Evolving Risk Management Strategies

The Impact of SP 800-53, Revision 4

Information Security and Privacy Advisory Board

October 10, 2012

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

Agenda

- Update on the development and publication status of NIST Special Publication 800-53, Revision 4.
- Implications of Special Publication 800-53, Revision 4.
- Status report on the transformation to the unified information security framework and potential impacts with regard to Special Publication 800-53, Revision 4 –
    - *DoD perspective.*
    - *ODNI and Intelligence Community perspective.*

Since we last met in May.

Several interesting things have occurred…

Key Events and Milestones

- Change in priority of Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*.
- Original schedule called for final public draft of Special Publication 800-53, Revision 4, in July 2012 with final publication in September 2012.
- Actual comment count increased from 1683 to over 2000 (due to additional working group comments).
- Decision to move Industrial Control System Appendix to Special Publication 800-82.

Current Milestones

- Targeting final public draft of Special Publication 800-53, Revision 4, for end of November 2012.
    - *Comment adjudications received from all Joint Task Force partners (DOD, IC, NIST) and other working groups.*
    - *Final markup now in progress.*
- Targeting final publication in January 2013 but keeping option open for publishing final document in November 2012 (sense of urgency / requests from customers).
- Possibility the publication date may slip due to complexity and size of update.

Special Publication 800-53, Revision 4.

Big changes on the way but first, let’s recap…

The federal cyber security strategy…

Build It Right, Then Continuously Monitor

The First Front.

What we have accomplished…

Joint Task Force Transformation Initiative

- In 2012, completed development of comprehensive security guidelines that can be adopted by all federal agencies including the national security community.
- Flexible and extensible tool box includes:
  - *An enterprise-wide risk management process.*
  - *State-of-the-practice, comprehensive, security controls.*
  - *Risk management framework.*
  - *Risk assessment process.*
  - *Security control assessment procedures.*

Unified Information Security Framework

- NIST Special Publication 800-39
  Managing Information Security Risk:
  Organization, Mission, and Information System View
- NIST Special Publication 800-30
  Guide for Conducting Risk Assessments
- NIST Special Publication 800-37
  Applying the Risk Management Framework
  to Federal Information Systems
- NIST Special Publication 800-53
  Recommended Security Controls for Federal
  Information Systems and Organizations
- NIST Special Publication 800-53A
  Guide for Assessing the Security Controls
  in Federal Information Systems and Organizations

The Second Front.

What we need to accomplish…

A New Approach for Information Security

- Work directly with mission/business owners and program managers.
- Bring all stakeholders to the table with a vested interest in the success or outcome of the mission or business function.
- Consider information security requirements as mainstream functional requirements.
- Conduct security trade-off analyses with regard to cost, schedule, and performance requirements.
- Implement enforceable metrics for key officials.

SP 800-53 Rev 4 Driving Major Changes

(1 of 2)

- Special Publication 800-82 (Industrial Control System Security) undergoing major changes.
  - *Phase I: ICS Appendix from SP 800-53, Revision 3, moving to SP 800-82 (simultaneous release with SP 800-53, Revision 4).*
  - *Phase II: Full update to SP 800-82 by September 2013.*
- Privacy requirements and controls will be part of standard lexicon and coordinated with security requirements.
- Overlay concept promotes specialization of security plans for federal agencies; potential significant expansion of use by private sector (voluntary basis).

SP 800-53 Rev 4 Driving Major Changes

(2 of 2)

- Special Publication 800-160 (Security Engineering Guideline) targeted for publication in late 2013.
  - *Security controls in SP 800-53, Revision 4, addressing trustworthy systems, assurance, and system resilience.*
  - *Exploring the possibility of system resiliency appendix in SP 800-53.*
- Opening up new discussions on the concept of assurance.
  - *How federal agencies can obtain IT products and information systems with greater assurance.*
  - *SP 800-53, Revision 4, (internal) mapping to Common Criteria (ISO/IEC 15408) requirements.*
- Impacting ISO/IEC 27001 and 27002.

What is the net effect of such changes?

Simplify, Specialize, and Integrate…

Increasing Strength of IT Infrastructure

- Simplify.
  - Reduce and manage *complexity* of IT infrastructure.
  - Use enterprise architecture to streamline the IT infrastructure; *standardize*, *optimize*, *consolidate* IT assets.
- Specialize.
  - Use guidance in SP 800-53, Rev 4 to *customize security plans* to support specific missions/business functions, environments of operation, and technologies.
  - Develop effective *monitoring strategies* linked to specialized security plans.

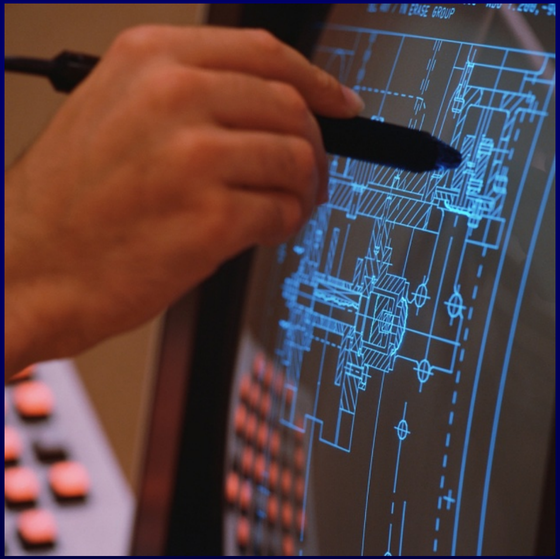
Increasing Strength of IT Infrastructure

- Integrate.
  - Build information security requirements and controls into mainstream organizational processes including:
    - *Enterprise Architecture*.
    - *Systems Engineering*.
    - *System Development Life Cycle*.
    - *Acquisition*.
  - Eliminate information security programs and practices as stovepipes within organizations.
  - Ensure information security decisions are risk-based and part of routine *cost*, *schedule*, and *performance* tradeoffs.

If we can’t understand it –

we can’t protect it…

We need to build our security programs like NASA builds space shuttles— using the *integrated project team* concept.



Functionality and Assurance.

They ride together…

FUNCTIONALITY

What is observable in front of the wall.

What is observable behind the wall.

ASSURANCE

SP 800-53
Revision 4

Increased Breadth and Depth of Security Controls

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

SP 800-30
Revision 1

Risk Assessments Play a Pivotal Role

Risk Tolerance.

How you know when to stop deploying security controls…

And until we build it right.

What should we do?

Important Stop-Gap Actions

- For high-end adversaries launching sophisticated and well-coordinated cyber attacks targeting: U.S. critical infrastructure; federal mission-essential functions and systems; and private sector industries—
  - ✓ Develop, implement, and exercise robust contingency plans to support full scale continuity of operations;
  - ✓ Implement continuous monitoring programs; and

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

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

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

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

Web: csrc.nist.gov/sec-cert

Comments: sec-cert@nist.gov