Revising NIST SP 800-53 to Include Industrial Control Systems (ICSs)
&
Status of NIST SP 800-82

Kema’s 6th Conference for Cyber Security of ICSs

August 8, 2006

Portland OR

Stu Katzke; Computer Security Division

and

Keith Stouffer; Intelligent Systems Division
National Institute of Standards and Technology

Presentation Contents

- NIST’s FISMA Implementation Project
  - The Risk Framework
  - FISMA Challenges and Compliance
  - Security categorization
  - Security requirements & controls
- CSD/ITL-ISD/MEL ICS Project

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

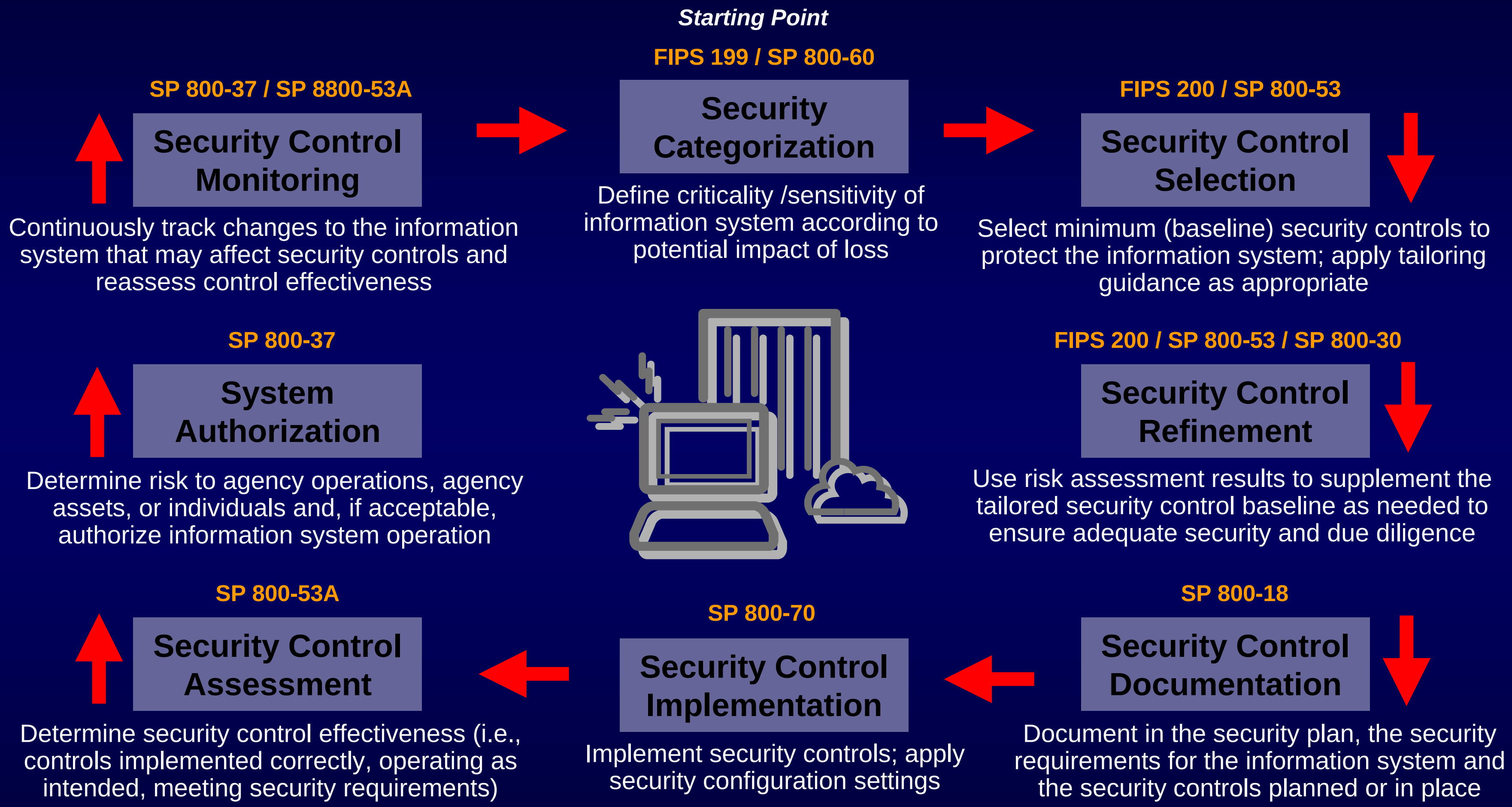
FISMA Requirements for NIST
(partial list)

- Standards for categorizing information and information systems…based on the objectives of providing appropriate levels of information security according to a range of risk levels
- Guidelines recommending the types of information and information systems to be included in each category
- Minimum information security requirements for information and information systems in each such category

Managing Enterprise Risk

- Key activities in managing enterprise-level risk—risk resulting from the operation of an information system:
  - ✓ **Categorize** the information system (criticality/sensitivity)
  - ✓ **Select** and tailor minimum (baseline) security controls
  - ✓ **Supplement** the security controls based on risk assessment
  - ✓ **Document** security controls in system security plan
  - ✓ **Implement** the security controls in the information system
  - ✓ **Assess** the security controls for effectiveness
  - ✓ **Determine** agency-level risk and risk acceptability
  - ✓ **Authorize** information system operation
  - ✓ **Monitor** security controls on a continuous basis

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

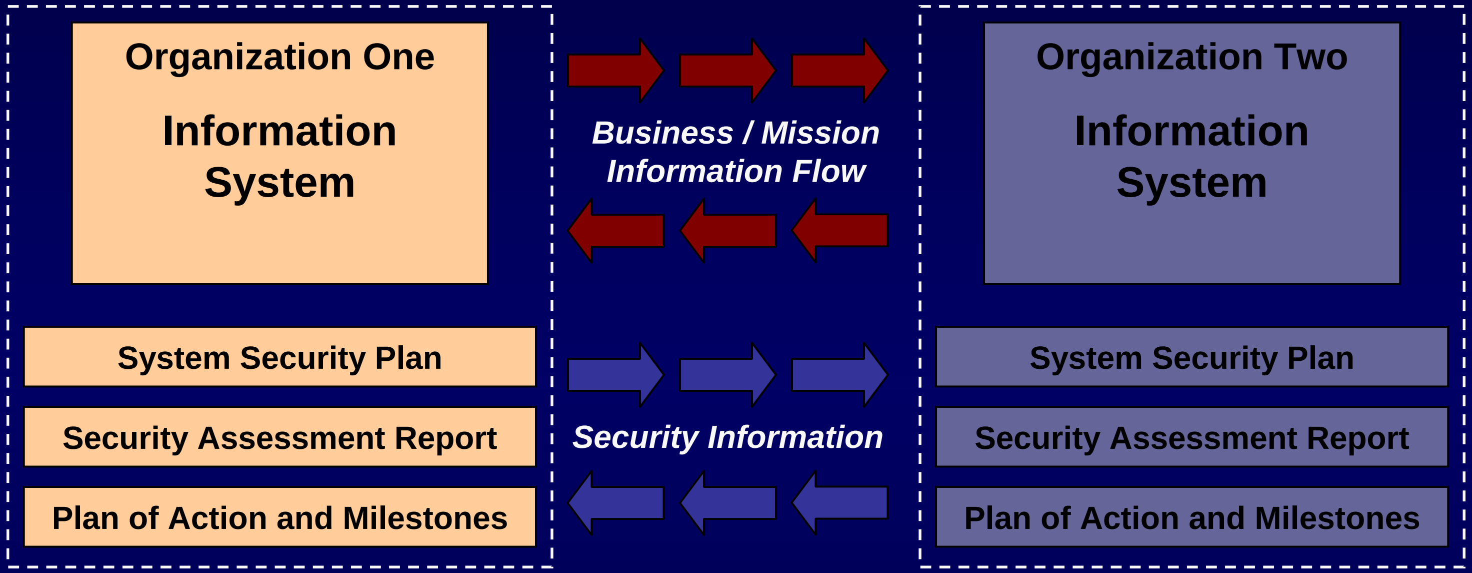
SP 800-37 / SP 8800-53A

Security Control Monitoring

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

The Desired End State

Security Visibility Among Business/Mission Partners



Organization One

Information System

System Security Plan

Security Assessment Report

Plan of Action and Milestones

Business / Mission Information Flow

Security Information

Organization Two

Information System

System Security Plan

Security Assessment Report

Plan of Action and Milestones

Determining the risk to the first organization’s operations and assets and the acceptability of such risk

Determining the risk to the second organization’s operations and assets and the acceptability of such risk

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.

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.

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 waiverable.
- 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…

Compliance Schedule

NIST Security Standards and Guidelines

- For legacy information systems, agencies are expected to be in compliance with NIST security standards and guidelines within one year of the publication date unless otherwise directed by OMB or NIST.*
- For information systems under development, agencies are expected to be in compliance with NIST security standards and guidelines immediately upon deployment of the system.

* The one-year compliance date for revisions to NIST Special Publications applies only to the new and/or updated material in the publications resulting from the periodic revision process. Agencies are expected to be in compliance with previous versions of NIST Special Publications within one year of the publication date of the previous versions.

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.

Compliance

NIST 800-Series Guidelines

- When assessing agency compliance with NIST guidance, auditors, evaluators, and/or assessors should consider:
  - The intent of the security concepts and principles articulated within the particular guidance document; and
  - How the agency applied the guidance in the context of its specific mission responsibilities, operational environments, and unique organizational conditions.

Categorization Standards

FISMA Requirement

- Develop standards to be used by federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels
- Publication status:
  - ✓ Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems"
  - ✓ Final Publication: February 2004

Security Categorization

Example: An Enterprise Information System

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

SP 800-60

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.

Security Categorization

Example: An Enterprise Information System

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

SP 800-60

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** [illegible]**ic** adverse eff[illegible]nizational ope[illegible]ganizational asse[illegible]iduals.
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 [illegible]lability could be ex[illegible]ave a **severe or cat**[illegible]dverse effect o[illegible]ional operation[illegible]tional assets, or in[illegible]

Minimum Security Controls for High Impact Systems

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

Minimum Security Controls

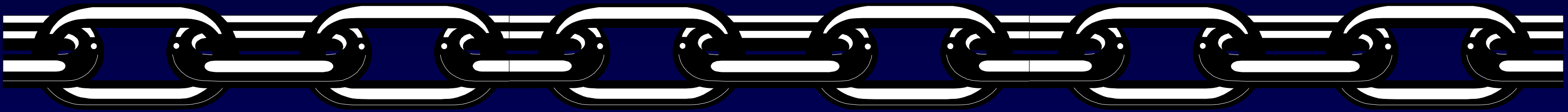
- Develop minimum security controls (management, operational, and technical) to meet the minimum security requirements in FIPS 200
- Publication status:
  - ✓ NIST Special Publication 800-53, “Recommended Security Controls for Federal Information Systems”
  - ✓ Final Publication: February 2005*

* SP 800-53, Revision 1(Second public draft) to be published in July 2006.

Security Control Structure

- Functional requirements
  - Master Security Control Catalogue
  - 17 Control Families
  - Functional requirements for each control in each family
- Assurance requirements
  - Dependent on the baseline the control is in
  - Includes: Low, Moderate, High, and Additional Assurance Requirements that Supplement the High Baseline

Information Security Program



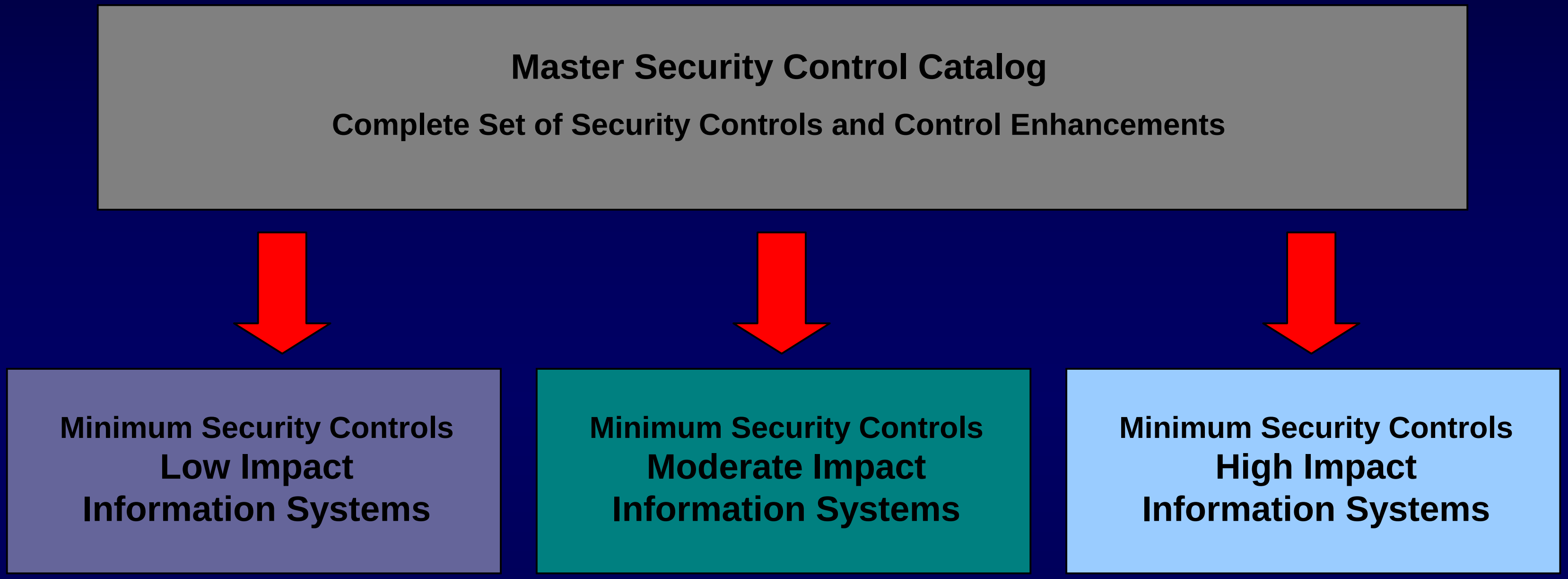
Links in the Security Chain: Management, Operational, and Technical Controls

- ✓ Risk assessment
- ✓ Security planning
- ✓ Security policies and procedures
- ✓ Contingency planning
- ✓ Incident response planning
- ✓ Security awareness and training
- ✓ Physical security
- ✓ Personnel security
- ✓ Certification, accreditation, and security assessments

- ✓ Access control mechanisms
- ✓ Identification & authentication mechanisms (Biometrics, tokens, passwords)
- ✓ Audit mechanisms
- ✓ Encryption mechanisms
- ✓ Firewalls and network security mechanisms
- ✓ Intrusion detection systems
- ✓ Security configuration settings
- ✓ Anti-viral software
- ✓ Smart cards

Adversaries attack the weakest link…where is yours?

Security Control Baselines



Master Security Control Catalog

Complete Set of Security Controls and Control Enhancements

Minimum Security Controls
Low Impact
Information Systems

Minimum Security Controls
Moderate Impact
Information Systems

Minimum Security Controls
High Impact
Information Systems

Baseline #1

Selection of a subset of security controls from the master catalog—consisting of ***basic*** level controls

Baseline #2

Builds on low baseline. Selection of a subset of controls from the master catalog—***basic*** level controls, additional controls, and control ***enhancements***

Baseline #3

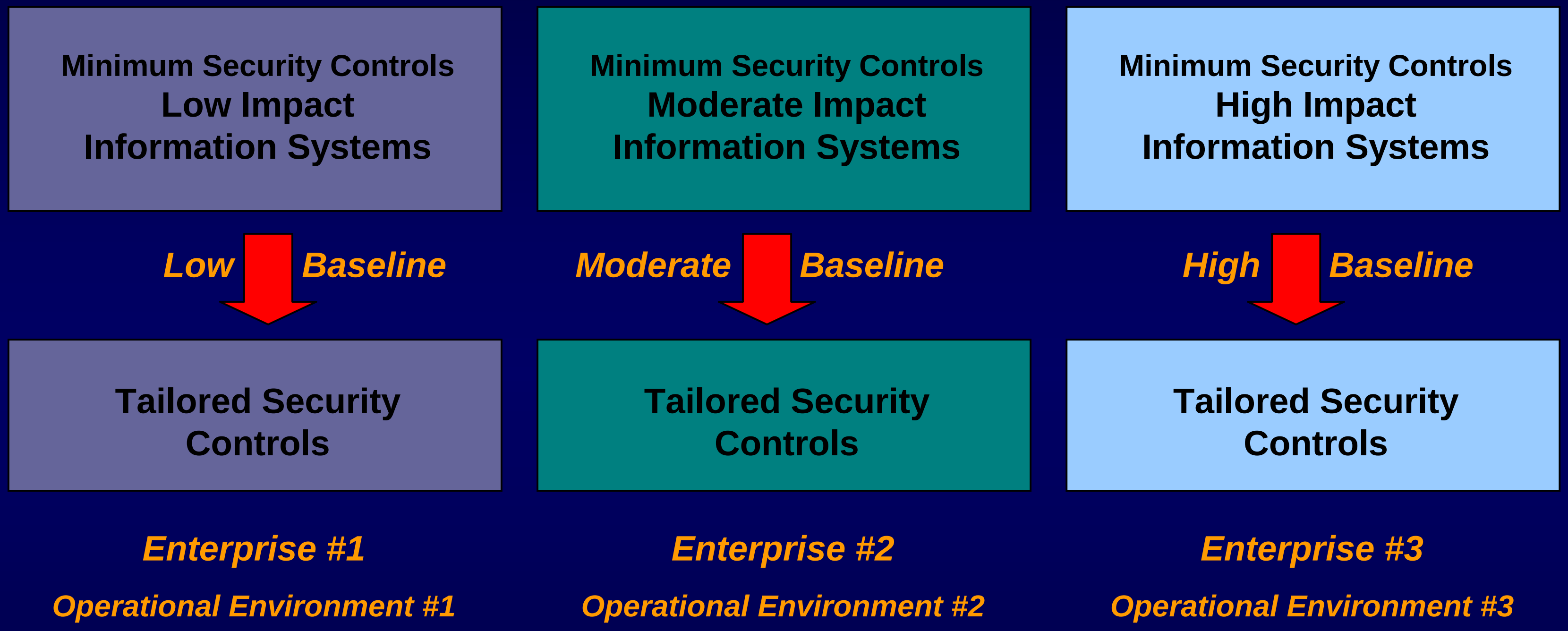
Builds on moderate baseline. Selection of a subset of controls from the master catalog—***basic*** level controls, additional controls, and control ***enhancements***

Minimum Security Controls

- Minimum security controls, or baseline controls, defined for low-impact, moderate-impact, and high-impact information systems—
    - Provide a ***starting point*** for organizations in their security control selection process
    - Are used in conjunction with ***tailoring guidance*** that allows the baseline controls to be adjusted for specific operational environments
    - Support the organization’s ***risk management process***

Tailoring Security Controls

Scoping, Parameterization, and Compensating Controls



Minimum Security Controls
Low Impact
Information Systems

Low *Baseline*

Tailored Security Controls

Enterprise #1

Operational Environment #1

Minimum Security Controls
Moderate Impact
Information Systems

Moderate *Baseline*

Tailored Security Controls

Enterprise #2

Operational Environment #2

Minimum Security Controls
High Impact
Information Systems

High *Baseline*

Tailored Security Controls

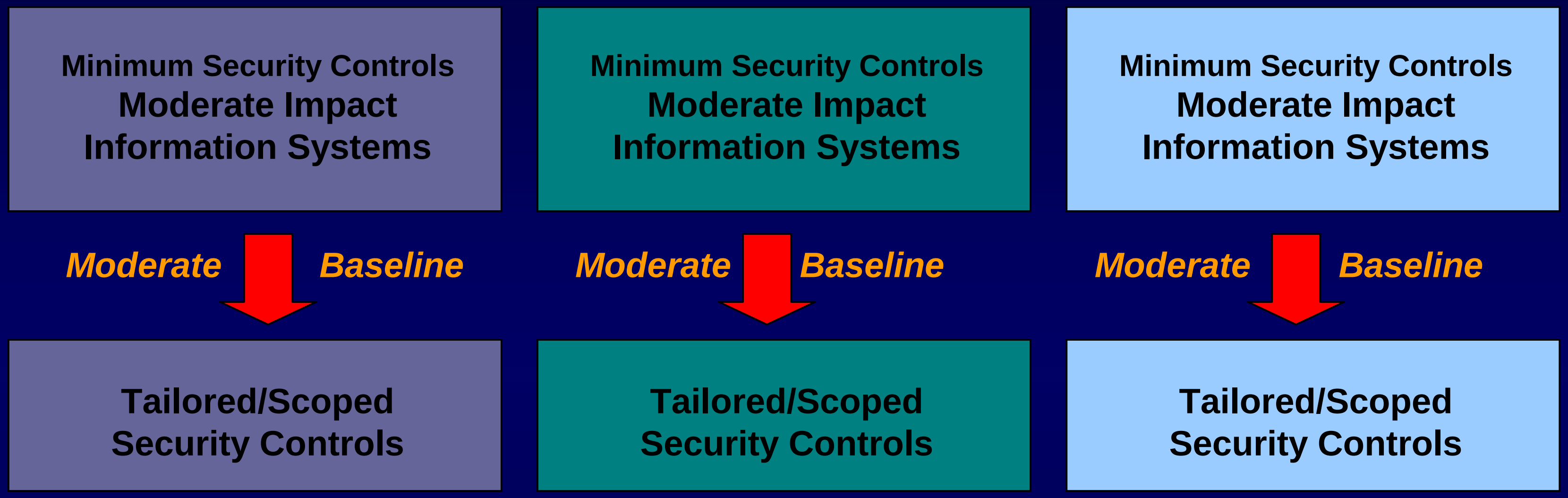
Enterprise #3

Operational Environment #3

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

Tailoring Security Controls

Application of Scoping Guidance



Minimum Security Controls
Moderate Impact
Information Systems

Moderate *Baseline*

Tailored/Scoped
Security Controls

Minimum Security Controls
Moderate Impact
Information Systems

Moderate *Baseline*

Tailored/Scoped
Security Controls

Minimum Security Controls
Moderate Impact
Information Systems

Moderate *Baseline*

Tailored/Scoped
Security Controls

Enterprise #1

Operational Environment #1

Enterprise #2

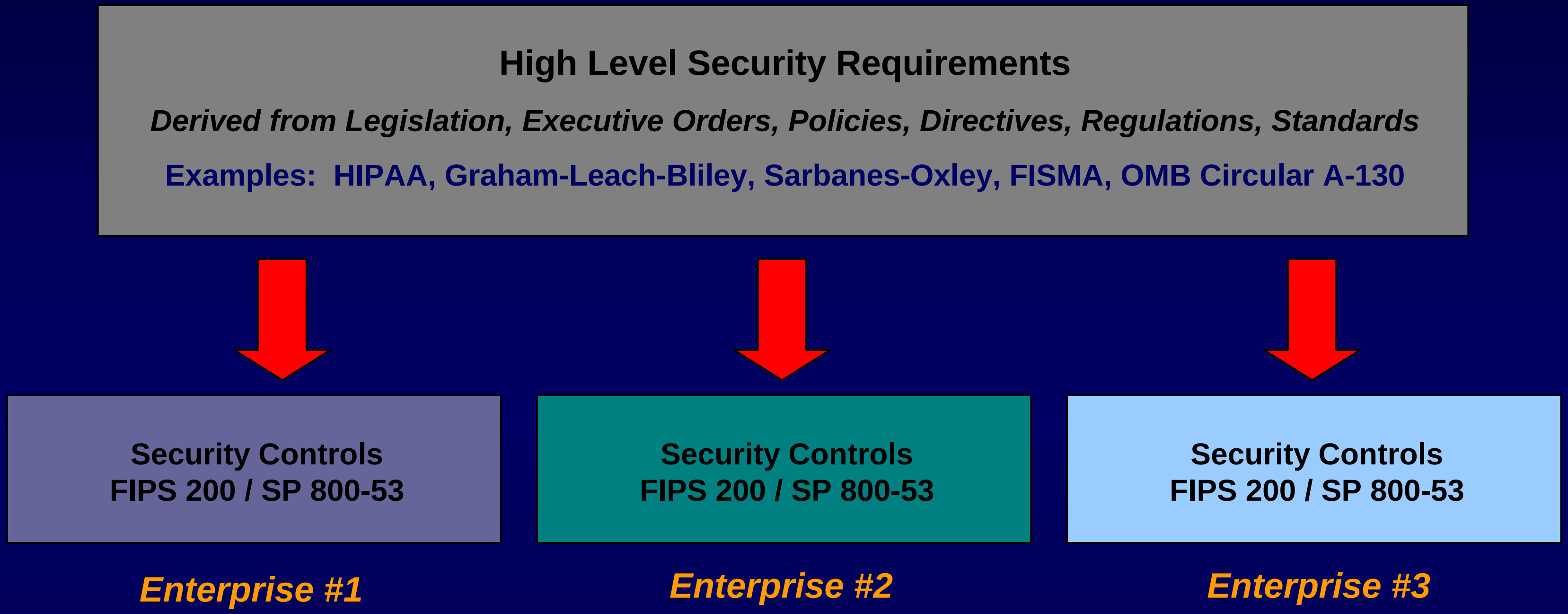
Operational Environment #2

Enterprise #3

Operational Environment #3

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?

CSD/ITL-ISD/MEL ICS Project

- Cooperative relationship between the CSD & ISD goes back about 5 years with start of the 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

CSD/ITL-ISD/MEL ICS Project

Deliverables (1)

- “ICS” version of SP 800-53
  - Develop bi-directional mappings of 800-53 to NERC CIPs
  - Hold workshop to
    - Get U.S. Government (USG) stake holder's inputs/experience
    - Develop the ICS version in cooperation with USG stake holders
  - Validate the “ICS” version through implementation by USG stake holders
- NIST SP 800-82: A guidance document on how to secure ICSs

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 and/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

Audience

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

Overview of Industrial Control Systems (ICS)

- Provides an overview of SCADA and industrial control systems
- Control Systems vs. Typical IT Systems
- Control System Components and Connectivity
- SCADA Systems
- DCS
- PLCs
- Industrial Sectors and Their Interdependencies

Industrial Control Systems Vulnerabilities and Threats

- Risk Factors
- Potential SCADA and industrial control systems vulnerabilities
- Threats
- Incidents
  - Direct
  - Indirect
  - Incidental

Industrial Control Systems Security Deployment

- Business case for security
- Developing a comprehensive security program

Network Architecture

- Firewalls
- Network Segmentation
- Redundancy and Fault Tolerance

ICS in the Federal Information Security Management Act (FISMA) Paradigm

- Security Categorization
- Security Control Selection
- Security Control Refinement
- Security Control Assessment
- Interim Guidance on the Application of Security Controls to ICS

Management Controls

- Risk Assessment
- Developing and Implementing a Security Program
- System and Services Acquisition
- Security Assessments

Operational Controls

- Personnel Security
- Patch Management
- Configuration Management
- Checklists
- Network Segmentation
- Incident Response
- Disaster Recovery Planning
- Physical Protection

Technical Controls

- User Identification, Authentication and Authorization
- Data Identification and Authentication
- Device Identification, Authentication and Authorization
- Logging
- Audit
- Secure Communications
- Access Control
- Intrusion Detection and Prevention
- Virus, Worm and Malicious Code Detection

Appendices

- Acronyms and Abbreviations
- Glossary of Terms
- Current Activities in SCADA/Industrial Control System Security
- Emerging Capabilities
- References
- Case Study (not in initial public draft)

CSD/ITL-ISD/MEL ICS Project

Deliverables (2)

- 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 government organizations that use/depend on ICSs.

Federal

- NIST SP800-53 Security control mapping and gap analysis with NERC CIP standard to discover and propose modifications to remove any conflicts
- Coordination
  - FERC
  - DHS NCSD and S&T

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

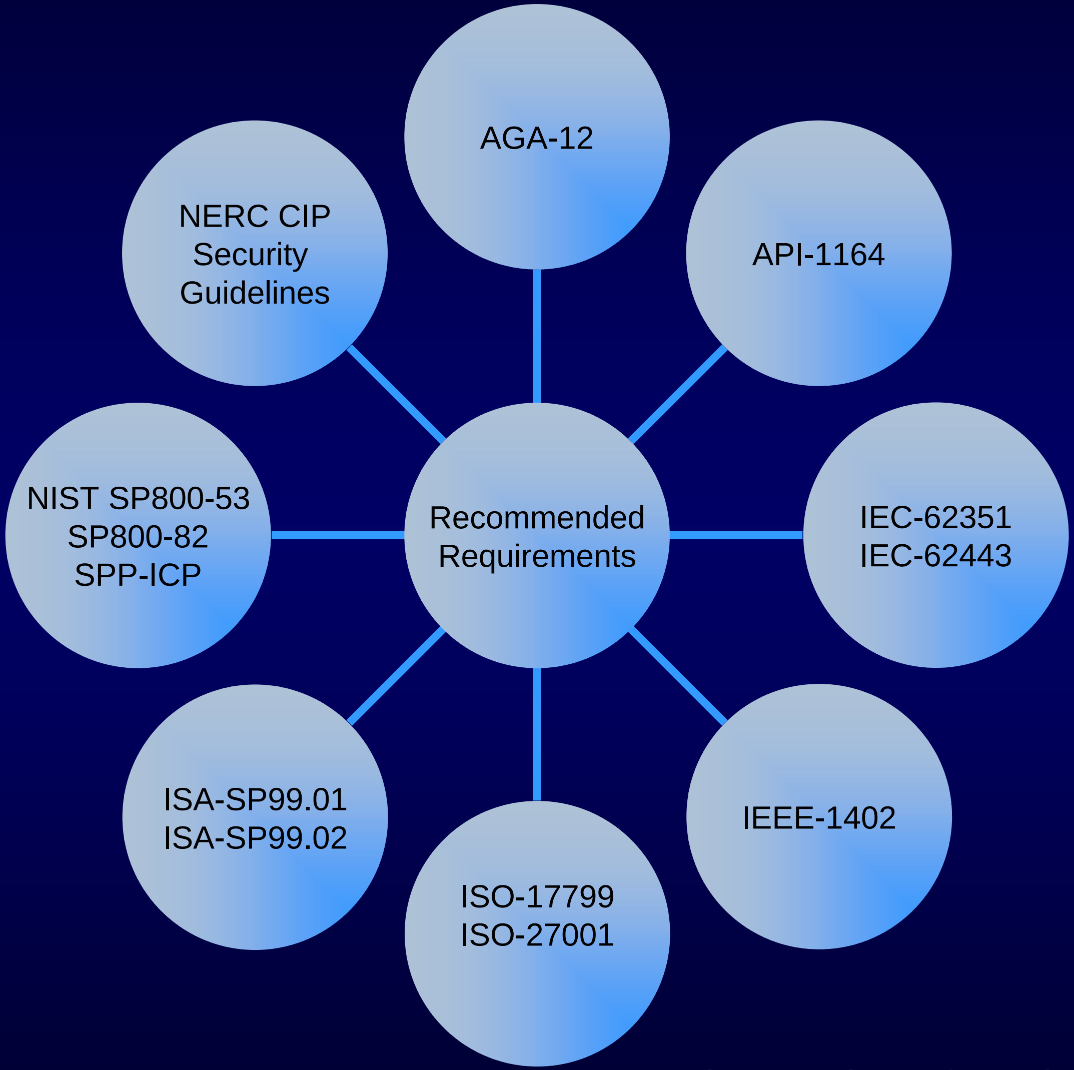
- Develop/agree on ***convergence*** strategy/goals with respect to other government and private sector activities in this area (e.g., NERC’s CIP standards, ISA standard 99, IEC-65C standard IEC 62443, FERC specifications, the January 2006 DOE *Road Map to Secure Control systems in the Energy Sector*).
- Implement the strategy to harmonize requirements across Federal sector and private sector to the degree possible and practical.

Recommended Requirements Document

- A baseline recommended cyber security requirements document is being drafted by the 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



Recommended Requirements

AGA-12

API-1164

IEC-62351
IEC-62443

IEEE-1402

ISO-17799
ISO-27001

ISA-SP99.01
ISA-SP99.02

NIST SP800-53
SP800-82
SPP-ICP

NERC CIP
Security
Guidelines

Requirements Format

The format of the requirements are based on the requirements structure used in NIST SP800-53:

- **Recommended Requirement**
  - Statement of the requirement and area addressed
- **Supplemental Guidance**
  - Additional guidance on how the requirement might be implemented, other possible interpretations, etc.
- **Requirement Enhancements**
  - Guidance to enhance the requirements based on criticality scale

Requirements Format Example

4.13.4 Contact with Control System Security Groups and Associations

Recommended Requirement

The organization should establish, participate, and maintain contacts with control system interest groups, industry vendor forums, specialized forums, or professional associations to stay up to date with the latest recommended security practices, techniques, and technologies.

Supplemental Guidance

It is in the best interest of the organization to establish contacts with industry and professional forums to stay abreast of new technologies, techniques, security issues, and mitigation solutions. The organization should join and actively participate in the development of standards, best practices, and operating procedures for securing the control system.

Requirement Enhancements

None.

PCSF Security Requirements Interest Group

- Newly formed Security Requirements Interest Group will focus on the harmonization of security requirements for control systems. It is hoped that this interest group will be the central resource to discuss the creation of a baseline set of security requirements that can be used by all sectors in the development of control system cyber security standards, recommended practices, etc.

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

Private Sector Acceptance

- **Standards for the ICS industry, if widely implemented, will raise the level of control systems security**
- **Greatest chance for industry acceptance and adoption publish security requirements 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**

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 a reference/starting document

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 baseline set of requirements that can be used by all sectors in the development of control system cyber security standards.
  - Draft is in progress

- **PCSF Security Requirements Interest Group**

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

  - Vehicle to discuss harmonization of requirements

FISMA Implementation Project 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

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

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

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

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