FISMA Implementation Project Phase II

WORKSHOP ON CREDENTIALING PROGRAM FOR SECURITY ASSESSMENT SERVICE PROVIDERS

April 26, 2006

Workshop Objective

- Provide FISMA Implementation Project Phase I overview and status
- Present FISMA Implementation Project Phase II Vision, Strategy and Models
- Discuss capability requirements, evaluation criteria, training requirements, and Federal Agency responsibilities
- Receive input from attendees

The FISMA Implementation Project

A Status Report on Past, Present, and Future Activities

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

FISMA Implementation Project

- Initiated in January 2003 to respond to the Federal Information Security Management Act of 2002
- NIST tasked with developing the implementing security standards and guidance necessary for federal agencies and contractors to demonstrate compliance to the legislation
- Three-phased approach employed in a multi-year effort to accomplish the goals and objectives established by the legislation

FISMA Implementation Project

- Phase I: Development of FISMA-related security standards and guidelines
  Status: Completed by the end of 2006
- Phase II: Development of credentialing program for security assessment service providers
  Status: Started in 2006; estimated completion in 2008
- Phase III: Development of validation program for information security tools
  Status: Projected start 2007-08

The Legislation

Public Law 107-347, Title III

"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

Why FISMA?

The Global Threat…

- Information security is not just a paperwork drill…there are dangerous adversaries out there capable of launching serious attacks on our information systems that can result in severe or catastrophic damage to the nation's critical information infrastructure and ultimately threaten our economic and national security…

U.S. Critical Infrastructures

Definition

- "...systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters."

-- USA Patriot Act (P.L. 107-56)

U.S. Critical Infrastructures

Examples

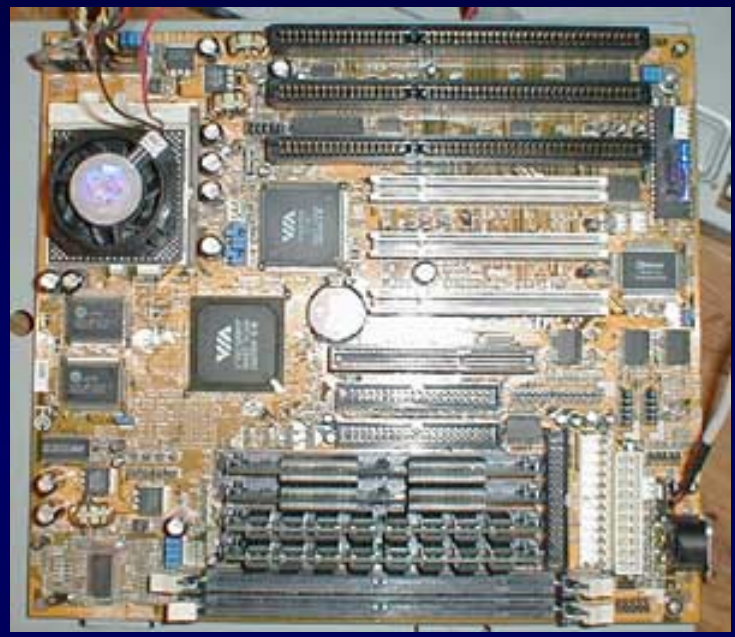
- Energy (electrical, nuclear, gas and oil, dams)
- Transportation (air, road, rail, port, waterways)
- Public Health Systems / Emergency Services
- Information and Telecommunications
- National Defense
- Banking and Finance
- Postal and Shipping
- Agriculture / Food / Water
- Chemical

Critical Infrastructure Protection

- The U.S. critical infrastructures are over 90% owned and operated by the private sector
- Critical infrastructure protection must be a partnership between the public and private sectors
- Information security solutions must be broad-based, consensus-driven, and address the ongoing needs of government and industry

Threats to Security

Connectivity



Complexity

What We Have Accomplished

- Developed two major security standards—
  - ✓ Federal Information Processing Standard FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*
  - ✓ Federal Information Processing Standard FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*

Federal Information Processing Standards are mandatory and non-waiverable under the provisions of FISMA.

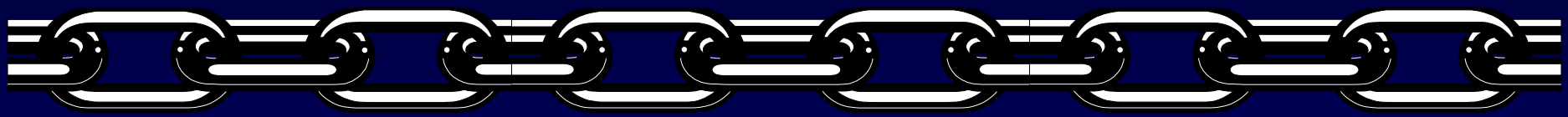
What We Have Accomplished

- Developed five security guidance documents—
  - ✓ **NIST Special Publication 800-37**, *Guide for the Security Certification and Accreditation of Federal Information Systems*
  - ✓ **NIST Special Publication 800-53**, *Recommended Security Controls for Federal Information Systems*
  - ✓ **NIST Special Publication 800-53A**, *Guide for Assessing the Security Controls in Federal Information Systems*
  - ✓ **NIST Special Publication 800-59**, *Guideline for Identifying an Information System as a National Security System*
  - ✓ **NIST Special Publication 800-60**, *Guide for Mapping Types of Information and Information Systems to Security Categories*

What We Have Accomplished

- Developed an Enterprise Risk Framework that—
  - ✓ Facilitates the development of comprehensive information security programs for federal agencies
  - ✓ Employs a security life cycle approach that can be integrated directly into the System Development Life Cycle for federal information systems
  - ✓ Integrates NIST Federal Information Processing Standards and Special Publications to maximize their effectiveness and utility for federal agencies
  - ✓ Provides a cost-effective approach to managing risk to enterprise operations and assets

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?

Managing Enterprise Risk

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

Information Security Life Cycle

The Risk Framework

Starting Point

FIPS 199 / SP 800-60

Security Categorization

Defines category of information system according to potential impact of loss

FIPS 200 / SP 800-53

Security Control Selection

Selects minimum security controls (i.e., safeguards and countermeasures) planned or in place to protect the information system

SP 800-37

Security Control Monitoring

Continuously tracks changes to the information system that may affect security controls and assesses control effectiveness

SP 800-53 / FIPS 200 / SP 800-30

Security Control Refinement

Uses risk assessment to adjust minimum control set based on local conditions, required threat coverage, and specific agency requirements

SP 800-37

System Authorization

Determines risk to agency operations, agency assets, or individuals and, if acceptable, authorizes information system processing

SP 800-18

Security Control Documentation

In system security plan, provides a an overview of the security requirements for the information system and documents the security controls planned or in place

SP 800-70

Security Control Implementation

Implements security controls in new or legacy information systems; implements security configuration checklists

SP 800-53A / SP 800-26 / SP 800-37

Security Control Assessment

Determines extent to which the security controls are implemented correctly, operating as intended, and producing desired outcome with respect to meeting security requirements

FISMA Implementation

Why is FISMA so challenging to implement?

- We are building a solid foundation of information security across the largest information technology infrastructure in the world based on comprehensive security standards.
- We are establishing a fundamental level of “security due diligence” for federal agencies and their contractors based on minimum security requirements and security controls.
- 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.

FISMA Implementation

Why is FISMA so challenging to 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.

FISMA Implementation Tips

Key strategies for successful implementation—

- Conduct FIPS 199 ***impact analyses*** as a corporate-wide exercise with the participation of key officials (e.g., Chief Information Officer, Senior Agency Information Security Officer, Authorizing Officials, System Owners).

  Rationale: The agency is heavily dependent upon its information systems and information technology infrastructure to successfully conduct critical missions. Therefore, the protection of those critical missions is of the highest priority. An incorrect information system impact analysis (i.e., incorrect FIPS 199 security categorization) results in the agency either over protecting the information system and wasting valuable security resources or under protecting the information system and placing important operations and assets at risk.

FISMA Implementation Tips

Key strategies for successful implementation—

- For each security control baseline (low, moderate, or high) identified in NIST Special Publication 800-53, apply the ***tailoring guidance*** to adjust set of controls to meet the specific operational requirements of the agency.

  Rationale: Application of the tailoring guidance in Special Publication 800-53 can eliminate unnecessary security controls, incorporate compensating controls when needed, specify agency-specific parameters in the controls, and add controls when greater mission-protection is required. Tailoring is an essential activity to ensure the final, agreed upon set of security controls for the information system provides adequate security. Tailoring activities and associated tailoring decisions should be well documented with appropriate justifications and rationale capable of providing reasoned arguments to auditors.

FISMA Implementation Tips

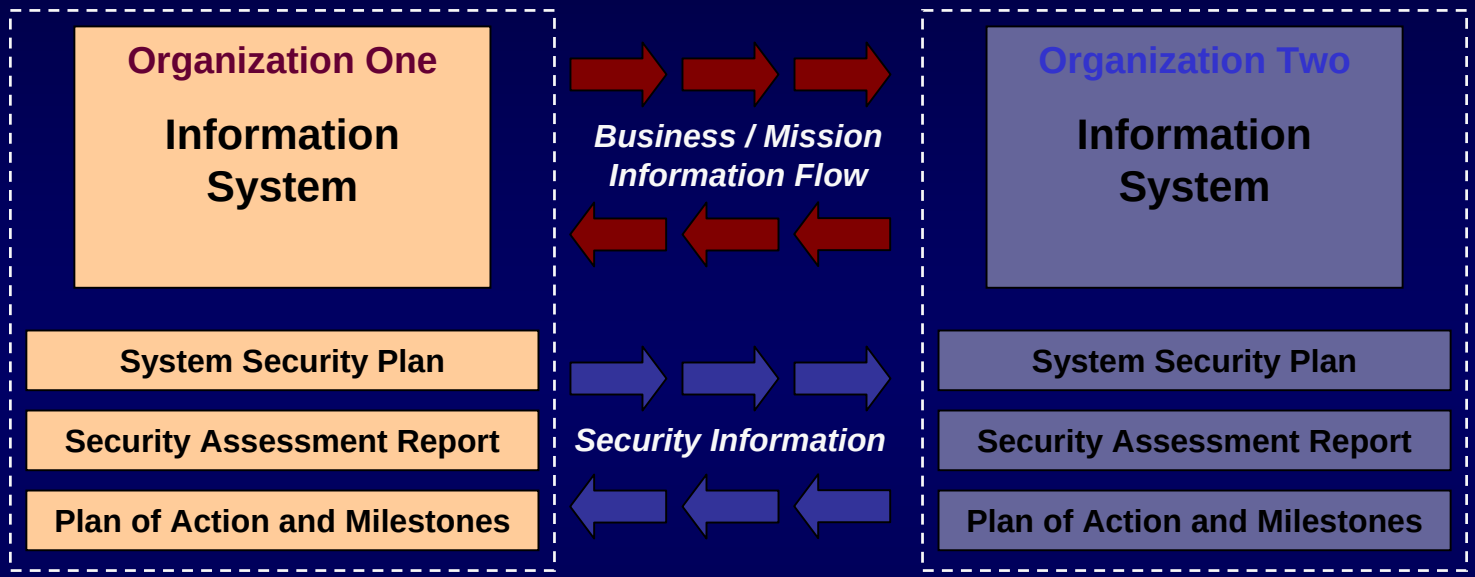
Key strategies for successful implementation—

- Conduct the selection of ***common security controls*** (i.e., agency infrastructure-related controls or controls for common hardware/software platforms) as a corporate-wide exercise with the participation of key officials (e.g., Chief Information Officer, Senior Agency Information Security Officer, Authorizing Officials, System Owners).

  Rationale: The careful selection of common security controls can save the agency significant resources and facilitate a more consistent application of security controls enterprise-wide. Agency officials must assign responsibility for the development, implementation, and assessment of the common controls and ensure that the resulting information is available to all interested parties.

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.

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.

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

Curt Barker
(301) 975-4768
wbarker@nist.gov

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

FISMA Implementation Project Phase II

Credentialing Program: Vision, Strategy and Models

Arnold Johnson

Computer Security Division
Information Technology Laboratory

Overview

- The Workshop Landscape
- FISMA Project Phase II Credentialing Program
- Program Goals and Objectives
- Program Implementation
- Credentialing Models

Principal Workshop Participants

- Federal Agencies (Consumers)
- Security Assessment Service Providers
- Credentialing Authorities and Proficiency Testing Organizations

Community Landscape

Made Simple

A + C = (C + A) = C & A

Terminology

Cross Word, Cross Community, Communication Challenge

- Accreditation / Certification (A + C) [organization / people]
  - Validating organization or persons capability/competence
  - Attesting to the capability/competence of organization or people
- Control Assessment (C + A) [information system]
  - Evaluate [Interview, Examine,Test] information system security controls
- Certification / Accreditation (C & A) [information system]
  - Confirm security controls correct, operating and meet requirements
  - Approval to operate an information system
- Credentialing [FISMA Implementation Project Phase II term]
  - **THE FOCUS OF THIS WORSHOP**

Managing Enterprise Risk

Credentialing Program Technical Landscape

Starting Point

FIPS 199 / SP 800-60

Security Categorization

Defines category of information system according to potential impact of loss

FIPS 200 / SP 800-53

Security Control Selection

Selects minimum security controls (i.e., safeguards and countermeasures) planned or in place to protect the information system

SP 800-37

Security Control Monitoring

Continuously tracks changes to the information system that may affect security controls and assesses control effectiveness

SP 800-53 / FIPS 200 / SP 800-30

Security Control Refinement

Uses risk assessment to adjust minimum control set based on local conditions, required threat coverage, and specific agency requirements

SP 800-37

System Authorization

Determines risk to agency operations, agency assets, or individuals and, if acceptable, authorizes information system processing

SP 800-18

Security Control Documentation

In system security plan, provides a an overview of the security requirements for the information system and documents the security controls planned or in place

SP 800-70

Security Control Implementation

Implements security controls in new or legacy information systems; implements security configuration checklists

SP 800-53A / SP 800-26 / SP 800-37

Security Control Assessment

Determines extent to which the security controls are implemented correctly, operating as intended, and producing desired outcome with respect to meeting security requirements

FISMA Phase II Credentialing Program

- Establish capability requirements for security assessment providers
- Define training needs and Federal agency responsibilities to support effective security assessments
- Establish process for evaluating and confirming capability/competence of security assessment providers
- For conducting assessments of information system security controls
- Consistent with NIST standards and guidelines in support of FISMA

FISMA Phase II
Program Goals and Objectives

- Provide federal agencies with basic set of requirements for acquiring security assessment services
- Provide security assessment providers with basic set of requirements to enable development of corporate strategies to cost-effectively respond to requests for security assessment services
- Enable more consistent and cost effective security assessments among information systems and agencies

FISMA Phase II
Program Goals and Objectives

- Facilitate security assessment provider understanding of NIST standards and guidelines in support of FISMA
- Provide federal agencies with a level of assurance that security assessment providers are qualified and capable of providing security assessment services
- Establish a pool of qualified security assessment providers

Program Implementation

- Conduct background analysis
- Develop draft requirements
- Solicit feedback through workshops and community reviews
- Develop final requirements
- Decide on appropriate credentialing model
- Implement the credentialing model selected

Background Analysis

- Accreditation-related standards (ISO, ANSI, NVLAP)
- Certification programs for individuals and organizations (CISSP, SSCP, CISA, CIPP certification and others, university and college curriculum, ISO 9000 certification)
- Other security assessment programs (SE-CMM, NSA's IA CMM, etc.)
- Lessons learned

FISMA Phase II Timeline

Credentialing Model Criteria

- Retain NIST role to define standards but minimize NIST involvement and resources in day-to-day activities
- Keep time and cost of security service provider credentialing reasonable
- Be able to accommodate a large number of security service provider credentialing requests
- Base the program on international standards
- Begin implementation as soon as possible

Credentialing Options

- Option #1: Consumer-Based
- Option #2: Public or Private
- Option #3: NIST Sponsored

Consumer-Based Credentialing

- Consumers draw upon established requirements to credential and acquire security assessment services.
- Possible consumer-based credentialing could include examples such as—
  - incorporating security assessment provider requirements in request for proposals (RFPs) and using evaluation criteria for evaluating security assessment provider proposals, or
  - informally using requirements and evaluation criteria for selecting independent in-house assessment services

Public or Private Credentialing

- Community develops and operates a credentialing process for security assessment providers based on established service provider capability requirements, evaluation criteria and training requirements ***without NIST sponsorship***
- Possible public or private credentialing could include examples such as establishing—
  - A sector or organization qualified supplier list, or
  - A national or international accreditation program based on national or international standards

NIST-Sponsored Credentialing

- NIST sponsors (or partners with others) in the establishment of a credentialing process for security assessment providers based on established service provider capability requirements, evaluation criteria, and training requirements
- NIST-sponsored credentialing may include sponsoring the development or operation of a credentialing process

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

Curt Barker
(301) 975-4768
wbarker@nist.gov

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

FISMA Implementation Project Phase II

Credentialing Requirements Initial Thoughts

Pat Toth

Computer Security Division
Information Technology Laboratory

Overview

- Project Overview
- Federal Agency Responsibilities
- Security Assessment Provider Requirements
  - Organizational Operating Requirements
  - Technical Requirements
- Evaluation Criteria
- Training Requirements
- Reviewer Guidance

FISMA Phase II Timeline

Draft Document

- Working Title: Requirements for Security Assessment Providers
- Available for public review June 2006

Federal Agency Responsibilities

- Describes the responsibilities that federal agencies have in making the program a success
  - Implement an Adequate Information Security Program
  - Integrate Security in the System Development Life Cycle
  - Ensure System Owners Complete Security Responsibilities

Federal Agency Responsibilities

- Integrate NIST Standards and Guidelines into Procurement Activities
- Artifacts and Individuals Available for Assessment Effort

Security Assessment Provider Requirements

- Defines the requirements that the security assessment provider must meet to become a ***credentialed*** security assessment provider
  - Organizational Operating Requirements
  - Technical Requirements

Organizational Operating Requirements

- Independence, Impartiality, and Integrity
- Confidentiality
- Organization and Management
- Personnel
- Document Control
- Methods and Procedures

Organizational Operating Requirements

- Handling Nonconformities and Correction Actions
- Records
- Results
- Handling Complaints

Organizational Operating Requirements

- Independence, Impartiality, and Integrity
  - Free from any commercial, financial, or other pressures that might affect judgment
  - Procedures to ensure that external persons or organizations cannot influence the results of the security assessment activities
  - May also provide security assessment services to that federal agency as long as adequate segregation of responsibilities and accountabilities exists between the sub-organizations

Organizational Operating Requirements

- Personnel
  - The security assessment provider has a sufficient number of permanent personnel with the range of expertise to carry out their assessment functions
  - The security assessment provider ensures that personnel:
    - Are familiar with security assessment procedures and other relevant requirements
    - Are familiar with NIST standards and guidelines
    - Have undergone relevant training
    - Have a thorough knowledge of the relevant security assessment methods

Organizational Operating Requirements

- Results
  - Documents its results in a security assessment report that describes the extent to which the information system under examination conforms to the pre-defined requirements.
  - A designated representative signs and approves the security assessment report prior to delivery; any updates or modifications are subject to the same approval process.
  - Documents the basis upon which the opinions and interpretations have been made if included in the security assessment report.

Technical Requirements

- Planning and Resources
- Documentation and Supporting Material
- Categorization of Information and Information Systems
- Risk Assessment
- System Security Plan

Technical Requirements

- Accreditation Boundary
- Security Controls
- Security Assessments
- Plan of Action and Milestones

Technical Requirements

- Security Controls
  - Implements documented, internal procedures to validate that the security controls:
    - Have been selected according to guidelines in NIST SP 800-53
    - Have been tailored based on NIST SP 800-53 scoping guidance and the risk assessment
    - Have incorporated agency-specific controls
    - Have included compensating controls where appropriate
    - Have been documented in the system security plan in accordance with NIST SP 800-18
  - Implements standard templates and checklists to assist in validating the security controls

Technical Requirements

- Security Assessments
  - Template for the security assessment plan and uses it to prepare the plan
  - Documents the following in the security assessment plan:
    - The goals and objectives of the security assessment
    - How the security assessment provider will conduct the security assessment
    - What common controls apply to the information system and how the assessment results for the common controls will be incorporated into the security assessment report

Technical Requirements

- Security Assessments (Continued)
  - The security assessment provider ensures the security assessment plan has been approved prior to initiating the security assessment.
  - The security assessment provider develops and follows standard assessment procedures, incorporating the guidance from NIST SP 800-53A and SP 800-37, to validate each security control documented in the system security plan, and to validate that the assessment procedures are attached to the security assessment plan.

Technical Requirements

- Security Assessments Continued
  - Implements documented, internal procedures to do the following:
    - Create assessment methods and procedures for agency-specific controls and attach them to the security assessment plan
    - Tailor the assessment methods and procedures based on specific system implementations
    - Incorporate appropriate checklists into the assessment process based on NIST SP 800-70

Evaluation Criteria

- Defines the criteria used to evaluate whether or not the security assessment provider has met the requirements
- Level of detail will greatly depend on which option is chosen

Sample Evaluation Criteria

- Personnel
  - The security assessment provider must make available the following objects and individuals to be assessed during the evaluation process for the personnel requirements:
    - Personnel Resumes
    - Summary of Personnel
    - Internal Procedures
    - Training System Documentation
    - Employees

Sample Evaluation Criteria

- Personnel 1 – The security assessment provider has a sufficient number of permanent personnel with the range of expertise to carry out their assessment functions.

Sample Evaluation Criteria

Procedures

1. **Examine** the security assessment provider's *personnel resumes* to verify that the personnel assigned to the security assessment activities have expertise in the specific technologies and assessment methods required for those activities.

Sample Evaluation Criteria

Procedures

2. Examine the security assessment provider's summary of personnel to verify that:
   - There are at least two people for every assessment task under contract
   - At least 85% of the individuals are permanent employees of the security assessment provider's organization

Training Requirements

- Defines the topics that individuals should know, and in which they should receive appropriate training, to demonstrate competence to participate in the program
  - Security Assessment Providers
  - Technical Managers
  - Executives

Training Requirements

- Security Assessment Providers
  - Risk Management
  - Certification and Accreditation Planning and Resource Management
  - Accreditation Boundary
  - Categorization of Information and Information Systems
  - Risk Assessment

Training Requirements

- Security Assessment Providers
  - Security Controls: Selection, Tailoring, and Validation
  - Security Assessment Plan
  - Security Assessment Methodologies
  - Security Assessment Report and POA&M

Training Requirements

- Technical Managers
  - Risk Management
  - Incorporating Security Assessment Provider Requirements into a Statement of Work
  - Evaluating Security Assessment Provider Compliance with Requirements
  - Federal Agency Responsibilities for Success
  - Activities to be Completed Prior to Assessment

Training Requirements

- Executive
  - Risk Management
  - Relevant Federal Regulations
  - Enterprise Information Security Program
  - Federal Agency Responsibilities for Success
  - Investment Management Process and Security

Reviewer Guidance

- Are the requirements appropriate, necessary, and sufficient?
- Are the requirements complete, consistent and coherent?
- Are the requirements and evaluation criteria at the appropriate level of detail?
- Do the requirements address the objectives of the FISMA Phase II Credentialing Program?

Reviewer Guidance

- Draft document to be posted June 2006
  - http://www.csrc.nist.gov/sec-cert
- Add your name to the mailing list

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

Curt Barker
(301) 975-4768
wbarker@nist.gov

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

Breakout Sessions

- Assessment Service Provider
  - Red Auditorium
- Credentialing Authorities
  - Employee Lounge
- Consumers of Assessment Services
  - Lecture Room B
  - Lecture Room D

Workshop Closing Reminders (Next Steps)

- Credentialing Requirements – 1st week of June
- Workshop slides posted this Friday at: http://csrc.nist.gov/sec-cert under "Events"
- Synopsis of workshop posted in two weeks on http://csrc.nist.gov/sec-cert under "Events"
- FISMA Phase II follow up workshop – November
- SP 800-53A comments due July 31st