NIST Support for DNI/DOD Transformation Initiative

Annual Computer Security Applications Conference

December 13, 2007

Gary Stoneburner

Johns Hopkins University/Applied Physics Laboratory

A Unified Framework

Civil, Defense, Intelligence Community Collaboration

The Generalized Model

Unique Information Security Requirements

The "Delta"

Common Information Security Requirements

Intelligence Community	Department of Defense	Federal Civil Agencies

Foundational Set of Information Security Standards and Guidance

- Standardized security categorization (criticality/sensitivity)
- Standardized security controls and control enhancements
- Standardized security control assessment procedures
- Standardized security certification and accreditation process

National security and non national security information systems

Building a Long-Term Partnership

Changing ways we are doing business…

- Civil, Defense, and Intelligence Communities collaborating on key security standards and guidelines for the federal government.
- Joint working groups share technical knowledge, implementation experiences, and new approaches for information security.
- Building a comprehensive, long-term, information security support infrastructure to support both non national security and national security systems.

Current Ongoing Initiatives

Collaborating with DNI, DOD, and CNSS…

- Serving in an advisory capacity to the Transformation Tiger Teams for development of unified risk management framework, security categorization scheme, security controls, and glossary of terms.
- Integrating new material into NIST publications to support other communities of interest.

Potential Joint Projects

- NIST Special Publication 800-39
  - *Managing Risk from Information Systems: An Organizational Perspective*
- NIST Special Publication 800-37, Revision 1
  - *Guide for the Security Certification and Accreditation for Federal Information Systems*
- NIST Special Publication 800-30, Revision 1
  - *Risk Assessment Guideline*
- NIST Special Publication 800-53A
  - *Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans*

Security Controls Convergence

- NIST Special Publication 800-53
  Recommended Security Controls for Federal Information Systems
- Revision 3 Planned for December 2008
- Incorporating all new material from the CNSS Security Controls Publication
- Repeating every two years in SP 800-53 update cycle; facilitating rapid convergence among communities

Security Control Assessments

- Assessment Case Development Project
- NIST, Intelligence Community, DOJ, DOE, and DOT joint interagency initiative
- Building detailed and comprehensive assessment cases for assessment procedures in NIST SP 800-53A
- Incorporating assessor experiences in building assessment cases
- Facilitating more cost effective and efficient testing and evaluation of information system security controls to determine effectiveness

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: Projected initiated; Draft NISTIR 7328.

FISMA Phase II

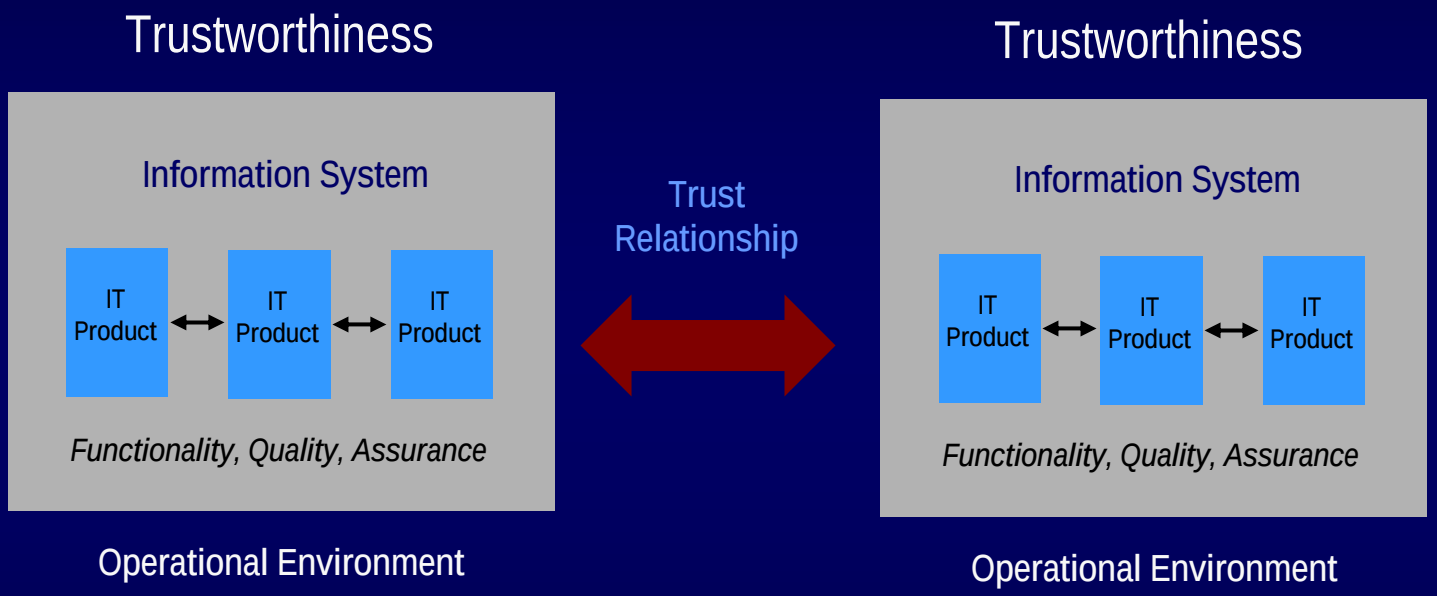
Demonstrating competence to provide information security services including—

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

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.

FISMA Phase II



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

ISE-PM Project

- Supporting the DNI Information Sharing Environment Initiative
- Incorporating key concepts from NIST SP 800-39
  - Trustworthiness of information systems
  - Trust model (for partnerships and information sharing)
  - Risk Management Framework

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 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.

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.

Elements of Trust

- Trust is earned by prospective service providers or business partners:
  - Identifying the common goals and objectives for the provision of services or information sharing;
  - Agreeing upon the risk associated with the provision of such services or information sharing;
  - Agreeing upon the degree of trustworthiness needed to adequately mitigate the risk;
  - Determining if the information systems are worthy of being trusted to operate within the agreed-upon levels of risk; and
  - Providing ongoing monitoring and oversight to ensure that the trust relationship is being maintained.

Information System Trustworthiness

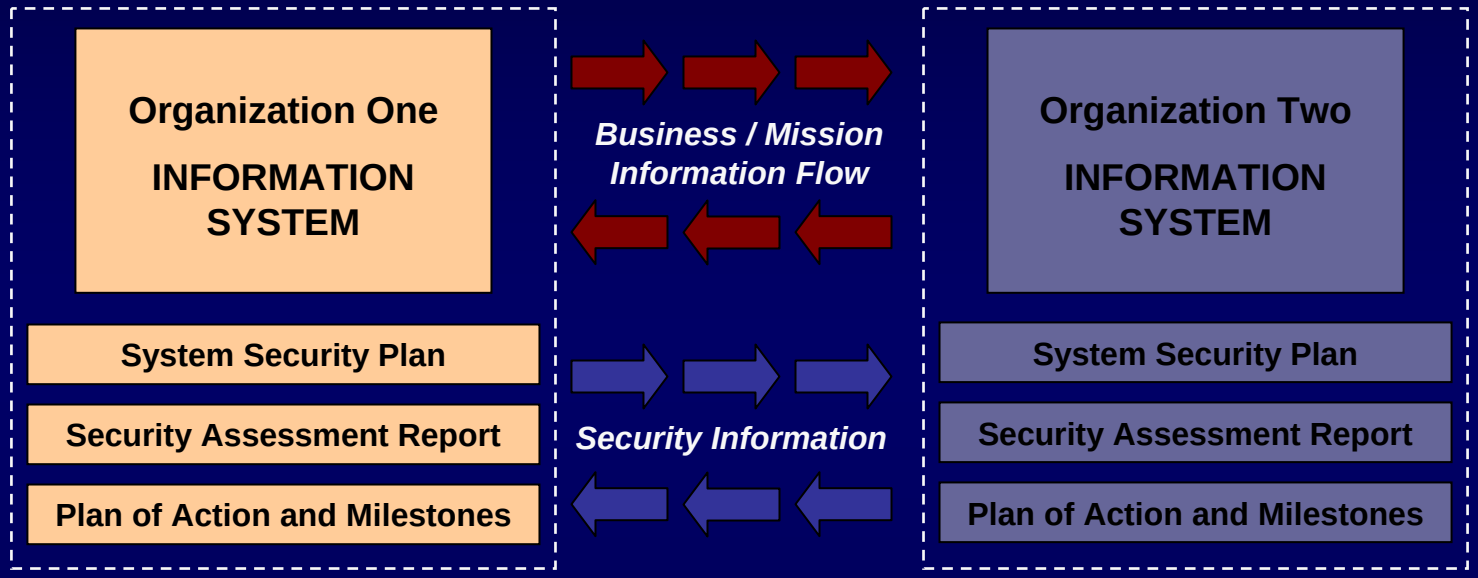
- Trustworthiness is a characteristic or property of an information system that expresses the degree to which the system can be expected to preserve the *confidentiality*, *integrity*, and *availability* of the information being processed, stored, or transmitted by the system.
- Trustworthiness defines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

Information System Trustworthiness

- *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 development and implementation*
  - Degree to which the functionality is correct, always invoked, non bypassable, and resistant to tampering.
  - Well-defined security policy models, structured, disciplined, and rigorous hardware and software development techniques, and good system/security engineering principles and concepts.
- *Security assurance*
  - Grounds for confidence that the claims made about the functionality and quality of the system are being met.
  - Evidence brought forward regarding the design and implementation of the system and the results of independent assessments.

Trust Relationships

Security Visibility Among Business/Mission Partners

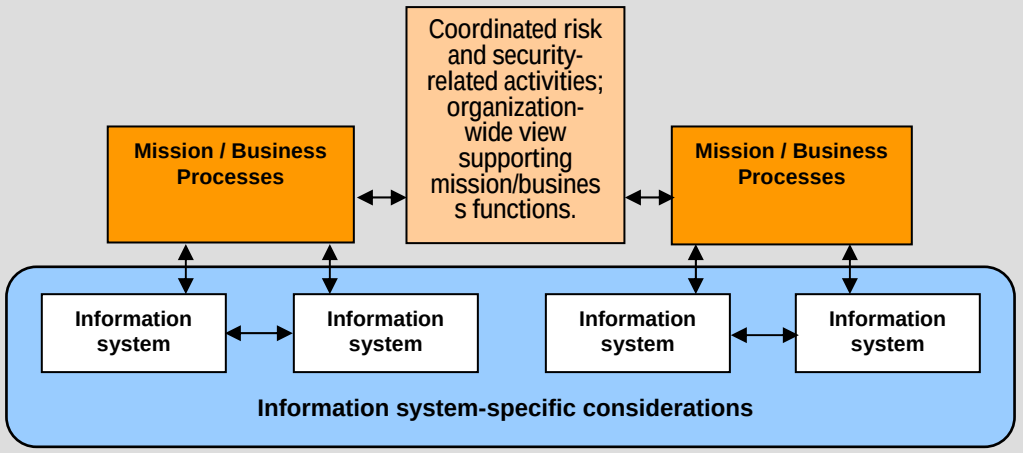


Determining risk to the organization's operations and assets, individuals, other organizations, and the nation; and the acceptability of such risk.

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.

Risk Executive Function



- Organizational information security priorities; allocation of resources.
- Systemic weaknesses and deficiencies addressed and corrected.
- Guidance on tailoring activities.
- Oversight of security categorizations.
- Common security controls identified and assignment of responsibilities.
- Common security control inheritance defined for information systems.
- Mandatory security configuration settings established and applied.

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