FISMA and Joint Task Force Project Updates

Information Security and Privacy Advisory Board

May 30, 2012

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

NIST SP 800-53, Revision 4 Supports

A New Cyber Defense Vision

Build it right – Continuously monitor

Cyber Defense – The Future

- Develop *risk-aware* mission and business processes.
- Develop and implement *enterprise architectures* with embedded information security architectures that support organizational mission/business processes.
- Use information technology *wisely* considering current threat landscape (capabilities, intent, and targeting).
- Develop and implement robust *continuous monitoring* programs.

Cyber Defense – Key Elements

- Incorporate cyber security requirements, principles, and concepts (through integrated project teams) into—
  - *Enterprise architecture.*
  - *Systems engineering processes.*
  - *Acquisition processes.*
- Employ architecture, engineering, and acquisition to develop stronger and more resilient information systems and system components.

Dual Protection Strategies

- **Boundary Protection**

  Primary Consideration: ***Penetration Resistance***
  Adversary Location: ***Outside the Defensive Perimeter***
  Objective: ***Repelling the Attack***

- **Agile Defense**

  Primary Consideration: ***Information System Resilience***
  Adversary Location: ***Inside the Defensive Perimeter***
  Objective: ***Operating while under Attack***

Agile Defense

- Boundary protection is a necessary but not sufficient condition for *Agile Defense*
- Examples of *Agile Defense* measures:
  - Compartmentalization and segregation of critical assets
  - Targeted allocation of security controls
  - Virtualization and obfuscation techniques
  - Encryption of data at rest
  - Limiting of privileges
  - Routine reconstitution to known secure state

Bottom Line: Limit damage of hostile attack while operating in a (potentially) degraded mode…

Highlights of SP 800-53 Update

Key Milestones

- 1000 comments from national data call in March 2011.
- Initial public draft released February 2012.
- Public comment period closed April 2012.
  - 1683 comments received.
  - Sources: public and private sector; national, international.
  - 95 contributors.
- Final public draft targeted for July 2012.
- Final publication targeted for September 2012.

Major Drivers for Update

- Current threat landscape.
- Empirical data obtained from cyber attacks.
- Gaps in coverage in current security control catalog.
- Insufficient attention to security assurance and trustworthiness.
- Need for additional tailoring guidance for specific missions, technologies, and environments of operation.

Gap Areas Addressed

- Insider threat.
- Application security.
- Supply chain risk.
- Security assurance and trustworthy systems.
- Mobile and cloud computing technologies.
- Advanced persistent threat.
- Tailoring guidance and overlays.
- Privacy.

Expanded Tailoring the Baseline

Document risk management decisions made during the tailoring process to provide information necessary for authorizing officials to make risk-based authorization decisions.

Control Enhancement Naming

AC-9 PREVIOUS LOGON (ACCESS) NOTIFICATION

Control: The information system notifies the user, upon successful interactive logon (access) to the system, of the date and time of the last logon (access).

Supplemental Guidance: This control is intended to cover both traditional logons to information systems and accesses to systems that occur in other types of architectural configurations (e.g., service oriented architectures). Related controls: AC-7, PL-4.

Control Enhancements:

(1) *PREVIOUS LOGON NOTIFICATION | UNSUCCESSFUL LOGONs*
The information system notifies the user, upon successful logon/access, of the number of unsuccessful logon/access attempts since the last successful logon/access.

(2) *PREVIOUS LOGON NOTIFICATION | SUCCESSFUL/UNSUCCESSFUL LOGONS*
The information system notifies the user of the number of [*Selection: successful logons/accesses; unsuccessful logon/access attempts; both*] during [*Assignment: organization-defined time period*].

Overlays

Overlays complement initial security control baselines—

- Provide the opportunity to add or eliminate controls.
- Provide security control applicability and interpretations.
- Establish community-wide parameter values for assignment and/or selection statements in security controls and control enhancements.
- Extend the supplemental guidance for security controls, where necessary.

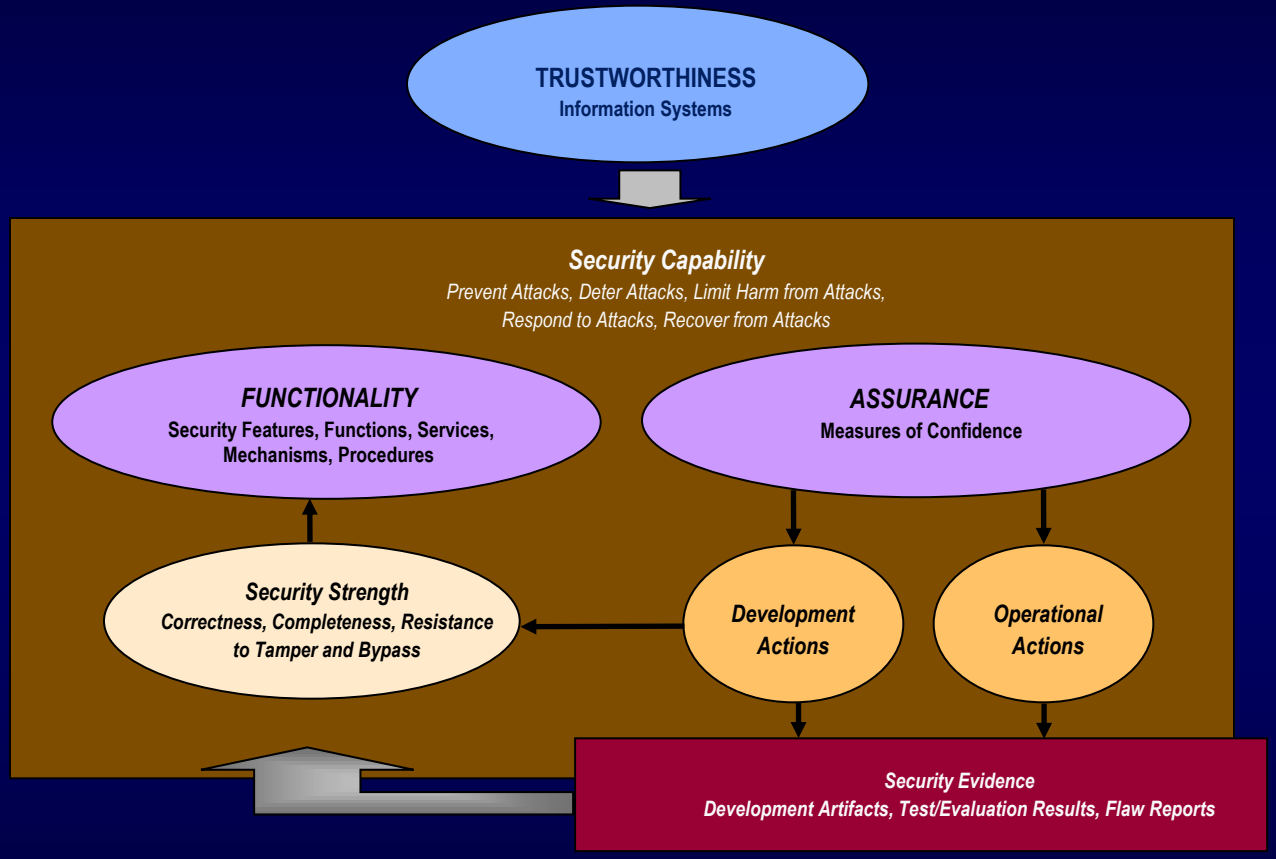
Types of Overlays

- Communities of interest (e.g., healthcare, intelligence, financial, law enforcement).
- Information technologies/computing paradigms (e.g., cloud/mobile, PKI, Smart Grid).
- Industry sectors (e.g., nuclear power, transportation).
- Environments of operation (e.g., space, tactical).
- Types of information systems (e.g., industrial/process control systems, weapons systems).
- Types of missions/operations (e.g., counter terrorism, first responders, R&D, test, and evaluation).

Rebranding the Concept of Assurance

- Objectives for SP 800-53, Revision 4—
  - What is assurance?
  - Why is assurance important?
  - How are organizations obtaining assurance now?
  - How can organizations obtain increased levels of assurance in the future?

Assurance and Trustworthiness



Enables Understanding of Security Capability

Trustworthiness and Assurance

- Significant changes to security controls and control enhancements in—
- Configuration Management (CM) family.
- System and Services Acquisition (SA) family.
- System and Information Integrity (SI) family.

Applying best practices in software application development at all stages in the SDLC.

Significant Updates to SA Family

Control Focus Areas

- Development process, standards, and tools.
- Developer security architecture and design.
- Developer configuration management.
- Developer security testing.
- Developer-provided training.
- Supply chain protection.

Minimum Assurance – Appendix E

- Appendix E has been completely revised and reworked.
- The *minimum* required assurance is provided by implementation of the appropriate baseline set of controls.
- The *assurance-related* controls for each baseline are provided in tables E-1, E-2, and E-3.
- Additional assurance-related controls are provided in table E-4, i.e., assurance-related controls not in any baseline.

Table E-1 - Minimum Assurance for Low Impact Baseline

ID	CONTROLS	ID	CONTROLS
AC	AC-1	MP	MP-1
AT	AT-1, AT-2, AT-3, AT-4	PE	PE-1, PE-6, PE-8
AU	AU-1, AU-6	PL	PL-1, PL-2, PL-4
CA	CA-1, CA-2, CA-3, CA-5, CA-6, CA-7	PS	PS-1, PS-6, PS-7
CM	CM-1, CM-2, CM-8	RA	RA-1, RA-3, RA-5
CP	CP-1, CP-3, CP-4	SA	SA-1, SA-2, SA-3, SA-4, SA-5, SA-9
IA	IA-1	SC	SC-1, SC-41
IR	IR-1, IR-2, IR-5	SI	SI-1, SI-4, SI-5
MA	MA-1		

OMB Policy Changes

OMB 2011 FISMA Reporting Guidance, *Memorandum-11-33*

http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf ***Question #28***

- "28. Is a security reauthorization still required every 3 years or when an information system has undergone significant change as stated in OMB Circular A-130?

  No. Rather than enforcing a static, three-year reauthorization process, agencies are expected to conduct ongoing authorizations of information systems through the implementation of continuous monitoring programs. Continuous monitoring programs thus fulfill the three year security reauthorization requirement, so a separate reauthorization process is not necessary……."

- Follow guidance consistent with NIST Special Publication 800-37, Revision 1.

Bottom Line: Rather than enforcing a static, every-three-year reauthorization process, agencies are expected to conduct ongoing authorizations of information systems through the implementation of continuous monitoring programs.

Continuous Monitoring

- Determine effectiveness of risk mitigation measures.
- Identify changes to information systems and environments of operation.
- Verify compliance.

Bottom Line: Increase situational awareness to help determine risk to organizational operations and assets, individuals, other organizations, and the Nation.

Focus Areas — 2012 and Beyond

- NIST Special Publication 800-30, Revision 1
  Guide for Conducting Risk Assessments
- NIST Special Publication 800-160
  Security Engineering Guideline
- Update to NIST Special Publication 800-53, Revision 4
  Security and Privacy Controls for Federal Information Systems and Organizations
- Update to NIST Special Publication 800-53A, Revision 2
  Guide for Assessing the Security Controls in Federal Information Systems and Organizations

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

Kelley Dempsey
(301) 975-2827
kelley.dempsey@nist.gov

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

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

Web: csrc.nist.gov/sec-cert

Comments: sec-cert@nist.gov