Impact Levels and Security Controls

Understanding FIPS 199, FIPS 200 and SP 800-53

NIST Cryptographic Key Management Workshop

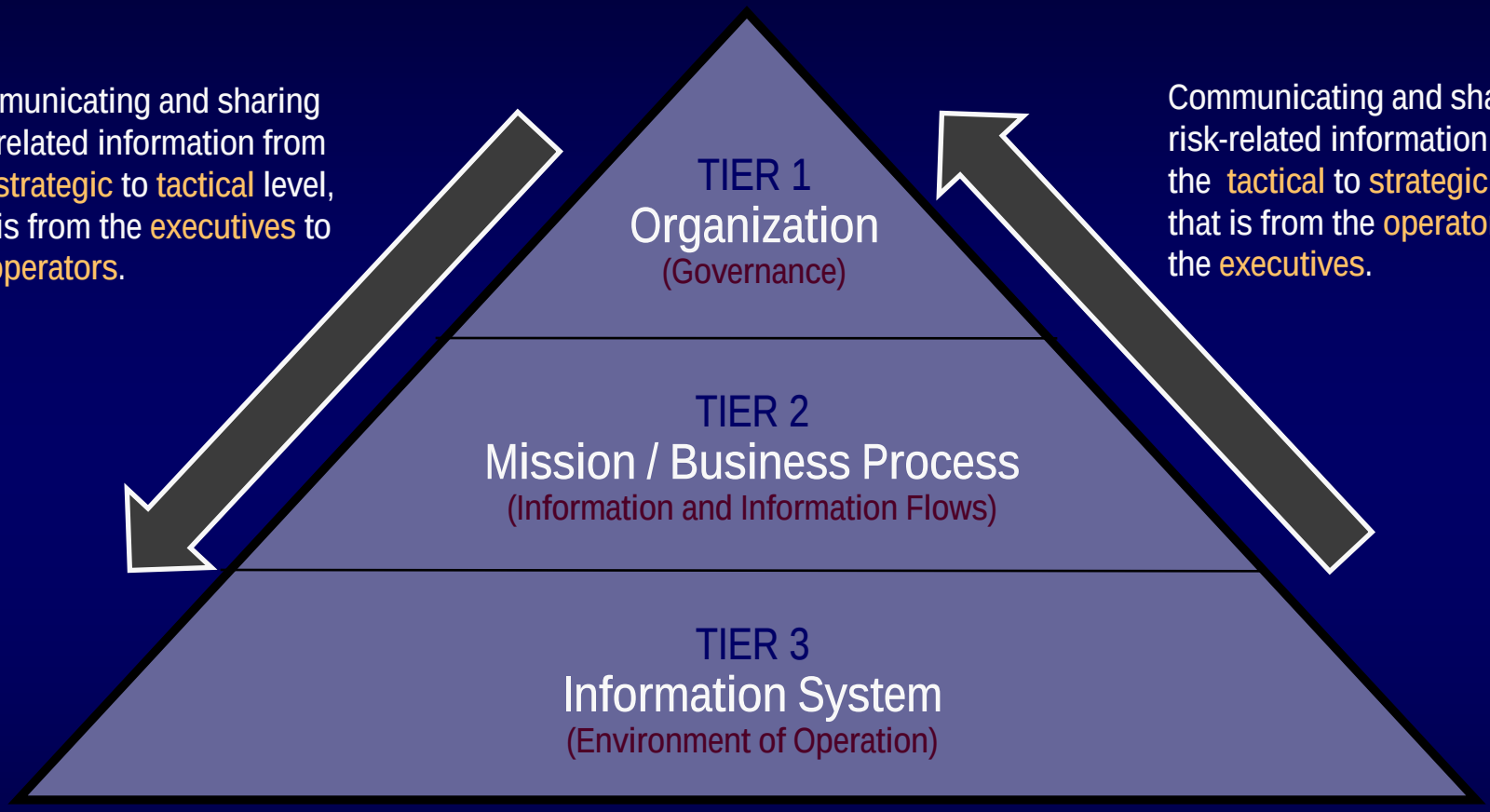
March 5, 2014

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

STRATEGIC (EXECUTIVE) RISK FOCUS

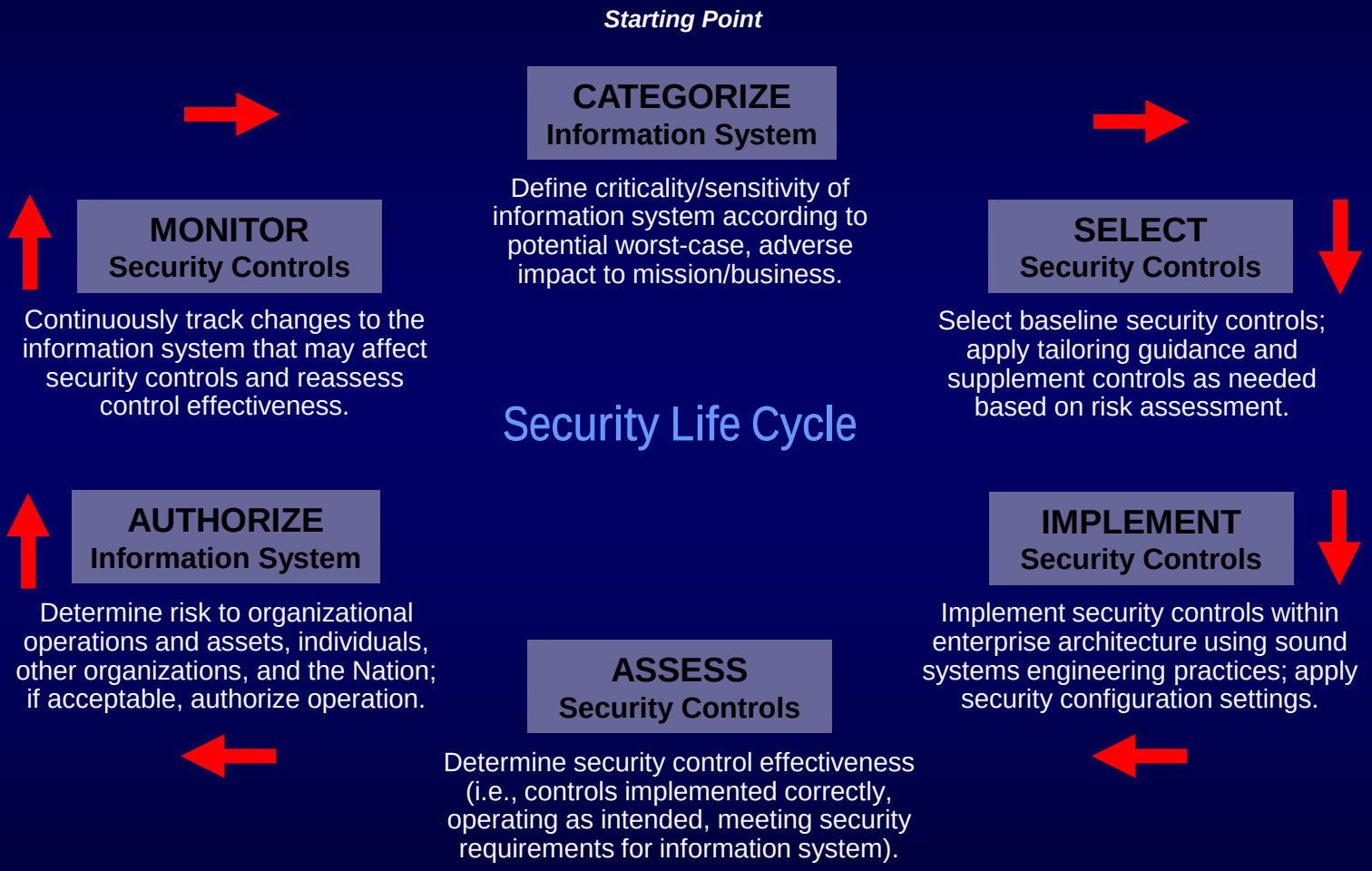
Communicating and sharing risk-related information from the strategic to tactical level, that is from the executives to the operators.



Communicating and sharing risk-related information from the tactical to strategic level, that is from the operators to the executives.

TACTICAL (OPERATIONAL) RISK FOCUS

Risk Management Framework



FIPS 199 Security Objectives

- CONFIDENTIALITY
  - "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…"
  - A loss of confidentiality is the unauthorized disclosure of information
- INTEGRITY
  - "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…"
  - A loss of integrity is the unauthorized modification or destruction of information
- AVAILABILITY
  - "Ensuring timely and reliable access to and use of information…"
  - A loss of availability is the disruption of access to or use of information or an information system

Security Categorization

Guidance for Mapping Types of Information and Information Systems to FIPS 199 Security Categories

SP 800-60

FIPS 199	LOW	MODERATE	HIGH
Confidentiality	The loss of confidentiality could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The loss of integrity could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a **severe or catastrophic** adve on orga operations, orga assets, or indivi
Availability	The loss of availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The los ability could b to have a **severe trophic** adverse e organizatio ons, organizationa individuals.

Baseline Security Controls for High Impact Systems

Security Controls

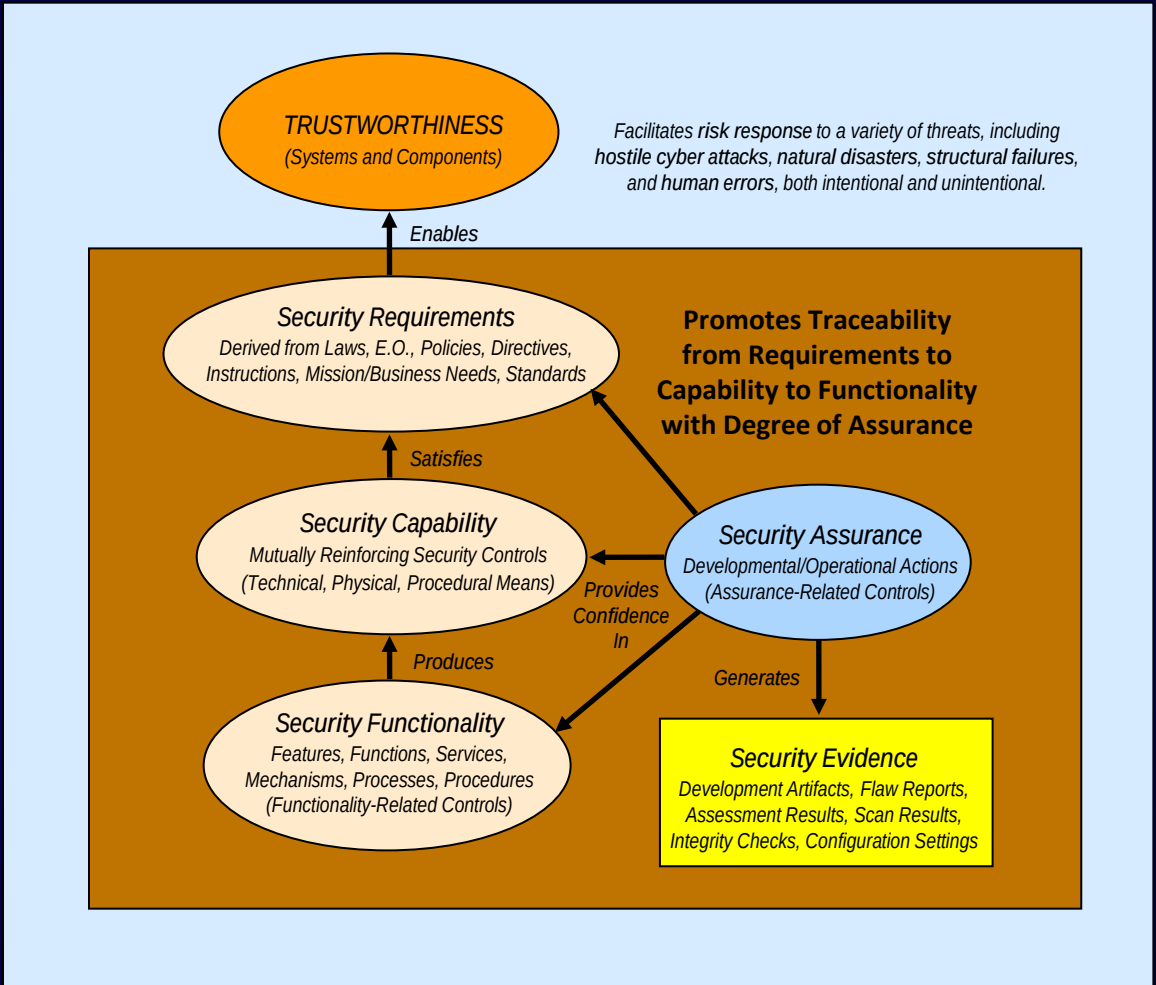
The safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Security Controls
Provide functionality and assurance.

What is observable in front of the wall.

What is observable behind the wall.

Assurance and Trustworthiness



NIST SP 800-53 Security Control Families

ID	FAMILY
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Security Assessment and Authorization
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
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
PM	Program Management

Control Naming Convention

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*].

Security Control Baselines

- Starting point for the security control selection process.
- Chosen based on the security category and associated impact level of the information system determined in accordance with FIPS 199 and FIPS 200, respectively.
- Three sets of baseline controls have been identified corresponding to low-impact, moderate-impact, and high-impact information system levels.
- Appendix D provides a listing of baseline security controls.

Security Control Baselines

- Baselines are determined by:
  - Information and system categorization (L, M, H)
  - Organizational risk assessment and risk tolerance
  - System level risk assessment
- Baselines can be tailored:
  - Instantiate parameters in controls
  - Implement scoping considerations and compensating controls
  - Supplement by with additional controls/enhancements.

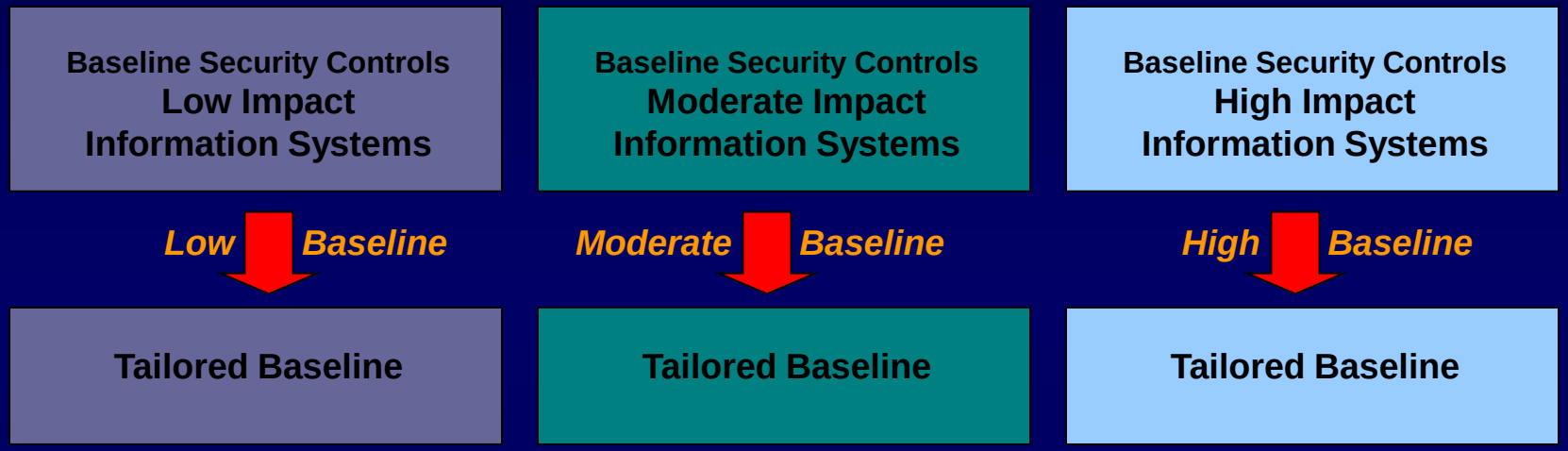
Clarification of Term *Baseline*

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 objective…

Tailoring Security Controls

Scoping, Parameterization, and Compensating Controls



A cost effective, risk-based approach to achieving adequate information security…

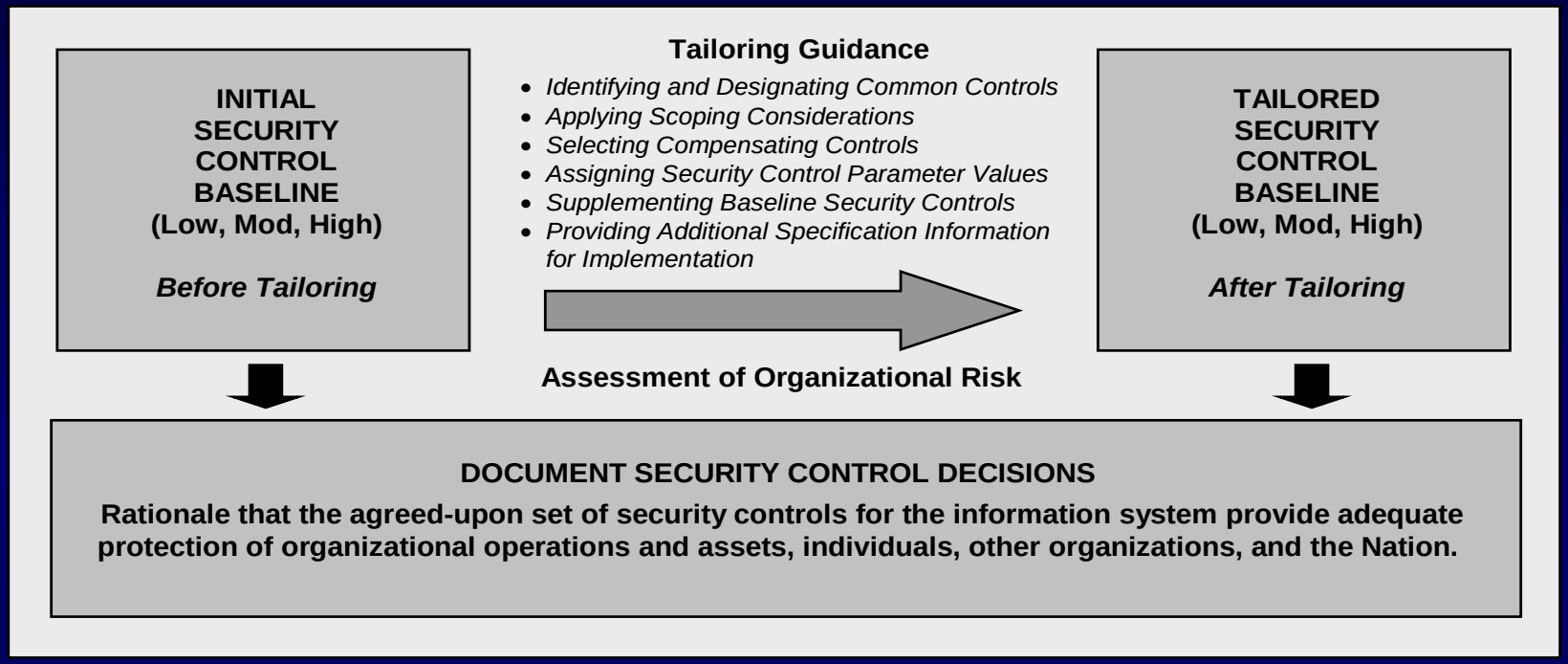
Expanded Tailoring Guidance
(1 of 2)

- 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.

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.

Tables in SP 800-53 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**					

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

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

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

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

Web: csrc.nist.gov/sec-cert

Comments: sec-cert@nist.gov