NIST's Industrial Control System (ICS) Security Project

Presented at the:

Secure Manufacturing in the Age of Globalization Workshop

November 28, 2007

Stuart Katzke and Keith Stouffer

National Institute of Standards and Technology

skatzke@nist.gov

Keith.stouffer@nist.gov

Presentation Contents

- *NIST's FISMA Implementation Project*
  - *NIST Risk Management Framework*
  - *Draft Special Publication 800-39*
  - *Special Publication 800-53, Revision 1*
- *NIST Industrial Control System Project*
  - *NIST Draft SP 800-53, Revision 2 for industrial control systems*
  - *NIST SP 800-82: Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security (2nd Draft)*

NIST's FISMA Implementation Project:

Phase I (2003 – 2008)

Phase II (2007 – 2010)

Phase I

- *Mission: Develop and propagate core set of security standards and guidelines for federal agencies and support contractors.*
- *Timeline: 2003-2008*
- *Status: On track to complete final publications in FY08.*

Phase II

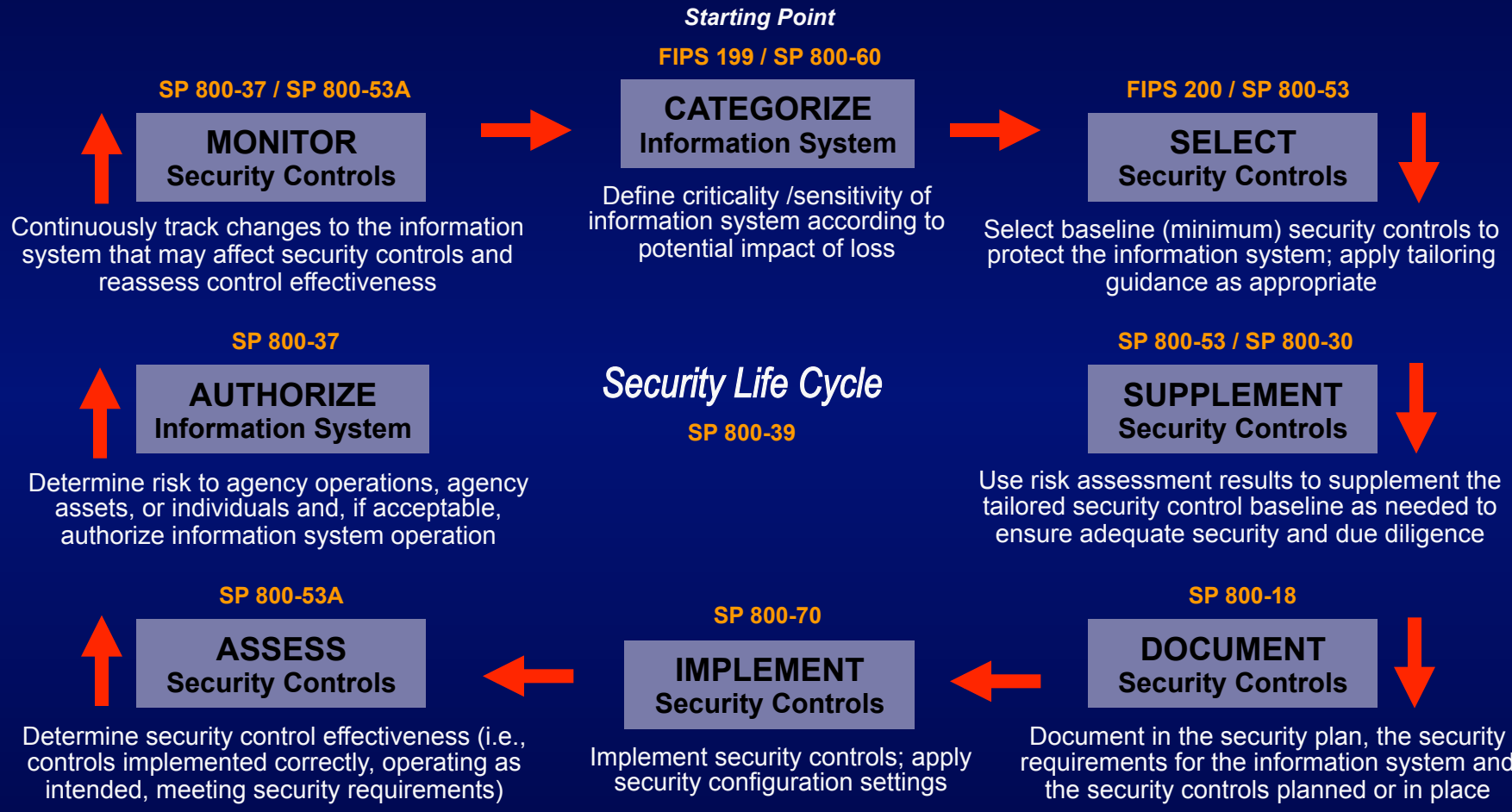
- *Mission: Develop and implement a standards-based organizational credentialing program for public and private sector entities to demonstrate core competencies for offering security services to federal agencies.*
- *Timeline: 2007-2010*
- *Status: Projected initiated; Draft NISTIR 7328.*

Phase I Publications

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Requirements)
- NIST Special Publication 800-18 (Security Planning)
- NIST Special Publication 800-30 (Risk Assessment) *
- NIST Special Publication 800-39 (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) *

* Publications currently under revision.
** Publications currently under development.

Risk Management Framework



A Unified Framework

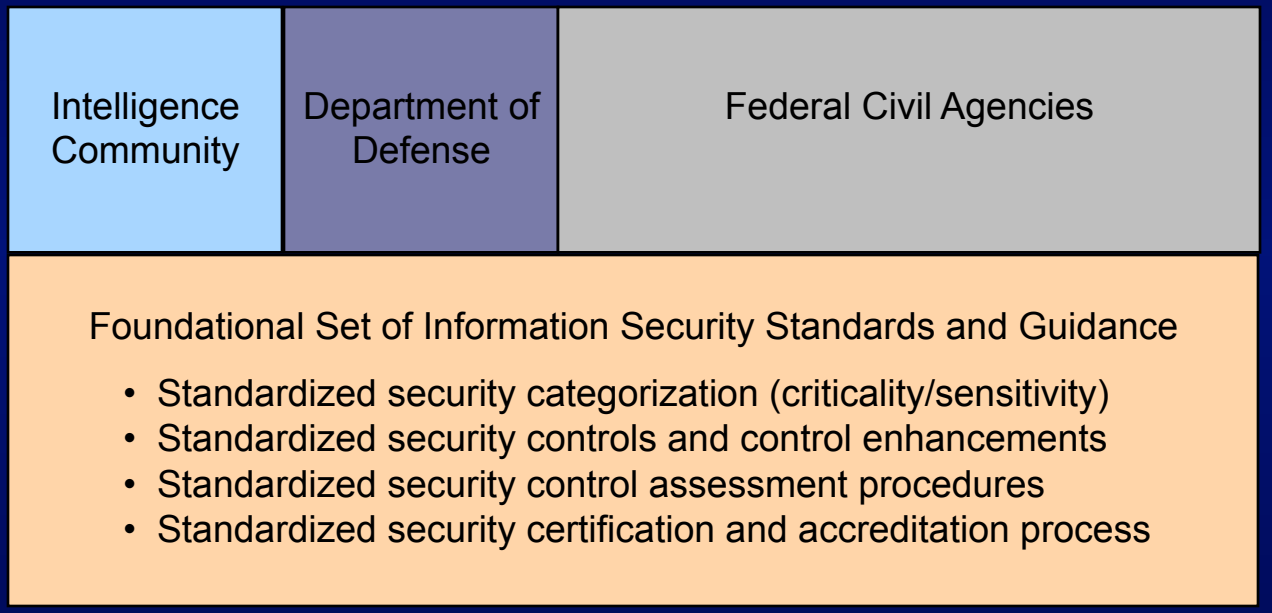
Civil, Defense, Intelligence Community Collaboration

The Generalized Model

Unique Information Security Requirements

The "Delta"

Common Information Security Requirements



National security and non national security information systems

Special Publication 800-39

Managing Risk from Information Systems
An Enterprise Perspective

- Extending the Risk Management Framework to enterprises.
- Risk-based mission protection.
- Common controls.
- Trustworthiness of information systems.
- Establishing trust relationships among enterprises.
- Risk executive function.
- Strategic planning considerations (defense-in-breadth).

Risk-based Mission Protection (1)

- *A Risk-based protection strategy requires the information system owner to:*
  - *Determine the appropriate balance between the risks from and the benefits of using information systems in carrying out their organizational missions and business functions*
  - *Carefully select, tailor, and supplement the safeguards and countermeasures (i.e., security controls) for information systems necessary to achieve this balance*

Risk-based Mission Protection (2)

- *A Risk-based protection strategy requires the authorization official to:*
  - *Take responsibility for the information security solutions agreed upon and implemented within the information systems supporting the organization*
  - *Fully acknowledge and explicitly accept the risks to organizational operations, organizational assets, individuals, other organizations, and the Nation that result from the operation and use of information systems to support the organization's missions and business functions*
  - *Be accountable for the results of their information security-related decisions.*

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 (including 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.*
- *The more common controls an enterprise identifies, the greater the cost savings and consistency of security capability during implementation.*

Business Relationships

Supply Chain Risks

- *Enterprises are becoming increasingly reliant on information system services and information provided by external providers to carry out important missions and business functions.*
- *External service provider relationships are established in a variety of ways—joint ventures, business partnerships, outsourcing arrangements, licensing agreements, supply chain exchanges.*
- *The growing dependence on external service providers and the relationships being forged with those providers present new challenges for enterprises, especially in the area of information security.*

Supply Chain Uncertainty

Challenges with using external providers include:

- *Defining the types of services and information provided to the enterprise.*
- *Describing how the services and information are protected in accordance with the security requirements of the enterprise.*
- *Obtaining the necessary assurances that the risk to the enterprise resulting from the use of the services or information is at an acceptable level.*

Information System Trustworthiness

- *Trustworthiness is a characteristic or property of an information system that expresses the degree to which the system can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system.*
- *Trustworthiness defines the security state of the information system at a particular point in time and is measurable.*

Information System Trustworthiness

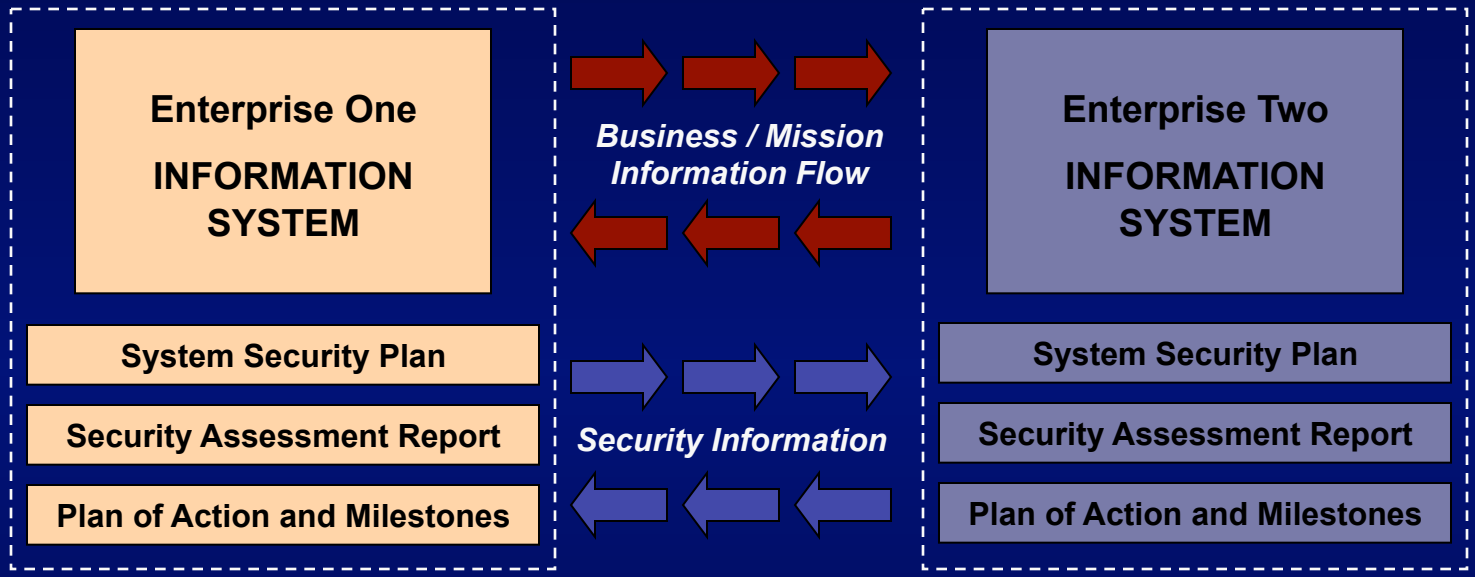
- *Security functionality*
  - *Security-related functions or features of the system, for example, identification and authentication mechanisms, access control mechanisms, auditing mechanisms, and encryption mechanisms.*
- *Quality of development and implementation*
  - *Degree to which the functionality is correct, always invoked, non bypassable, and resistant to tampering.*
  - *Well-defined security policy models, structured, disciplined, and rigorous hardware and software development techniques, and good system/security engineering principles and concepts.*
- *Security assurance*
  - *Grounds for confidence that the claims made about the functionality and quality of the system are being met.*
  - *Evidence brought forward regarding the design and implementation of the system and the results of independent assessments.*

Elements of Trust

- *Trust is earned by prospective service providers/partners:*
  - *Identifying the **common goals and objectives** for the provision of services or information sharing;*
  - *Agreeing upon the **risk** associated with the provision of such services or information sharing;*
  - *Agreeing upon the degree of **trustworthiness** needed to adequately mitigate the risk;*
  - *Determining if the information systems are **worthy of being trusted** to operate within the agreed-upon levels of risk; and*
  - *Providing ongoing **monitoring and oversight** to ensure that the trust relationship is being maintained.*

Trust Relationships

Security Visibility Among Business/Mission Partners

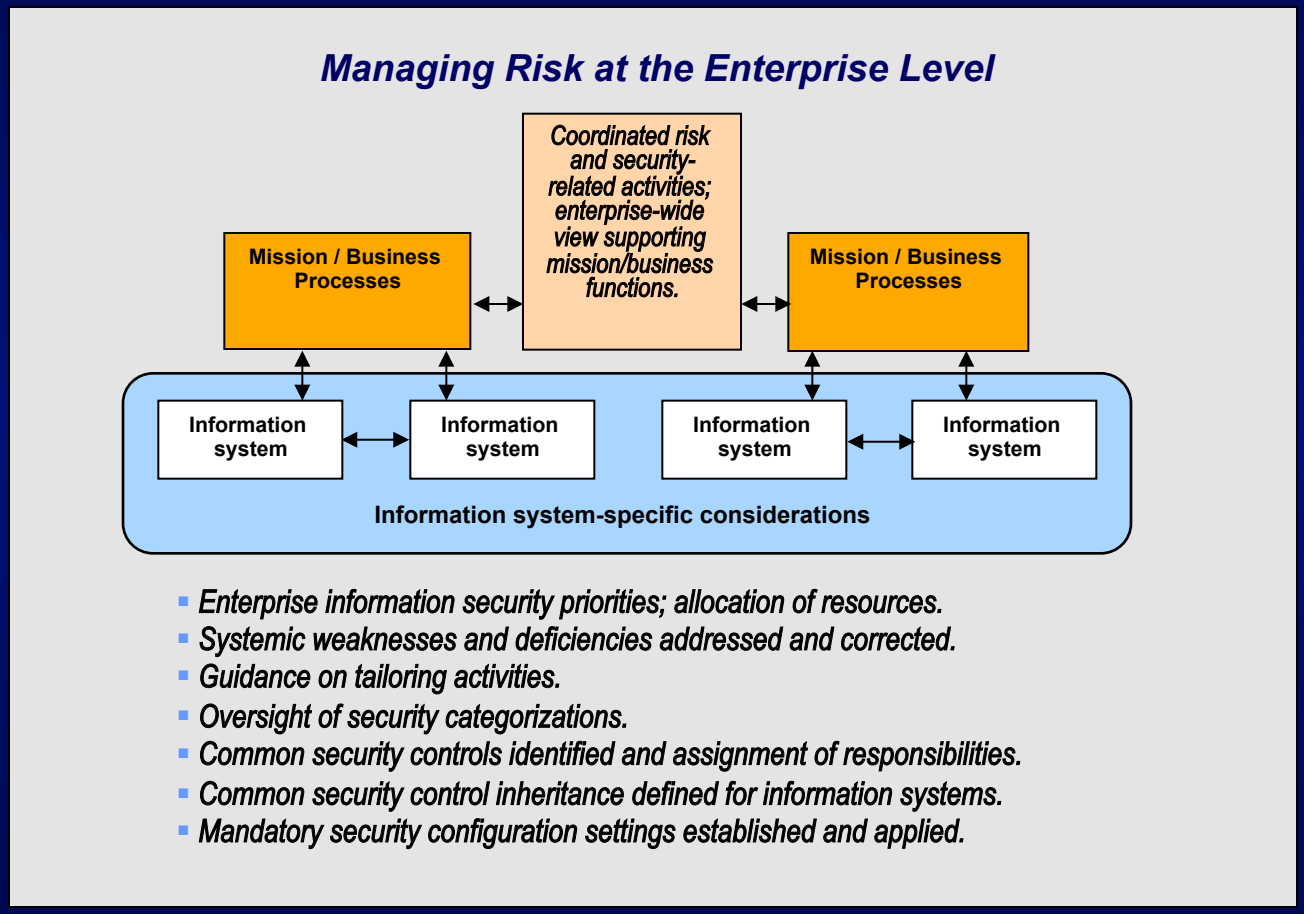


Determining risk to the enterprise's operations and assets, individuals, other organizations, and the nation; and the acceptability of such risk.

Determining risk to the enterprise's operations and assets, individuals, other organizations, and the nation; and the acceptability of such risk.

The objective is to achieve *visibility* into prospective business/mission partners information security programs…establishing a trust relationship based on the trustworthiness of information systems.

Risk Executive Function



Strategic Planning Considerations

Defense-in Breadth

- *Diversify information technology assets.*
- *Reduce information system complexity.*
- *Consider vulnerabilities of new information technologies before deployment.*
- *Apply a balanced set of management, operational, and technical security controls in a defense-in-depth approach.*

Strategic Planning Considerations

Defense-in Breadth

- *Detect and respond to breaches of information system boundaries.*
- *Reengineer business/mission processes.*

NIST's Industrial Control Systems (ICS) Project

Industrial Control Systems - ICS

- *What are ICS?*
  - *Supervisory Control and Data Acquisition (SCADA) Systems*
  - *Distributed Control Systems (DCS)*
  - *Programmable Logic Controllers (PLC)*
  - *Intelligent Field devices*
- *Used in all process control and manufacturing processes including electric, water, oil/gas, chemicals, auto manufacturing, etc*

Federal Agency Challenges (1 of 2)

- *Federal agencies required to apply NIST SP 800-53 Recommended Security Controls for Federal Information Systems (general IT security requirements) to their ICSs*
- *Federal agencies that own/operate electric power-related ICSs could potentially have to meet 2 standards (FIPS 200/NIST SP 800-53 and Federal Energy Regulatory Commission--FERC standards*)*

* *Most mature industry candidate is the NERC Critical Infrastructure Protection (CIP) standards*

Federal Agency Challenges (2 of 2)

- *Such agencies include:*
  - *Bonneville Power Administration (BPA)*
  - *Southwestern Power Administration (SWPA)*
  - *Western Area Power Administration (WAPA)*
  - *Tennessee Valley Administration (TVA)*
  - *DOI Bureau of Reclamation*
  - *Post Office*
  - *FAA*

CSD/ITL-ISD/MEL ICS Project (1 of 3)

- Cooperative relationship between the Computer Security Division (CSD) & Intelligent Systems Division (ISD) goes back about 6 years with start of the Process Control Security Requirements Forum (PCSRF--Stu Katzke & Al Wavering).
  - CSD: IT security expertise
  - ISD: ICS experience & ICS community recognition
- Federal agencies required to apply SP 800-53 to their ICSs
- Immediate (short term) focus on improving the security of ICSs that are part of the USG's critical infrastructure (CI).
- Longer term focus on fostering ***convergence*** of approaches/ standards in government & private sectors

ITL: Information Technology Laboratory

MEL: Manufacturing Engineering Laboratory

CSD/ITL-ISD/MEL ICS Project (2 of 3)

- "ICS" augmentation to SP 800-53, Revision 1
  - Develop bi-directional mappings of 800-53 to NERC CIPs *
  - Hold workshops (3) to
    - Explore the applicability of FIPS 199, FIPS 200, and NIST SP 800-53 to federally owned/operated ICSs.
    - Get U.S. Government (USG) stake holder's inputs/experience
    - Develop a comparison of SP 800-53 to the NERC CIPs
    - Develop the ICS version in cooperation with USG stakeholders
    - Validate the "ICS" version through implementation by USG stake holders and case studies (e.g., Bellingham Cyber Incident)
- NIST SP 800-82: A guidance document on how to secure ICSs

*In anticipation of possible Federal Energy Regulatory Commission's (FERC) adoption of the North American Electric Reliability Corporation 's (NERC) Critical Infrastructure Protection Standards (CIPs)

CSD/ITL-ISD/MEL ICS Project (3 of 3)

- *Assist/support FERC, DHS, and DOE/National Labs in their missions/roles to protect the government's energy/power critical infrastructure from intentional (e.g., cyber attacks) and unintentional events (e.g., natural disasters).*
- *Foster **convergence** of approaches/standards in all government & private sectors that use/depend on all ICSs.*

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

- *Generally, conforming to moderate baseline in SP 800-53 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 CIPs 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

Mapping Table Extract

			CIP-002				CIP-003						CIP-004				CIP-005						CIP-006						CIP-007								CIP-008		CIP-009				
LEGEND High baseline (no shading) Moderate baseline (12.5% grey shading) Low baseline (25% grey shading) Not in baseline (50% grey shading)			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											2,																			19													
Other - Notes						2	3	2	11	2	7	2							18			12							,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																																									

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

NIST Comments to FERC on FERC's Preliminary Assessment of the NERC CIPs

(Issued December 11, 2007; Docket RM06-22-000)
Filed by NIST on February 9, 2007

- *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 Comments to FERC (Cont.)

- *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).*

SP 800-53, Revision 2

- *Currently posted for public comment*
- *Does not change SP 800-53, Rev. 1*
- *Is an augmentation to Rev. 1*
  - *Appendix I replaced*
- *For ICS-related controls, recommends:*
  - *Scoping guidance*
  - *Compensating controls*
  - *Adds ICS supplemental guidance & ICS enhancements*

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*
- *Second public draft released September 2007*
- *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*

FY 2008 NIST Plans

- *Products/Deliverables*
  - *ICS augmentation of SP 800-53 (Revision 2)*
  - *SP 800-82: Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*
  - *Bellingham Cyber Incident case study (plus others)*
- *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*
- *Continue working with private sector ICS stakeholders, including standards committees*

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