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

Joe Weiss, PE, CISM
Executive Consultant
Applied Control Solutions, LLC
(408) 253-7934
joe.weiss@realtimeacs.com

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

What Makes ICS Different than IT

- Deterministic systems with VERY high reliability constraints
  - Priority is availability, integrity, then confidentiality (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

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 general IT
  - 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, defaults often unchanged
- Patching
  - May not be timely, no automation
- Administrator
  - Control system engineer

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 counter-measures because of ICS-unique needs

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

Current State of Affairs

- Continuing serious attacks on federal information systems, large and small; targeting key federal operations and assets.
- Significant exfiltration of critical and sensitive information and implantation of malicious software.
- Attacks are organized, disciplined, aggressive, and well resourced; many are extremely sophisticated.
- Adversaries: nation states, terrorist groups, hackers, criminals, and any individuals or groups with intentions of compromising a federal information system.
- Increasing number of trusted employees taking dangerous and imprudent actions with respect to organizational information systems.

FISMA Project Strategic Vision

- We are building a solid foundation of information security across one of the largest information technology infrastructures in the world based on comprehensive security standards and technical guidance.
- We are institutionalizing a comprehensive Risk Management Framework that promotes flexible, cost-effective information security programs for federal agencies.
- We are establishing a fundamental level of “security due diligence” for federal agencies and their contractors based on minimum security requirements and security controls.

FISMA Project Characteristics

- The NIST *Risk Management Framework* and the associated security *standards* and *guidance* documents provide a process that is:
  - Disciplined
  - Flexible
  - Extensible
  - Repeatable
  - Organized
  - Structured

"Building information security into the infrastructure of the organization… so that critical enterprise missions and business cases will be protected."

Key Standards and Guidelines

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Requirements)
- NIST Special Publication 800-18 (Security Planning)
- NIST Special Publication 800-30 (Risk Management)
- NIST Special Publication 800-37 (Certification & Accreditation)
- NIST Special Publication 800-53 (Recommended Security Controls)
- NIST Special Publication 800-53A (Security Control Assessment)
- NIST Special Publication 800-59 (National Security Systems)
- NIST Special Publication 800-60 (Security Category Mapping)

Many other FIPS and NIST Special Publications provide security standards and guidance supporting the FISMA legislation…

Risk Management Framework

Starting Point

FIPS 199 / SP 800-60

CATEGORIZE
Information System

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

FIPS 200 / SP 800-53

SELECT
Security Controls

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

SP 800-53 / SP 800-30

SUPPLEMENT
Security Controls

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

SP 800-18

DOCUMENT
Security Controls

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

SP 800-70

IMPLEMENT
Security Controls

Implement security controls; apply security configuration settings

SP 800-53A

ASSESS
Security Controls

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

SP 800-37

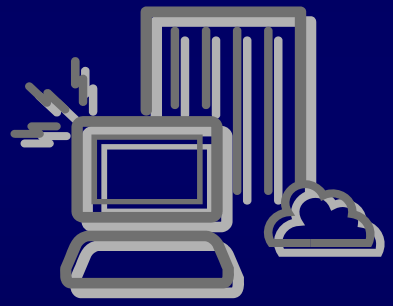
AUTHORIZE
Information System

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

SP 800-37 / SP 800-53A

MONITOR
Security Controls

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



Six Essential Activities

- FIPS 199 security categorizations
- Identification of common controls
- Application of tailoring guidance for FIPS 200 and SP 800-53 security controls
- Effective strategies for continuous monitoring of security controls (assessments)
- Security controls in external environments
- Use restrictions

Security Categorization

- The most important step in the Risk Management Framework.
- Affects all other steps in the framework from selection of security controls to level of effort in assessing control effectiveness.
- Expect the distribution of categorized federal information systems to look like a normal or Bell-curve centered on moderate-impact.

Security Categorization

- Important change in SP 800-53, Revision 1, security control RA-2.
- FIPS 199 security categorizations consider both agency, other organizations, and national impacts.
- New language:

  "The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system."

Common Controls

- Categorize all information systems first, enterprise-wide.
- Select common controls for all similarly categorized information systems (low, moderate, high impact).
- Be aggressive; when in doubt, assign a common control.
- Assign responsibility for common control development, implementation, assessment, and tracking (or documentation of where employed).

Common Controls

- Ensure common control-related information (e.g., assessment results) is shared with all information system owners.
- In a similar manner to information systems, common controls must be continuously monitored with results shared with all information system owners.
- Information system owners must supplement the common portion of the security control with system specific controls as needed to complete security control coverage.

Common Controls

- The more common controls an organization identifies, the greater the cost savings and consistency of security capability during implementation.
- Common controls can be assessed by organizational officials (other than the information system owner), thus taking responsibility for effective security control implementation.

Tailoring Guidance

- FIPS 200 and SP 800-53 provide significant flexibility in the security control selection and specification process—if organizations choose to use it.
- Includes:
  - Scoping guidance;
  - Compensating security controls; and
  - Organization-defined security control parameters.

Scoping Guidance

- Common security control-related considerations
- Operational/environmental-related considerations
- Physical Infrastructure-related considerations
- Public access-related considerations
- Technology-related considerations
- Policy/regulatory-related considerations
- Scalability-related considerations
- Security objective-related considerations

Scoping Guidance I

- Common security control-related considerations

  Common controls are managed by an organizational entity other than the information system owner. Organizational decisions on which security controls are viewed as common controls may greatly affect the responsibilities of individual information system owners.

- Operational/environmental-related considerations

  Security controls that are dependent on the nature of the operational environment are applicable only if the information system is employed in an environment necessitating the controls. (e.g., physical security controls for space-based information systems; temperature/humidity controls for information system components in outdoor locations)

Scoping Guidance II

- Physical Infrastructure-related considerations

  Security controls that refer to organizational facilities (e.g., physical controls such as locks and guards, environmental controls for temperature, humidity, lighting, fire, and power) are applicable only to those sections of the facilities that directly provide protection to, support for, or are related to the information system.

- Public access-related considerations

  Security controls associated with public access information systems should be carefully considered and applied with discretion since some security controls from the specified control baselines (e.g., identification and authentication, personnel security controls) may not be applicable to users accessing information systems through public interfaces.

Scoping Guidance III

- Technology-related considerations
  - Security controls that refer to specific technologies (e.g., wireless, cryptography, public key infrastructure) are applicable only if those technologies are employed or are required to be employed within the information system.
  - Security controls are applicable only to the components of the information system that provide or support the security capability addressed by the control and are sources of potential risk being mitigated by the control.
  - Security controls that can be either explicitly or implicitly supported by automated mechanisms, do not require the development of such mechanisms if the mechanisms do not already exist or are not readily available in commercial or government off-the-shelf products.

Scoping Guidance IV

- Policy/regulatory-related considerations

  Security controls that address matters governed by applicable laws, Executive Orders, directives, policies, standards, or regulations (e.g., privacy impact assessments) are required only if the employment of those controls is consistent with the types of information and information systems covered by the applicable laws, Executive Orders, directives, policies, standards, or regulations.

Scoping Guidance V

- Scalability-related considerations

  Security controls are scalable with regard to the extent and rigor of the control implementation. Scalability is guided by the FIPS 199 security categorization of the information system being protected.

- Security objective-related considerations

  Security controls that uniquely support the confidentiality, integrity, or availability security objectives may be downgraded to the corresponding control in a lower baseline (or appropriately modified or eliminated if not defined in a lower baseline) if, and only if, the downgrading action: (i) is consistent with the FIPS 199 security categorization before moving to the high water mark; (ii) is supported by an organizational assessment of risk; and (iii) does not affect the security-relevant information within the information system.

Compensating Security Controls

- A compensating security control is a management, operational, or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provides equivalent or comparable protection for an information system.
- Mission-driven considerations may require alternate solutions (e.g., AC-11 session lock not advisable in certain systems).

Compensating Security Controls

- The organization selects a compensating control from NIST SP 800-53, or if an appropriate compensating control is not available in the security control catalog, the organization adopts a suitable compensating control;
- The organization provides a complete and convincing rationale for how the compensating control provides an equivalent security capability or level of protection for the information system and why the related baseline security control could not be employed; and
- The organization assesses and formally accepts the risk associated with employing the compensating control in the information system.

Organization-defined Parameters

- Security controls containing organization-defined parameters (i.e., assignment and/or selection operations) give organizations the flexibility to define selected portions of the controls- to support specific organizational requirements or objectives.

CP-9 INFORMATION SYSTEM BACKUP

Control: The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [*Assignment: organization-defined frequency*] and protects backup information at the storage location.

Continuous Monitoring

- Transforming certification and accreditation from a static to a *dynamic* process.
- Strategy for *monitoring* selected security controls; which controls selected and how often assessed.
- Control selection driven by *volatility* and *Plan of Action and Milestones (POAM).*
- Facilitates annual FISMA *reporting* requirements.

External Service Providers

- Organizations are becoming increasingly reliant on information system services provided by external service providers to carry out important missions and functions.
- External information system services are services that are implemented outside of the system's accreditation boundary (i.e., services that are used by, but not a part of, the organizational information system).
- Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges.

External Service Providers

- Organizations have varying degrees of control over external service providers.
- Organizations must establish trust relationships with external service providers to ensure the necessary security controls are in place and are effective in their application.
- Where control of external service providers is limited or infeasible, the organization factors that situation into its risk assessment.

Information System Use Restrictions

- A method to reduce or mitigate risk, for example, when:
  - Security controls cannot be implemented within technology and resource constraints; or
  - Security controls lack reasonable expectation of effectiveness against identified threat sources.
- Restrictions on the use of an information system are sometimes the only prudent or practical course of action to enable mission accomplishment in the face of determined adversaries.

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/operate electric power-related ICSs could potentially have to meet 2 standards (FIPS 200/NIST SP 800-53 and FERC standards)

Federal Strategy (1 of 3)

- Develop bi-directional mapping and gap analysis between NIST SP 800-53 and the North America Electric Reliability Corporation's (NERC) Critical Infrastructure Protection standards (CIPs)
- If needed, propose modifications to SP 800-53 management, operational and technical security requirements to ensure "coverage" of the NERC CIPs' respective security requirements.
- Held two federal workshops (April 2006 and March 2007) to discuss:
  - The applicability of FIPS 199, FIPS 200, and NIST SP 800-53 to federally owned/operated ICSs.
  - The comparison of SP 800-53 to the NERC CIPs
  - Development of an ICSs interpretation of SP 800-53

Federal Strategy (2 of 3)

- Develop an “ICS” interpretation of SP 800-53 that would also comply with the management, operational and technical security requirements in the NERC CIP.
- Develop a comprehensive guidance document (NIST SP 800-82) on how to secure industrial control systems.

Federal Strategy (3 of 3)

- 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 Workshops

- 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

- Workshop March 27-28, 2007 at NIST to discuss and vet draft security requirements and baseline security controls for federally owned/operated industrial/process control systems based on NIST SP 800-53

- Initial public draft scheduled for release Summer 2007

Federal ICS Workshops

- Attended by Federal stakeholders
  - Bonneville Power Administration
  - Southwestern Power Administration
  - Tennessee Valley Authority
  - Western Area Power Administration
  - Federal Aviation Administration
  - DOI Bureau of Reclamation
  - DOE
  - DOE Labs (Argonne, Sandia, Idaho)
  - FERC
  - DHS

NIST Workshop on Applying NIST SP 800-53

August 16-17, 2007

- Follows the Control System Cyber Security Conference, Knoxville, TN
- Representatives from national and international industrial control system (ICS) communities (e.g. electric, oil, gas, water, manufacturing)
- Purpose:
  - To share information about SP 800-53
  - To obtain direct input/comments on SP 800-53
  - To determine level of interest in voluntarily adopting and using NIST's ICS interpretation of NIST Special Publication (SP) 800-53.

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 Confgn 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 Summary

- NERC CIPs do not provide levels of protection commensurate with the mandatory federal standards prescribed by NIST (in FIPS 200/SP 800-53) for protecting non-national security information and information systems
- NIST recommends FERC consider issuing interim cyber security standards for the bulk electric system that:
  - Are a derivative of the NERC CIPs (e.g., NERC CIPs; NERC CIPs appropriately modified, enhanced, or strengthened), and
  - Would allow for planned transition (say in two to three years) to cyber security standards that are identical to, consistent with or based on SP 800-53 and related NIST standards and guidelines (as interpreted for ICSs).
- http://csrc.nist.gov/sec-cert/ics/papers/ICS-in-SP800-53_final_21Mar07.pdf

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#sp800-82

FY 2007 NIST Plans

- Anticipated Products
  - White paper on ICS cyber security in the FISMA paradigm
  - Annotated SP 800-53 addressing conformance to NERC CIP
  - Draft ICS interpretation of SP 800-53
  - ICS Workshop August 16-17, 2007 in Knoxville
  - SP 800-82: *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*
- 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
- Continue working with private sector ICS stakeholders

White Paper on ICS Cyber Security in the FISMA Paradigm

- FISMA Paradigm includes FIPS 199 and 200, SPs 800-37, 53, and 53A
- Actual experiences (successes, difficulties encountered, and lessons learned) from federal agencies (e.g., BPA, TVA, SWPA, WAPA, DOI) when performing security categorization and applying/interpreting the minimum baseline security controls, including tailoring, non-applicable controls, and compensating controls.
- Private sector's experience in implementing security controls in ICSs (if and/or when such information is available).
- Treatment of fragile systems (i.e., systems that tend to fail if their design assumptions are violated by contemporary security controls).

ISO 27000 series – NIST Risk Management Framework (RMF) Convergence

- Preliminary discussions are being held with the British Standards Institute on:
  - Comparison of 27001 with NIST RMF
  - Possibility of achieving dual conformance
  - Would also apply to ICS interpretation of SP 800-53
- Study being conducted by a federal agency

Conjecture

- SP 800-53 is a superset of ISO 17799/27002 (fact)
- The NIST RMF, including SP 800-53, can be considered as a “FISMA” instantiation or interpretation of 27001.
- As such, compliance with the NIST RMF will ensure compliance with 27001 (ISMS).
- Therefore, compliance with the RMF and SP 800-53 ICS will also ensure compliance with 27001
- In general, compliance with 27001 will not ensure compliance with the NIST RMF
- A delta set of FISMA-related requirements beyond those already in 27001 will have to be defined to extend general compliance with 27001 to the FISMA interpretation of 27001
- A 27001 compliant organization would be required to comply with the delta to be FISMA-compliant

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