FISMA Phase II
Credentialing Program Workshop

Pat Toth

Computer Security Division
Information Technology Laboratory

Agenda

- What is the FISMA Phase II Credentialing Program Workshop?
- Why should you be involved in the Workshop?
- What does the program hope to achieve?
- How will the program be implemented?

Managing Enterprise Risk

The 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

What is the FISMA Credentialing Program?

- A program to credential public and private sector organizations to conduct security certification services for federal agencies

Why is NIST involved in the Program?

- Federal agencies are concerned about the amount of money they are spending. How can they feel confident that …
  - They are spending security money wisely?
  - Security service provider is capable and competent to assess their system?
  - Their information systems are adequately protected and enable them to conduct their business/mission securely?

Workshop Participants

- NIST
- Federal Agencies
- OMB/GAO
- Oversight Bodies
- Proficiency Testing Organizations
- Security Service Providers

Why should you be involved in the Workshop?

- NIST – Establishes the standards & guidelines
- Federal Agencies – Acquires security services. Seeks assurance that security service providers are competent
- OMB/GAO – Seeks to reduce burden of FISMA audits
- Oversight Bodies – Provide consistent, proven methodology to validate security service provider competence
- Proficiency Testing Organizations – Validate that security service provider individuals have the required skills
- Security Service Providers – Demonstrate competence to provide security services

What does the Program hope to achieve?

- Ensure security service providers understand the NIST FISMA-related standards and guidance and can implement them consistently
- Provide federal agencies with a level of assurance that security service providers are qualified and capable of providing the requested services

Potential Model Criteria

- Retain NIST role to define standards but minimize NIST involvement and resources in day-to-day activities
- Keep costs to security service providers reasonable
- Give security service providers an opportunity to develop internal procedures over time
- Be able to process a large number of security service providers in a short period of time, eventually reaching a steady pace in accreditation requests
- Provide flexibility for security service providers to gain a status appropriate to the services they want to provide
- Base the program on international standards
- Begin implementation as soon as possible

Background Analysis

- Accreditation-related standards (ISO, ANSI, NVLAP). List references.
- 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

Credentialing Options

1: Consumer-Based

2: Public or Private Based

3: NIST Sponsored Public or Private Based

Consumer Based

- Consumers draw upon NIST established requirements to credential and acquire assessment services. Possible consumer-based credentialing could include examples such as (i) drawing on NIST established requirements for inclusion in request for proposals (RFPs) and proposal evaluations for procuring security assessment services, or (ii) informally using requirements and evaluation criteria for selecting independent in-house assessment services.

Public or Private Based

Community develops and operates a credentialing process for security assessment service providers based on NIST established service provider capability requirements, evaluation criteria and training requirements without NIST sponsorship. Possible public or private –based credentialing could include examples such as (1) establishing a sector or organization qualified supplier list, or (ii) establishing a national or international accreditation program base on national or international standards.

NIST Sponsored

- NIST sponsors (or partners with others) in establishment of a credentialing process for security assessment service providers based on NIST established service provider capability requirements, evaluation criteria and training requirements. The NIST sponsored credentialing may include only developing a credentialing process or both developing and operating a credentialing process.

Federal Agencies

- Participate in the Workshop
- April 26, 2006 at NIST
- Registration fee $20 per person
- http://rproxy.nist.gov/CRS

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