

FISMA Implementation

The Strategy, Challenges, and Roadmap Ahead

September, 2006

Matthew Scholl

Computer Security Division

Information Technology Laboratory

Legislative and Policy Drivers

- Public Law 107-347 (Title III)
Federal Information Security Management Act of 2002
- Homeland Security Presidential Directive #7
Critical Infrastructure Identification, Prioritization, and Protection
- OMB Circular A-130 (Appendix III)
Security of Federal Automated Information Resources
- OMB Memorandum M-06-16
Protection of Sensitive Information

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

FISMA Challenges

- We are building a solid foundation of information security across the largest information technology infrastructure 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.

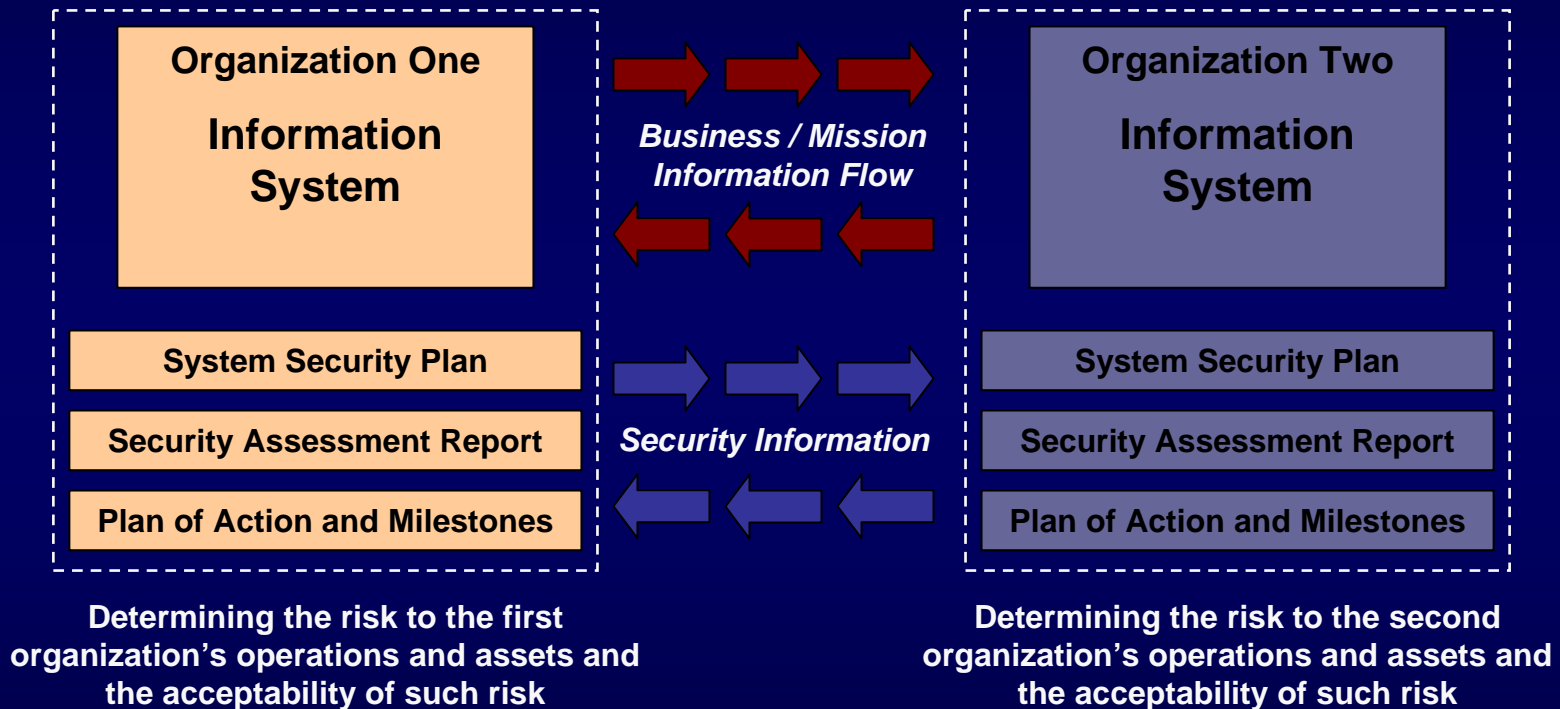
FISMA Challenges

Federal agencies are at various levels of maturity with respect to assimilating the new security standards and guidance; an extensive and important investment that will take time to fully implement.

- There is no consistency in the evaluation criteria used by auditors across the federal government when assessing the effectiveness of security controls in federal information systems; thus results vary widely.
- We (collectively) underestimate the complexity and the enormity of the task of building a higher level of security into the federal information technology infrastructure; expectations and measures of success vary.

The Desired End State

Security Visibility Among Business/Mission Partners



The objective is to achieve *visibility* into prospective business/mission partners information security programs **BEFORE** critical/sensitive communications begin...establishing levels of security due diligence and trust.

NIST Publications

Security Standards and Guidelines

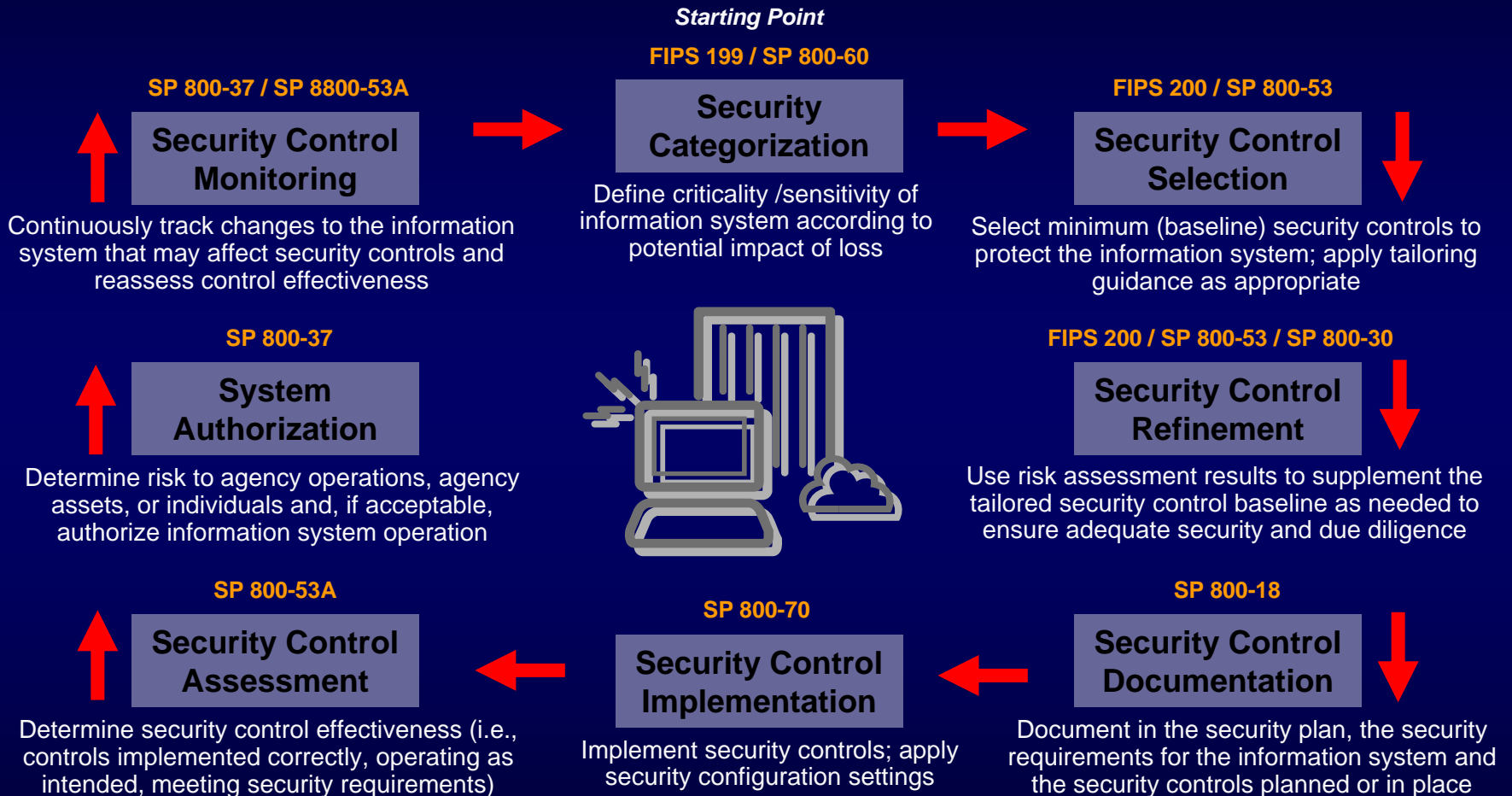
- **Federal Information Processing Standards (FIPS)**
 - Developed by NIST in accordance with FISMA.
 - Approved by the Secretary of Commerce.
 - Compulsory and binding for federal agencies; not waivable.
- **NIST Guidance (Special Publication 800-Series)**
 - OMB Memorandum M-05-15, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* states that for other than national security programs and systems, agencies must follow NIST guidance.
- **Other security-related publications**
 - NIST Interagency and Internal Reports and Information Technology Laboratory Bulletins provide technical information about NIST's activities.
 - Mandatory only when so specified by OMB.

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...

The Risk Framework



Compliance

NIST Standards and Guidelines

- While agencies are required to follow NIST *guidance* in accordance with OMB policy, there is flexibility in how agencies apply the guidance.
- Unless otherwise specified by OMB, the 800-series guidance documents published by NIST generally allow agencies some *latitude* in their application.
- Consequently, the application of NIST guidance by agencies can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the OMB definition of *adequate security* for federal information systems.

Security Categorization

Example: An Enterprise Information System

FIPS Publication 199	Low	Moderate	High
Confidentiality	The loss of confidentiality could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The loss of integrity could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability	The loss of availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Guidance for Mapping Types of Information and Information Systems to FIPS Publication 199 Security Categories



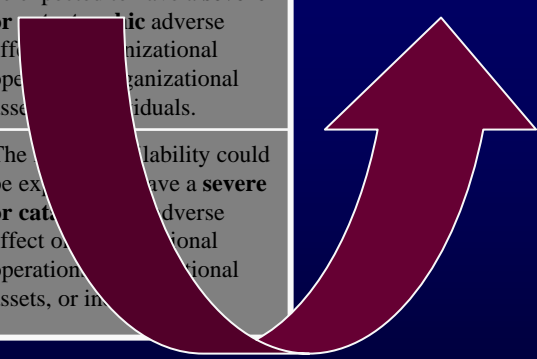
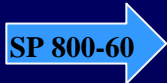
Security Categorization

Example: An Enterprise Information System

FIPS Publication 199	Low	Moderate	High
Confidentiality	The loss of confidentiality could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The loss of integrity could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability	The loss of availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Minimum Security Controls for High Impact Systems

Guidance for Mapping Types of Information and Information Systems to FIPS Publication 199 Security Categories

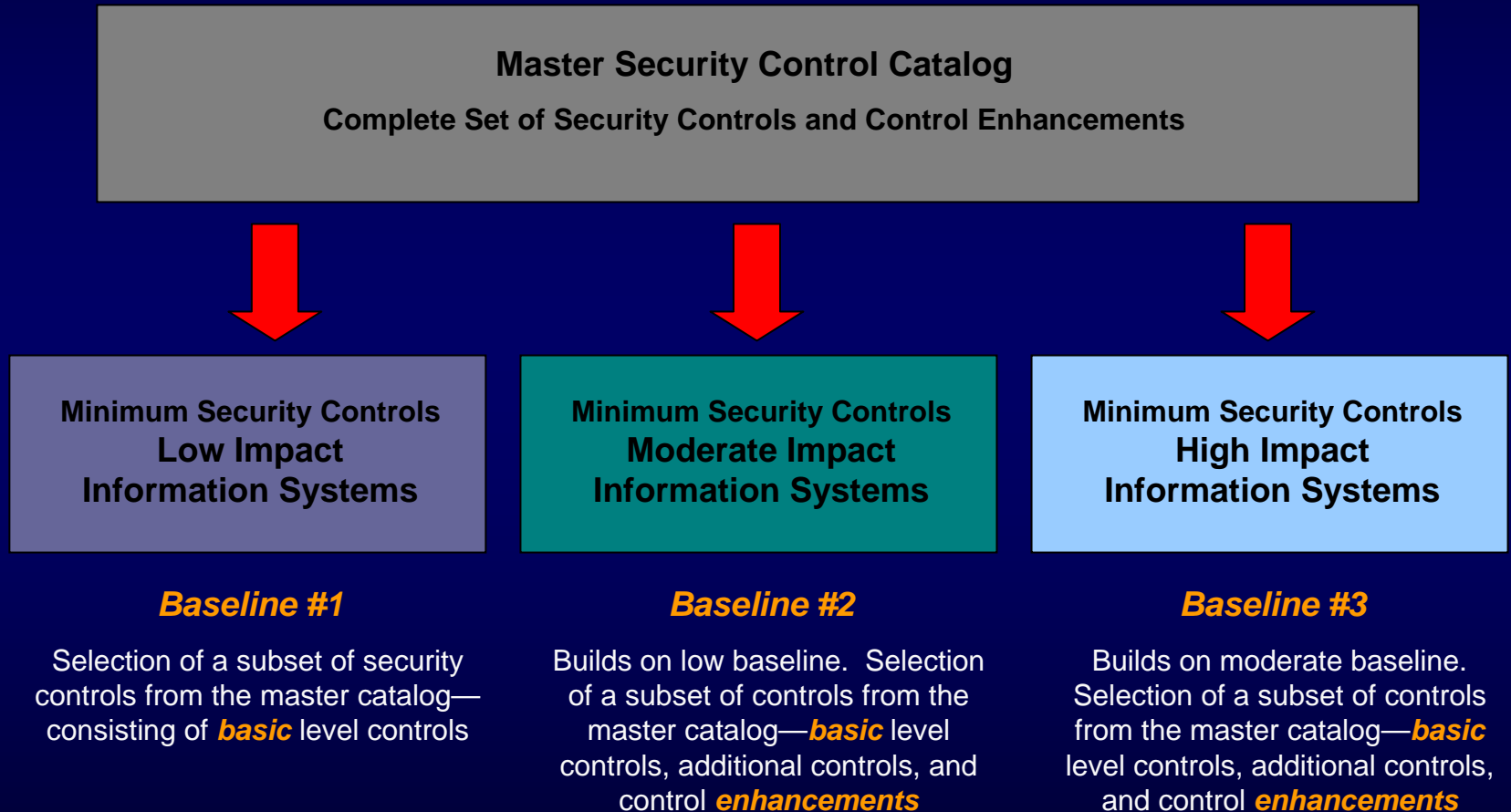


Minimum Security Requirements

FISMA Requirement

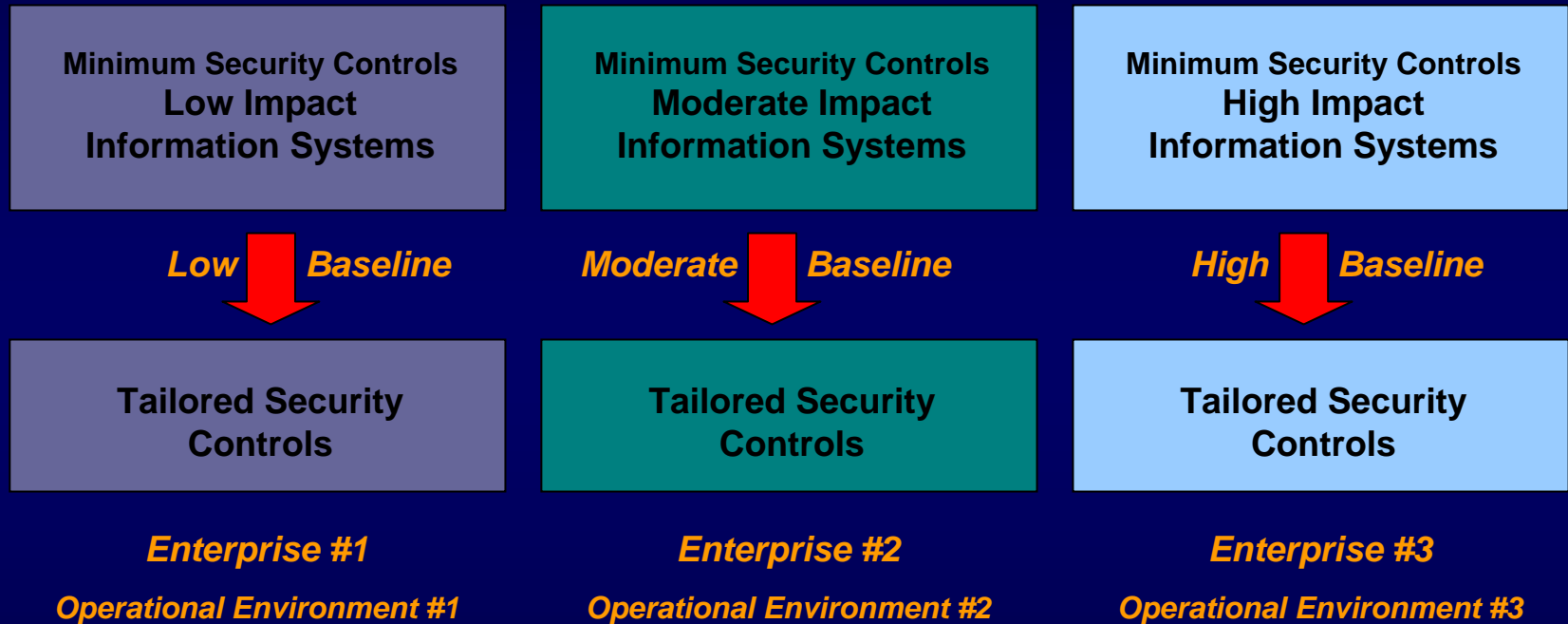
- Develop minimum information security requirements for information and information systems in each security category defined in FIPS 199
- Publication status:
 - ✓ Federal Information Processing Standards (FIPS) Publication 200, “Minimum Security Requirements for Federal Information and Information Systems”
 - ✓ Final Publication: **March 2006**

Security Control Baselines



Tailoring Security Controls

Scoping, Parameterization, and Compensating Controls



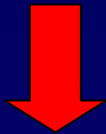
Cost effective, risk-based approach to achieving adequate information security...

Requirements Traceability

High Level Security Requirements

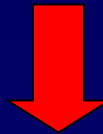
Derived from Legislation, Executive Orders, Policies, Directives, Regulations, Standards

Examples: HIPAA, Graham-Leach-Bliley, Sarbanes-Oxley, FISMA, OMB Circular A-130



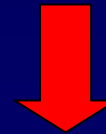
Security Controls
FIPS 200 / SP 800-53

Enterprise #1



Security Controls
FIPS 200 / SP 800-53

Enterprise #2



Security Controls
FIPS 200 / SP 800-53

Enterprise #3

What set of security controls, if implemented within an information system and determined to be effective, can show compliance to a particular set of security requirements?

New Initiatives

- Applying FISMA security standards and guidance to Industrial Control/SCADA Systems—
 - Completed two-day workshop at NIST involving major federal entities with Industrial Control/SCADA systems or having significant interest in those types of systems (e.g., Bonneville Power Administration, Tennessee Valley Authority, Western Area Power Administration, Federal Energy Regulatory Commission, Department of Interior Bureau of Land Management)
 - Analyzed the impact of applying the security controls in NIST SP 800-53 to Industrial Control/SCADA Systems; soliciting recommendations for additional security controls and/or developing control interpretations.