The Future of Cyber Security

NIST Special Publication 800-53, Revision 4

Cybersecurity Innovation Forum

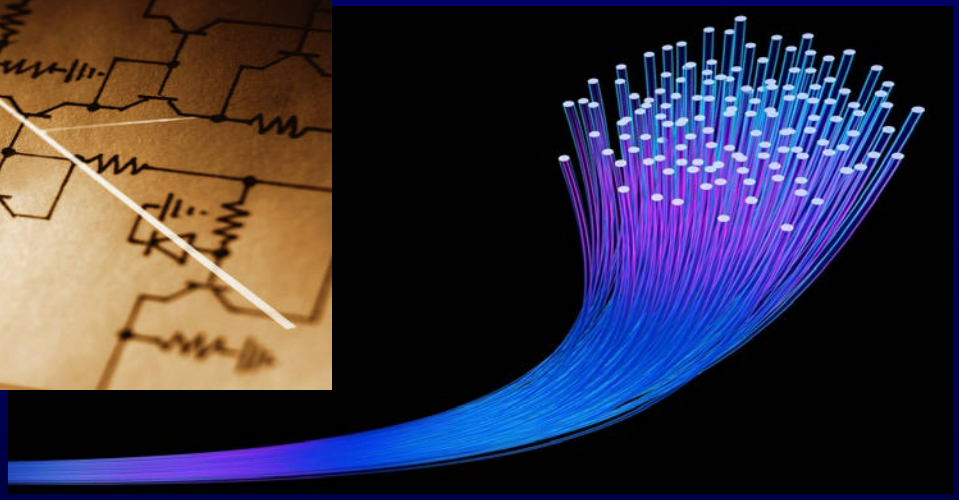
January 30, 2014

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

The federal cyber security strategy…

Build It Right, Continuously Monitor



Good housekeeping is necessary…

But not sufficient.

You can't count, configure, or patch your way out of this problem space.

Tough decisions ahead.

The national imperative for building stronger, more resilient information systems…

Software assurance.

Systems and security engineering.

Supply chain risk management.

Necessary *and* Sufficient Security Solutions…

Cyber Security Hygiene

COUNTING, CONFIGURING, AND PATCHING IT ASSETS

Strengthening the IT Infrastructure

ARCHITECTURE, ENGINEERING, AND SYSTEM RESILIENCY

Has your organization achieved the appropriate balance?

Simplify.

Specialize.

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 into organizational processes.
    - *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.

Special Publication 800-53, Revision 4.

Big changes have arrived…

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

Highlights of SP 800-53 Update

Structural Changes

Security Control Class Designations

Eliminated management, operational, and technical class labels on security control families—

ID	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	
CA	Security Assessment and Authorization	
CM	Configuration Management	
CP	Contingency Planning	
IA	Identification and Authentication	
IR	Incident Response	
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	
PL	Planning	
PS	Personnel Security	
RA	Risk Assessment	
SA	System and Services Acquisition	
SC	System and Communications Protection	
SI	System and Information Integrity	Operational
PM	Program Management	Management

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*].

Tables Added to Appendix D

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
PL-1	**Security Planning Policy and Procedures**		**A**	X	X	X
PL-2	**System Security Plan**		**A**	X	X	X
PL-2 (1)	*SYSTEM SECURITY PLAN | CONCEPT OF OPERATIONS*	**W**	Incorporated into PL-7.			
PL-2 (2)	*SYSTEM SECURITY PLAN | FUNCTIONAL ARCHITECTURE*	**W**	Incorporated into PL-8.			
PL-2 (3)	*SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES*		**A**		X	X
PL-3	**System Security Plan Update**	**W**	Incorporated into PL-2.			
PL-4	**Rules of Behavior**		**A**	X	X	X
PL-4 (1)	*RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS*		**A**		X	X
PL-5	**Privacy Impact Assessment**	**W**	Incorporated into Appendix J, AR-2.			
PL-6	**Security-Related Activity Planning**	**W**	Incorporated into PL-2.			
PL-7	**Security Concept of Operations**					
PL-8	**Security Architecture**					

Assumptions, Baselines, and Tailoring

Clarification of Term *Baseline*

The use of the term *baseline* is intentional. The security controls and control enhancements listed in the initial baselines are *not* a minimum—but rather a proposed starting point from which controls and controls enhancements may be removed or added based on the tailoring guidance in Section 3.2.

Specialization of security plans is the goal…

Assumptions Applied to Baselines

- Information systems are located in fixed, physical facilities, complexes, or locations.
- User information in systems is (relatively) persistent.
- Information systems are multi-user (either serially or concurrently) in operation.
- Information systems exist in networked environments.
- Information systems are general purpose in nature.
- Organizations have the necessary structure, resources, and infrastructure to implement the security controls.

Assumptions Not Applied to Baselines

- Insider threats exist within organizations.
- Classified information is processed, stored, or transmitted.
- Advanced persistent threats exist within organizations.
- Information requires specialized protection based on federal legislation, Executive Orders, directives, regulations, or policies.
- Information systems communicate or interconnect with systems in different policy domains.

Expanded Tailoring Guidance
(1 of 2)

- Identifying and designating common controls in initial security control baselines.
- Applying scoping considerations to the remaining baseline security controls.
- Selecting compensating security controls, if needed.
- Assigning specific values to organization-defined security control parameters via explicit assignment and selection statements.

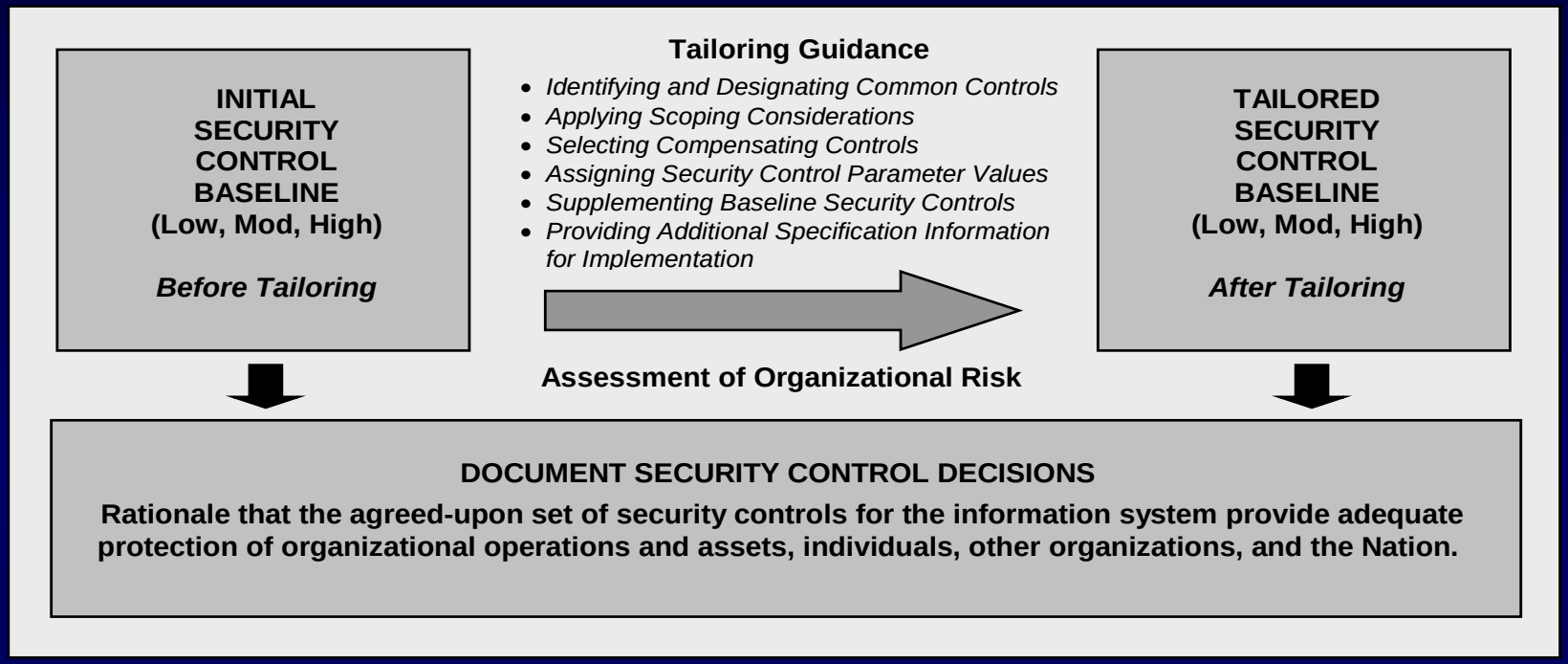
Expanded Tailoring Guidance
(2 of 2)

- Supplementing baselines with additional security controls and control enhancements, if needed.
- Providing additional specification information for control implementation.

Supplementing the Baseline

- Inputs may include risk assessment during the security control selection process and/or regulations, policies, etc.
- Example of supplementation for a specific threat—
  - ADVANCED PERSISTENT THREAT
    Security control baselines do not assume that the current threat environment is one where adversaries have achieved a significant foothold and presence within organizations and organizational information systems; that is, organizations are dealing with an advanced persistent threat. Adversaries continue to attack organizational information systems and the information technology infrastructure and are successful in some aspects of such attacks. To more fully address the APT, concepts such as insider threat protection (CM-5 (4)), diversity/heterogeneity (SC-27 and SC-29), deception (SC-26 and SC-30), non-persistence (SC-25 and SC-34), and segmentation (SC-7(13)) can be considered.

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.

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).

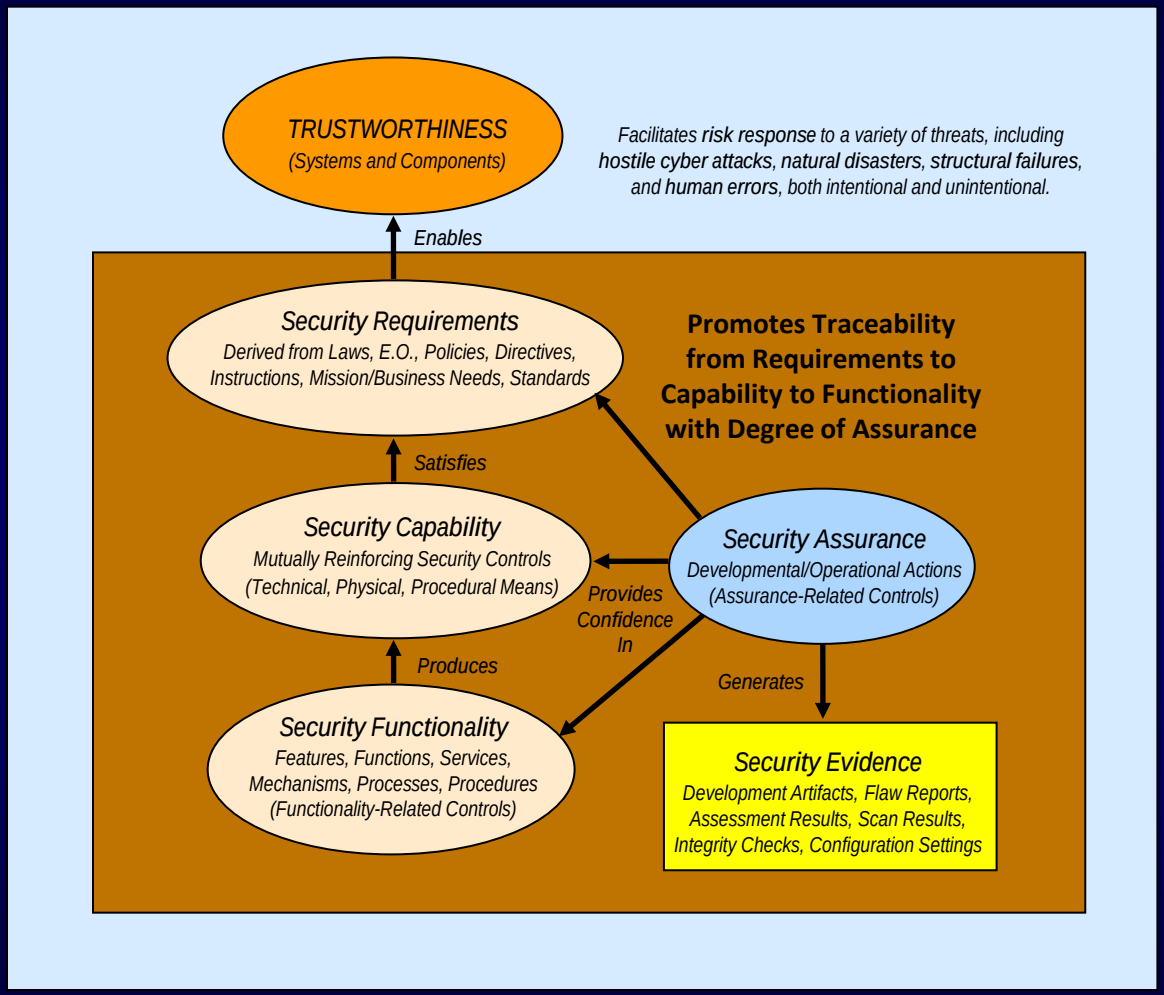
Functionality and Assurance.

They ride together…

What is observable in front of the wall.

What is observable behind the wall.

Assurance and Trustworthiness



Where Do We Need Assurance?

Security assurance must be addressed on three fronts—

- Information technology products.
- Information systems.
- Organizations.
  - *Acquisition processes.*
  - *Enterprise architecture.*
  - *System development life cycle.*
  - *Systems engineering.*

Minimum Assurance – Appendix E

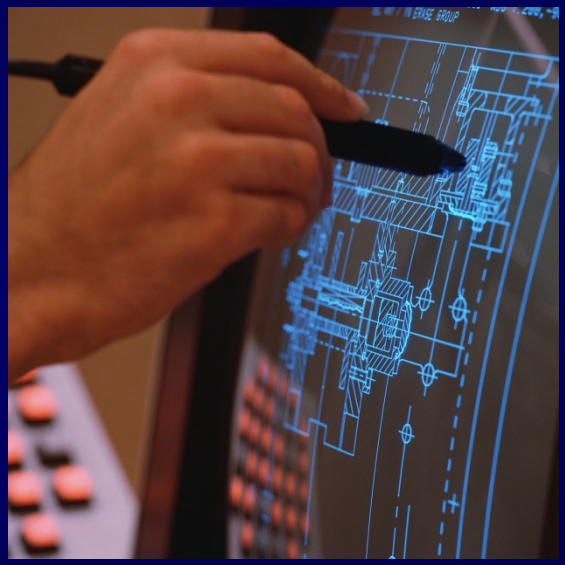
- Appendix E has been completely revised and reworked.
- The *minimum* required assurance is provided by implementation of the appropriate baseline set of controls.
- The *assurance-related* controls for each baseline are provided in tables E-1, E-2, and E-3.
- Additional assurance-related controls are 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		

Strengthening Specification Language

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



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

Significant Updates to Security Controls

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

Privacy Control Families

- Authority and Purpose (AP)
- Accountability, Audit, and Risk Management (AR)
- Data Quality and Integrity (DI)
- Data Minimization and Retention (DM)
- Individual Participation and Redress (IP)
- Security (SE)
- Transparency (TR)
- Use Limitation (UL)

There are no shortcuts.

Question and Answer Session.

Time to hear from you…

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