FISMA IMPLEMENTATION

Transitioning from Phase I to Phase II

September 20, 2007

Ron Ross

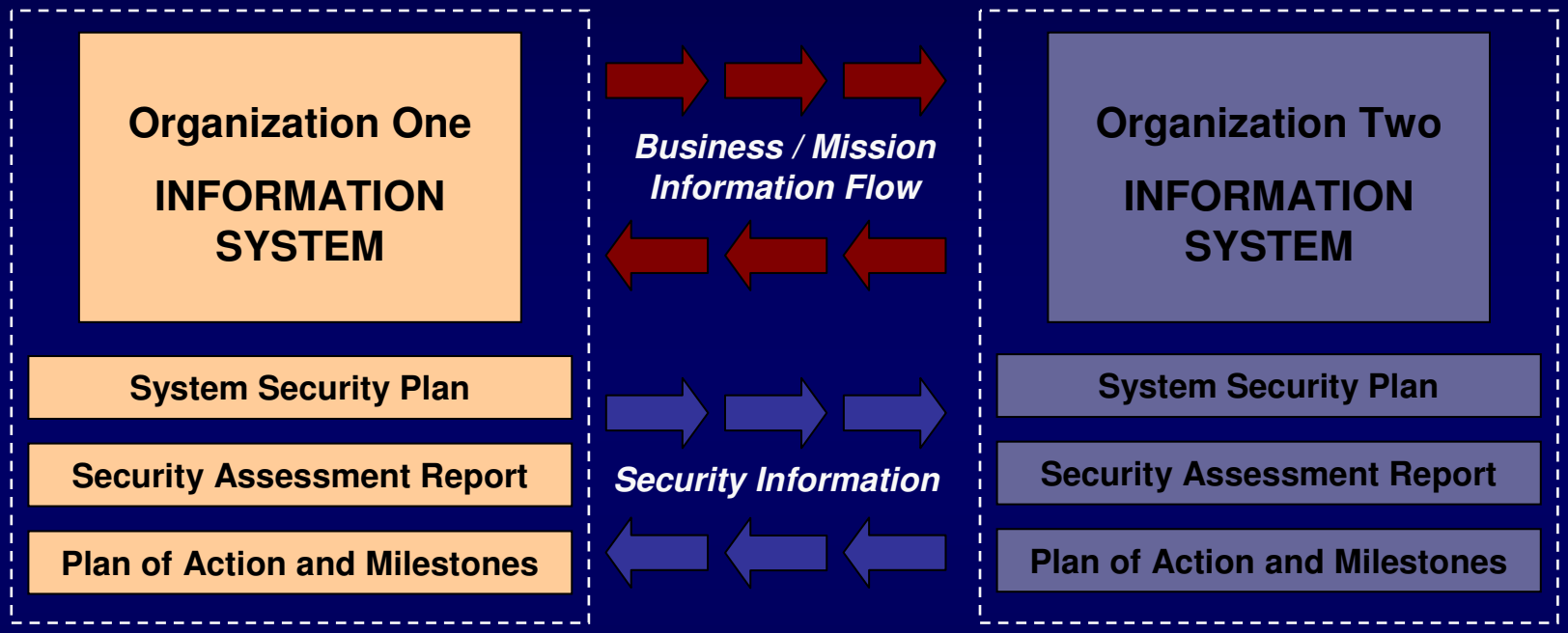
Computer Security Division
Information Technology Laboratory

Agenda

- Trust Relationships and Information Sharing
- FISMA Phase I
  - *What we have accomplished to date…*
- FISMA Phase II
  - *Where we are headed and why…*
- Questions and Answers

Trust Relationships

Security Visibility Among Business/Mission Partners



Determining risk to the organization's operations and assets, individuals, other organizations, and the nation; and the acceptability of such risk.

Determining risk to the organization's operations and assets, individuals, other organizations, and the nation; and the acceptability of such risk.

The objective is to achieve ***visibility*** into prospective business/mission partners information security programs…establishing a trust relationship based on the trustworthiness of information systems.

Information Security Imperatives

For Information Exchanges Among Partners

- The *responsibility to provide* information depends on a *trust relationship* established among partners.
- Trust cannot be *conferred*; it must be *earned*.
- Trust is *earned* by understanding the *security state* of your partner's information system.
- Understanding the security state of an information system depends on the *evidence* produced by partnering organizations demonstrating the effective employment of *safeguards and countermeasures*.

Information System Trustworthiness

- Trustworthiness is a characteristic or property of an information system that expresses the degree to which the system can be expected to preserve the *confidentiality*, *integrity*, and *availability* of the information being processed, stored, or transmitted by the system.
- Trustworthiness defines the *security state* of the information system at a particular point in time and is *measurable*.

Trustworthy Information Systems

- Trustworthy information systems are systems that are worthy of being trusted to operate within defined levels of *risk* to organizational operations and assets, individuals, other organizations, or the nation despite the *environmental disruptions*, *human errors*, and *purposeful attacks* that are expected to occur in the specified environments of operation.

System Trustworthiness Factors

- ***Security functionality***
  - Security-related functions or features of the system, for example, identification and authentication mechanisms, access control mechanisms, auditing mechanisms, and encryption mechanisms.
- ***Quality*** of the design, development, implementation, and operation
  - Degree to which the functionality is correct, always invoked, non bypassable, and resistant to tampering.
  - Achieved by employing well-defined security policy models, structured, disciplined, and rigorous hardware and software development techniques, and good system/security engineering principles and concepts when building an information system from information technology component products.
- ***Security assurance***
  - Grounds for confidence that the claims made about the functionality and quality of the system are being met.
  - Achieved through a variety of sources including post-development evidence brought forward regarding the design and implementation of the information system and the results of independent assessments (e.g., analyses, testing, evaluation, inspections, and audits) of the system conducted by qualified assessors.

Information Security Paradigm Shift

- From: *Policy-based compliance*
  - Policy dictates discrete, pre-defined information security requirements and associated safeguards/countermeasures;
  - Minimal flexibility in implementation; and
  - Little emphasis on explicit acceptance of mission risk.
- To: *Risk-based mission protection*
  - Enterprise missions and business functions drive security requirements and associated safeguards/countermeasures;
  - Highly flexible in implementation; and
  - Focuses on acknowledgement and acceptance of mission risk.

Defense-in-Breadth Strategy

- Diversify information technology assets.
- Reduce the information technology target size.
- Consider vulnerabilities of new information technologies before deployment.
- Apply a balanced set of management, operational, and technical security controls in a defense-in-depth approach.

FISMA Phase I

- Mission: Develop and propagate core set of FISMA-related security standards and guidelines for federal agencies and support contractors.
- Timeline: 2003-2007
- Status: On track to complete final publications this calendar year.

FISMA Phase I Publications

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Requirements)
- NIST Special Publication 800-18 (Security Planning)
- NIST Special Publication 800-30 (Risk Assessment) *
- NIST Special Publication 800-39 (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) *

* Publications currently under revision.
** Publications currently under development.

Final Phase I Projects

- Publication of the NIST Special Publication 800-39 (NIST Risk Management Framework)
- Completion of NIST Special Publication 800-53A
- Revision of NIST Special Publication 800-37
- Revision of NIST Special Publication 800-30
- Publication of an Authorizing Official's Handbook
- Industrial Control System Security Project
- DNI and DOD C&A Transformation Initiative

Milestone Schedule

- NIST Special Publication 800-39
  Managing Enterprise Risk
  A Framework for Addressing Cyber Threats to Organizations, Individuals, and the Nation
  Initial Public Draft: October 2007
  Final Publication: January 2008

- NIST Special Publication 800-30, Revision 1
  Effective Use of Risk Assessments in Managing Enterprise Risk
  Initial Public Draft: December 2007
  Second Public Draft: March 2008
  Final Publication: June 2008

Milestone Schedule

- NIST Special Publication 800-37, Revision 1
  Guide for the Security Certification and Accreditation of Federal Information Systems

  Initial Public Draft: January 2008
  Second Public Draft: April 2008
  Final Publication: July 2008

- NIST Special Publication 800-XXX
  Authorizing Official's Handbook

  Initial Public Draft: January 2008
  Second Public Draft: April 2008
  Final Publication: July 2008

FISMA Phase II

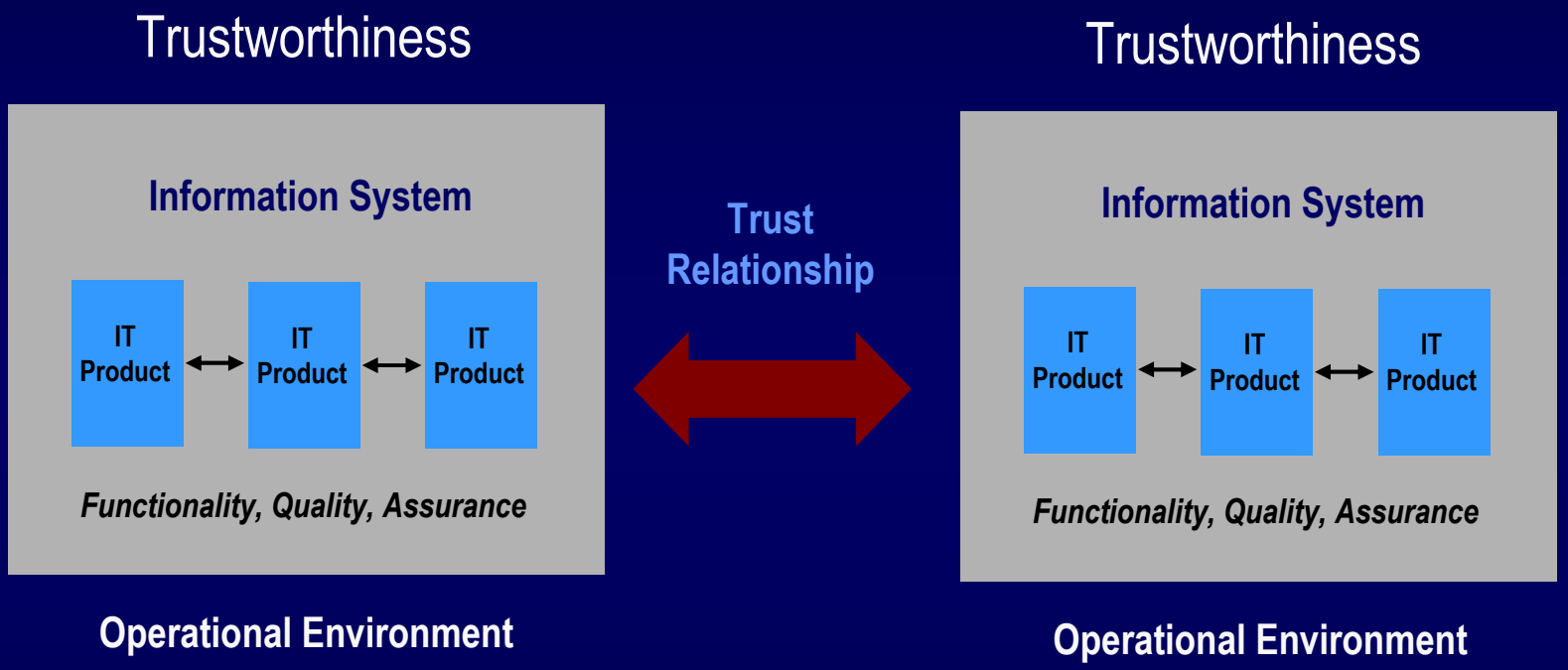
- Mission: Develop and implement a standards-based organizational credentialing program for public and private sector entities to demonstrate core competencies for offering security services to federal agencies.
- Timeline: 2007-2010
- Status: To begin initial work in late 2007.

FISMA Phase II

Demonstrating competence to provide information security services including—

- Assessments of Information Systems
  (Operational environments)
  - ***Security controls***
  - ***Configuration settings***
- Assessments of Information Technology Products
  (Laboratory environments)
  - ***Security functionality (features)***
  - ***Configuration settings***

FISMA Phase II



Producing evidence that supports the grounds for confidence in the design, development, implementation, and operation of information systems.

Training Initiative

- Information security training initiative underway to provide increased support to organizations using FISMA-related security standards and guidelines.
- Training initiative includes three components—
  - Frequently Asked Questions
  - Publication Summary Guides (Quickstart Guides)
  - Formal Curriculum and Training Courses
- NIST will provide initial training in order to fine-tune the curriculum; then transition to other providers.

ISO 27001 Harmonization Initiative

- Define relationship between the FISMA security standards and guidelines and the ISO 27001 Information Security Management System.
- Provide comprehensive mapping from FISMA standards and guidelines to ISO 27001.
- Develop and publish a “delta document” that states commonalities and differences among the standards.
- Explore possibilities for recognition and acceptance of assessment results to reduce information security costs.

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