R6. Maintenance and Testing | R1. Test Procedures | R2. Ports and Services | R3. Security Patch Management | R4. Malicious Software Prevention | R5. Account Management | R6. Security Status Monitoring | R7. Disposal or Redeployment | R8. Cyber Vulnerability Assessment | R9. Documentation Review and | R1. Cyber Security Incident Response | R2. Cyber Security Incident | R1. Recovery Plans | R2. Exercises | R3. Change Control | R4. Backup and Restore | R5. Testing Backup Media |
| NERC CIP FINAL | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Other - Notes | | | | | | 2 | 3 | 2 | 11 | 2 | 2, 7 | 2 | | | | | | | 18 | | | 12 | | | | | | | 19 ,2 | | 21 | 21 | | | | | 22 | | 23 | | | | |
| SP 800-53 Rev. 1 Controls | | Count | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 5 | 3 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Access Control | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AC-1 | Access Control P & P | 4 | | | | | 8 | | | | 8 | | | | | | | 13 | | | | 13 | | | | | | | | | | | | | | | | | | | | | |
| AC-2 | Account Management | 3 | | | | | | | | | 13 | | | | | 17 | | | | | | | | | | | | | | | | 13 | | | | | | | | | | |
| AC-3 | Access Enforcement | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AC-4 | Information Flow Enforcement | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AC-5 | Separation of Duties | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AC-6 | Least Privilege | 3 | | | | | | | | | | | | | | 17 | | | | | | | | | | | | 13 | | | | 13 | | | | | | | | | | |
| AC-7 | Unsuccessful Logon Attempts | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AC-8 | System Use Notification | 1 | | | | | | | | | | | | | | | | 8 | | | | | | | | | | | | | | | | | | | | | | | | | |
| AC-9 | Previous Logon Notification | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AC-10 | Concurrent Session Control | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AC-11 | Session Lock | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AC-12 | Session Termination | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AC-13 | Supervision and Review—A C | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AC-14 | Permitted Actions without I or A | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AC-15 | Automated Marking | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AC-16 | Automated Labeling | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AC-17 | Remote Access | 3 | | | | | | | | | | | | | | | 12 | 9 | 8 | | | | | | | | | | | | | | | | | | | | | | | | |
| AC-18 | Wireless Access Restrictions | 3 | | | | | | | | | | | | | | | 7 | 17 | 17 | | | | | | | | | | | | | | | | | | | | | | | | |
| AC-19 | Access Control for Portable and Mobile Systems | 2 | | | | | | | | | | | | | | | | 17 | 17 | | | | | | | | | | | | | | | | | | | | | | | | |
| AC-20 | Personally Owned Information Systems | 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| LEGEND |
|---|
| High baseline (no shading) |
| Moderate baseline (12.5% grey shading) |
| Low baseline (25% grey shading) |
| Not in baseline (50% grey shading) |

## Codes

8 NERC req ≅ SP 800-53 controls

9 NERC more specific than SP 800-53 control

13 NERC ⊂ SP 800-53 control

17 NERC less specific than SP 800-53 control

# SP 800-53/NERC CIP Mapping Findings (1 of 2)

- Generally, conforming to moderate baseline in SP 800-53 generally complies with the management, operational and technical security requirements of the NERC CIPs; the converse is not true.
- NERC contains requirements that fall into the category of business risk reduction
  - High level business-oriented requirements
  - Demonstrate that enterprise is practicing due diligence
  - SP 800-53 does not contain analogues to these types of requirements as SP 800-53 focuses on information security controls (i.e., management, operational, and technical) at the information system level.

# SP 800-53/NERC CIP Mapping Findings (2 of 2)

- NERC approach is to define critical assets first and their cyber components second
  - Definition of critical asset vague
  - Non-critical assets not really addressed
- FIPS 199 specifies procedure for identifying security impact levels based on a worst case scenario (called security categorization)
  - applies to all information and the information system
  - Considers impact to the organization, potential impacts to other organizations and, in accordance with the Patriot Act and Homeland Security Presidential Directives, potential national-level impacts
  - Confidentiality, availability, and integrity evaluated separately
  - Possible outcomes are low, moderate, and high
  - Highest outcome applies to system (High Water Mark)
- Documentation requirements differ; more study required

# NIST SP 800-82

- Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security
  - Provide guidance for establishing secure SCADA and ICS, including the security of legacy systems
- Content
  - Overview of ICS
  - ICS Characteristics, Threats and Vulnerabilities
  - ICS Security Program Development and Deployment
  - Network Architecture
  - ICS Security Controls
  - Appendixes
    - Current Activities in Industrial Control System Security
    - Emerging Security Capabilities
    - ICS in the Federal Information Security Management Act (FISMA) Paradigm
- Initial public draft released September 2006
- http://csrc.nist.gov/publications/drafts.html

# SP 800-82 Audience

- Control engineers, integrators and architects when designing and implementing secure SCADA and/or ICS
- System administrators, engineers and other IT professionals when administering, patching, securing SCADA and/or ICS
- Security consultants when performing security assessments of SCADA and/or ICS
- Managers responsible for SCADA and/or ICS
- Researchers and analysts who are trying to understand the unique security needs of SCADA and/or ICS
- Vendors developing products that will be deployed in SCADA and/or ICS

# Future NIST Plans

- Anticipated FY07 Products
  - White paper on ICS cyber security in the FISMA paradigm
  - Annotated SP 800-53 addressing conformance to NERC CIP
  - Annotated NERC CIP showing correspondence to FISMA paradigm
  - Input to revision 2 of SP 800-53
- Continue working with the federal ICS stakeholders
  - Including FERC, Department of Homeland Security (DHS), Department of Energy (DOE), the national laboratories, and federal agencies that own, operate, and maintain ICSs
  - To develop an interpretation of SP 800-53 for ICSs that permits real/practical improvements to the security of ICSs and, to the extent possible, ensures compliance with the management, operational, and technical requirements in the NERC CIP standards
- Continue working with private sector ICS stakeholders

# NIST ICS Security Project Summary

- Issue ICS security guidance
  - Evolve SP 800-53 *Recommended Security Controls for Federal Information Systems* security controls to better address ICSs
  - Publish SP 800-82 *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security* initial public draft released September 2006
- Improve the security of public and private sector ICSs
  - Raise the level of control system security
    - R&D and testing
  - Work with on-going industry standards activities
    - Assist in standards and guideline development
    - Foster convergence
    - http://csrc.nist.gov/sec-cert/ics

# NIST ICS Security Project Contact Information

***Project Leaders***

**Keith Stouffer**
**(301) 975-3877**
**keith.stouffer@nist.gov**

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

**sec-ics@nist.gov**

***Web Pages***

**Federal Information Security Management Act (FISMA) Implementation Project**

**http://csrc.nist.gov/sec-cert**

**NIST ICS Security Project**

**http://csrc.nist.gov/sec-cert/ics**

# Questions