NIST Workshop on Applying NIST Special Publication 800-53, Revision 1: *Recommended Security Controls for Federal Information systems,* to Industrial Control Systems.

August 16 (1-5 PM) & August 17 (9-Noon), 2007

Marriott Knoxville Hotel

Knoxville, TN

Purpose of this workshop

- Introduce NIST's:
  - Risk Management Framework (RMF) & supporting IT security standards & guidelines (S&Gs) for information systems, including extensions for industrial control systems (ICS)
  - ICS program
- The IT RMF & S&Gs are forming the foundation for security "due diligence" throughout federal government
- Explore how to foster convergence among the various ICS communities to a common security foundation (i.e., baseline security controls)
- How can NIST's ICS-related S&Gs be best used by the private sector?

Introduction to NIST's Risk Management Framework (RMF) and Related Standards and Guidelines

August 16, 2007

Dr. Stuart Katzke

Senior Research Scientist

Computer Security Division
Information Technology Laboratory

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 Tasks for NIST

- 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
- Guidelines recommending the types of information and information systems to be included in each category
- Minimum information security requirements (management, operational, and technical security controls) for information and information systems in each such category

FISMA 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 (RMF) 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.

RMF is a Process Applied to an Information System

- 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."

Information Security Strategy

- Successful FISMA implementation demands that organizations adopt an ***enterprise-wide*** security strategy.
- Metrics of a successful implementation:
  - Cost-effective
  - Consistent
  - Comprehensive
  - Effective

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

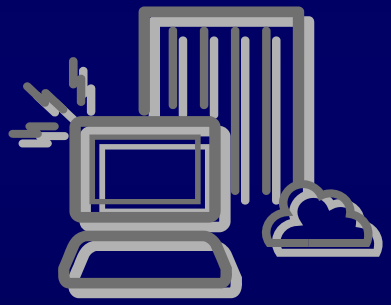
Authorize
Information System

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



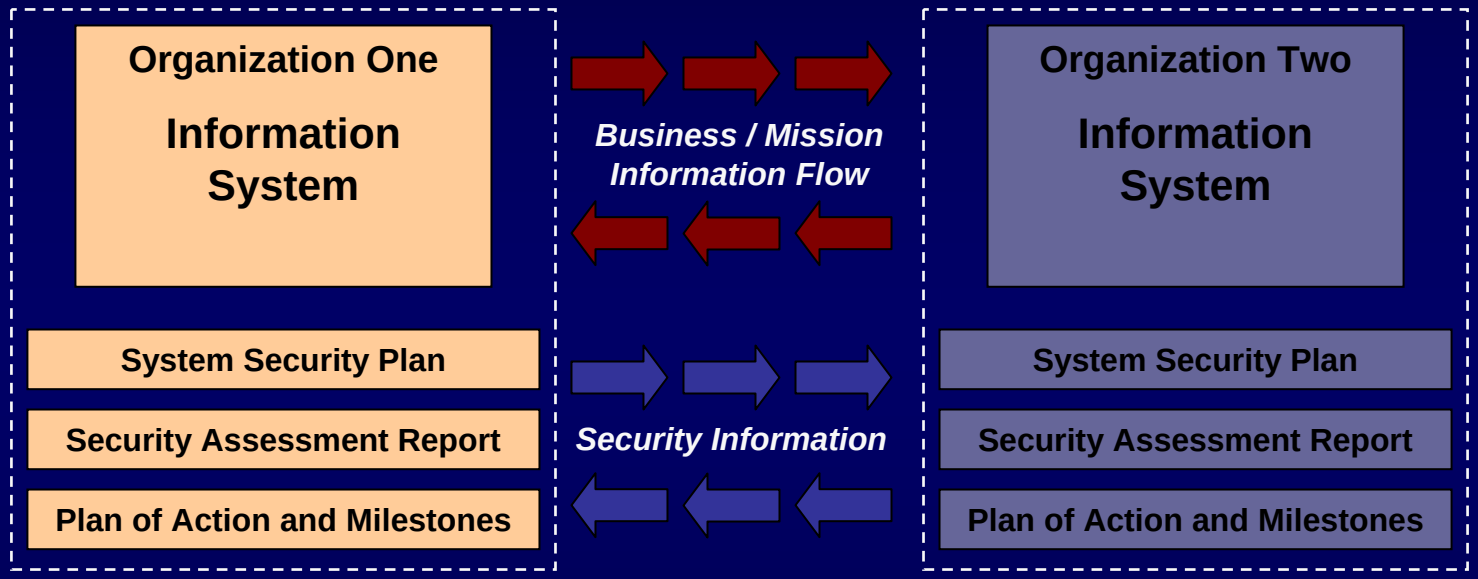
Key Standards and Guidelines

- 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 Desired End State

Security Visibility Among Business/Mission Partners



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.

Characteristics of the RMF (1)

- Security Categorization
  - Based on worst case impact analysis
  - Determines level of effort
  - Determines protection priorities
- Generic
  - Not government centric; applies to all organizations (IEEE P 1700)
  - Plug and play components to meet needs of different sectors (ICS, healthcare, financial)
- Superset of existing control sets

Characteristics of the RMF (2)

- Minimum/ baseline controls for Low, Moderate, & High impact systems were selected from master control catalogue
  - Hierarchical
  - Increase in functionality
- Assurance requirements
  - Baseline dependent: one for each baseline
  - Increase control developer/implementer's analysis and evidence to demonstrate implementation quality, correctness, and confidence

Characteristics of the RMF (3)

- Assurance requirements are related to and support control assessment approach
- Possibility of becoming “due diligence” in commercial and other sectors through:
  - Government critical infrastructure liaisons to private sector counterparts (e.g., energy, financial, transportation)
  - Extension of government security standards and requirements to systems operated on behalf of the federal government (State, Local, Contractors)

Characteristics of the RMF (4)

- Cost effective and flexible (See August 2007 edition of IEEE Computer)
  - Tailoring of minimum baselines
  - Common security controls concept
    - Agency-wide (e.g., training, personal security)
    - Site-wide (e.g., physical security, contingency plan)
    - Common subsystem (e.g., deployed at multiple sites)
  - Self assessments for Low impact systems

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

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

- Preliminary discussions are being held with various stakeholders 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

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

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

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

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

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

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

Information and Feedback
Web: csrc.nist.gov/sec-cert
Comments: sec-cert@nist.gov

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