Federal Computer Security Program Manager's Forum

Department of Commerce

August 8, 2013

Computer Security Division
Information Technology Laboratory

Today's Agenda.

9:00 – 9:15	Welcome and Introduction
9:15 – 10:30	NIST Special Publication 800-53, Revision 4
10:30 – 10:45	Morning Break
10:45 – 11:30	Fundamentals of Continuous Monitoring
11:30 – 12:00	Question and Answer Session
12:00 – 1:15	Lunch
1:15 – 2:45	Panel 1: RMF Case Studies
2:45 – 3:00	Afternoon Break
3:00 – 4:15	Panel 2: Ongoing Authorization Case Studies
4:15 – 4:30	Concluding Remarks

The Future of Cyber Security

NIST Special Publication 800-53, Revision 4

Federal Computer Security Program Manager's Forum

August 8, 2013

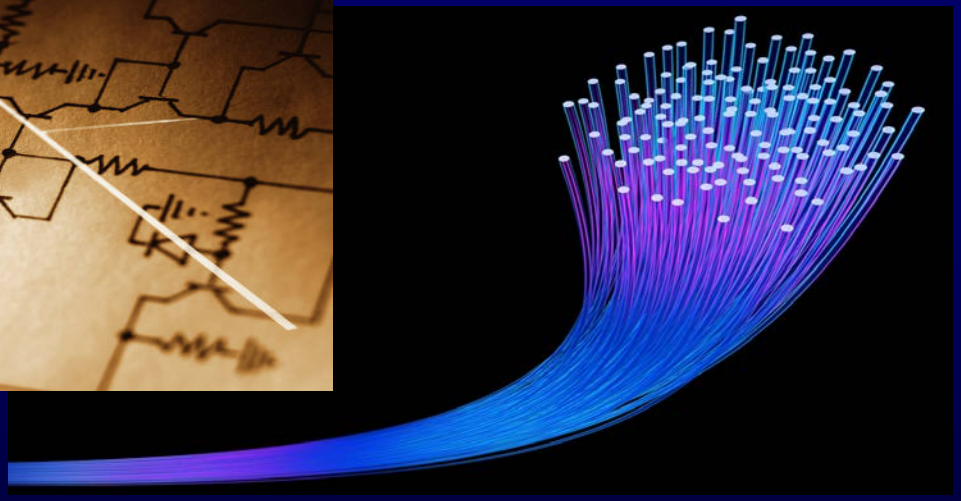
Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

Some initial thoughts.

The federal cyber security strategy…

Build It Right, Continuously Monitor



Being satisfied with stopping 85% of cyber attacks is like being happy you have plugged up 85% of the holes in the bottom of your boat…

Not good enough for critical information systems and critical infrastructure.

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…

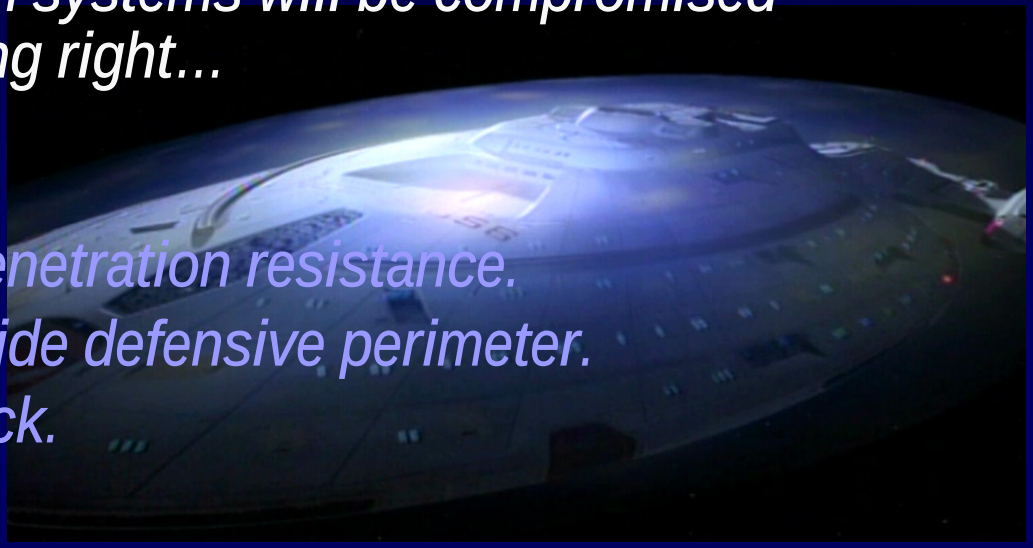
Software assurance.

Systems and security engineering.

Supply chain risk management.

Dual Protection Strategies

Sometimes your information systems will be compromised even when you do everything right…



- **Boundary Protection**

  Primary Consideration: *Penetration resistance.*
  Adversary Location: *Outside defensive perimeter.*
  Objective: *Repel the attack.*

- **Agile Defense**

  Primary Consideration: *Information system resilience.*
  Adversary Location: *Inside defensive perimeter.*
  Objective: *Operate while under attack, limit damage, survive.*

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?

What we have accomplished.

Unified Information Security Framework

The Generalized Model

Unique Information Security Requirements

The "Delta"

Common Information Security Requirements

Intelligence Community	Department of Defense	Federal Civil Agencies	Private Sector State and Local Govt

Foundational Set of Information Security Standards and Guidance

- Standardized risk management process
- Standardized security categorization (criticality/sensitivity)
- Standardized security controls (safeguards/countermeasures)
- Standardized security assessment procedures
- Standardized security authorization process

National security and non national security information systems

The Toolbox

- 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
  Security and Privacy Controls for Federal Information Systems and Organizations
- NIST Special Publication 800-53A
  Guide for Assessing the Security Controls in Federal Information Systems and Organizations

Netflix.

Intel.

ADP.

A New Approach for Information Security

- Work directly with executives, 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 executives.

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.

It's not the *number* of security controls that matters…

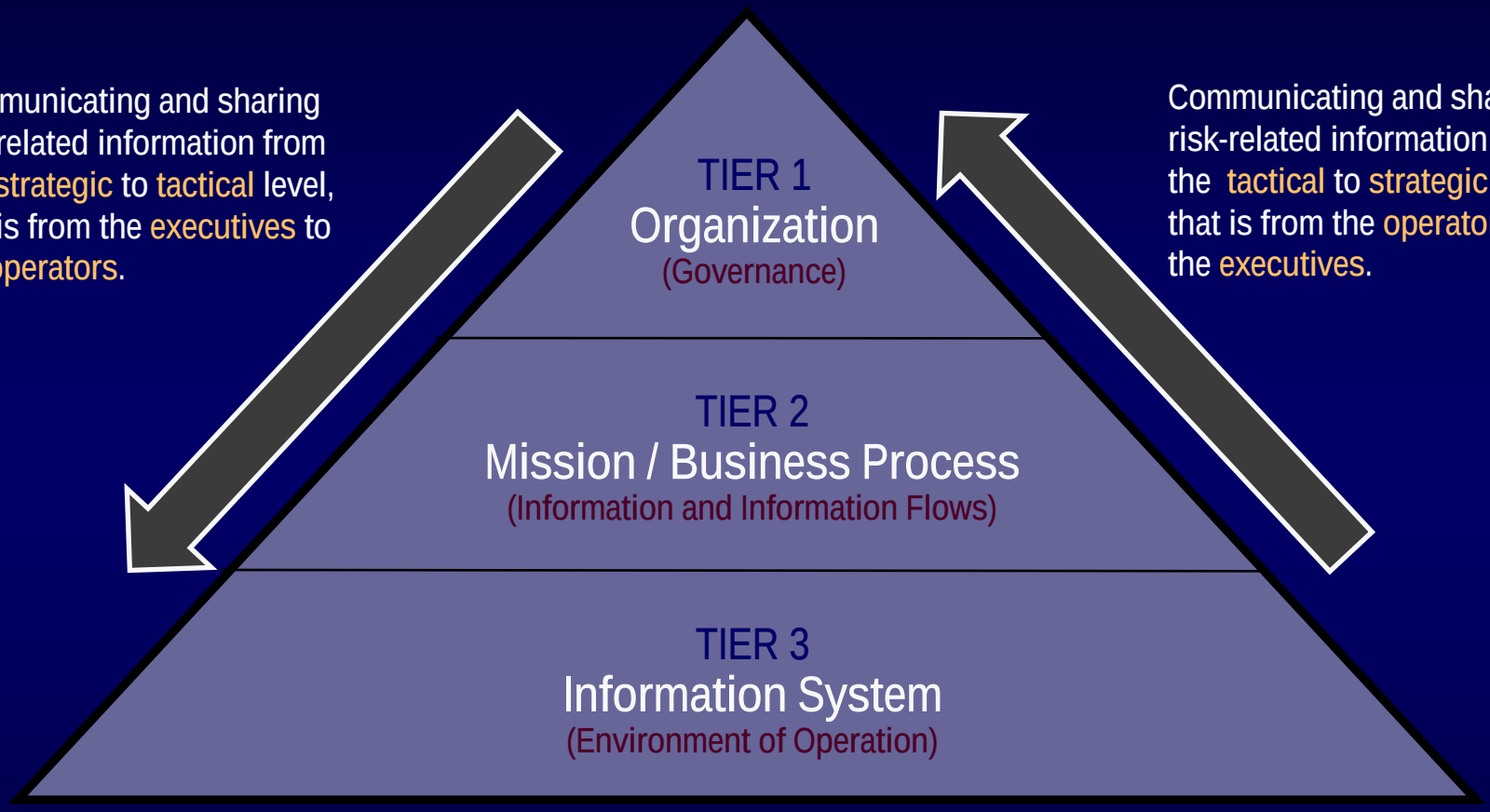
It's having the *right* controls to do the job.

Think strategic.

Execute tactical…

STRATEGIC (EXECUTIVE) RISK FOCUS

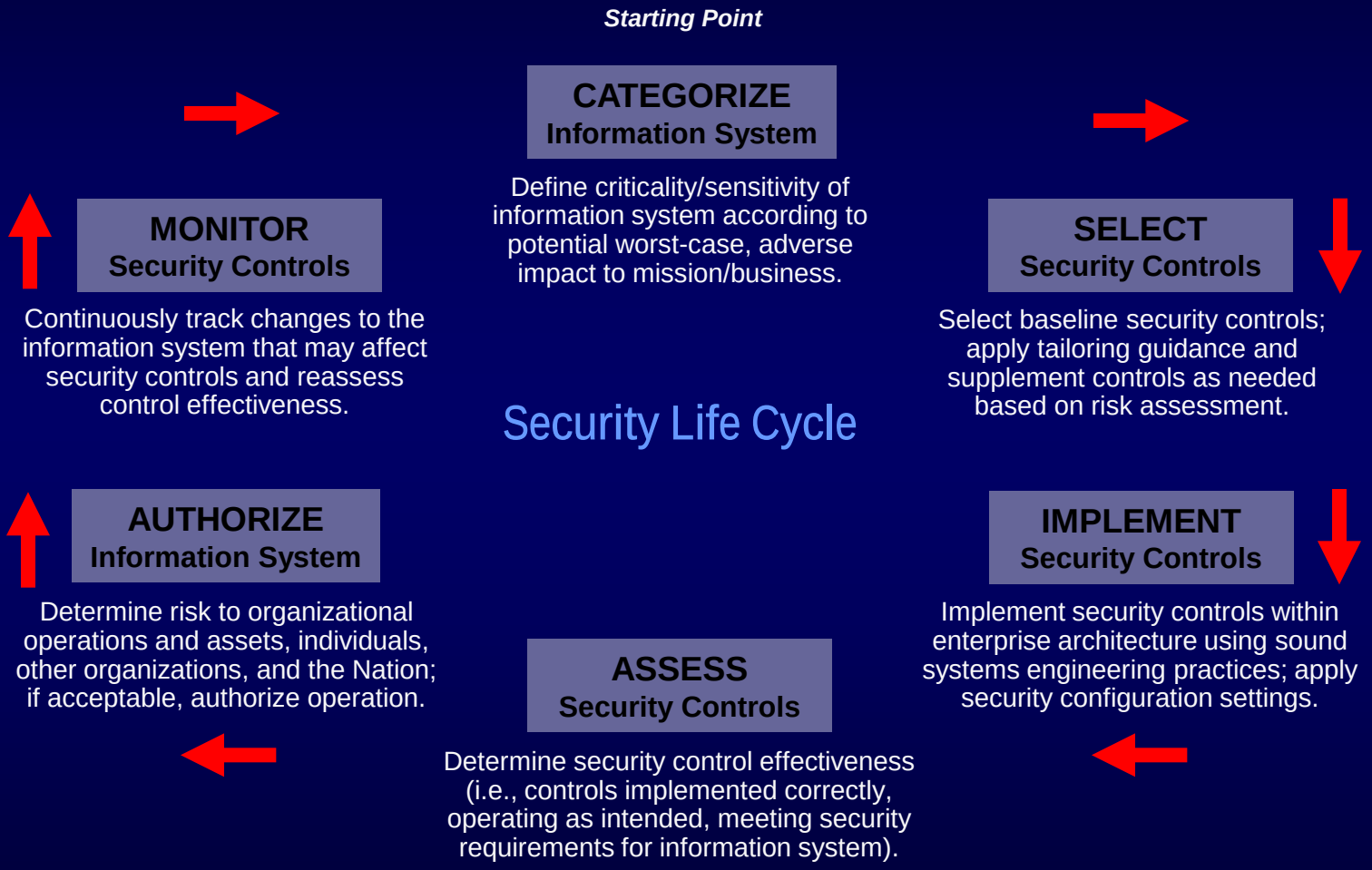
Communicating and sharing risk-related information from the strategic to tactical level, that is from the executives to the operators.



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

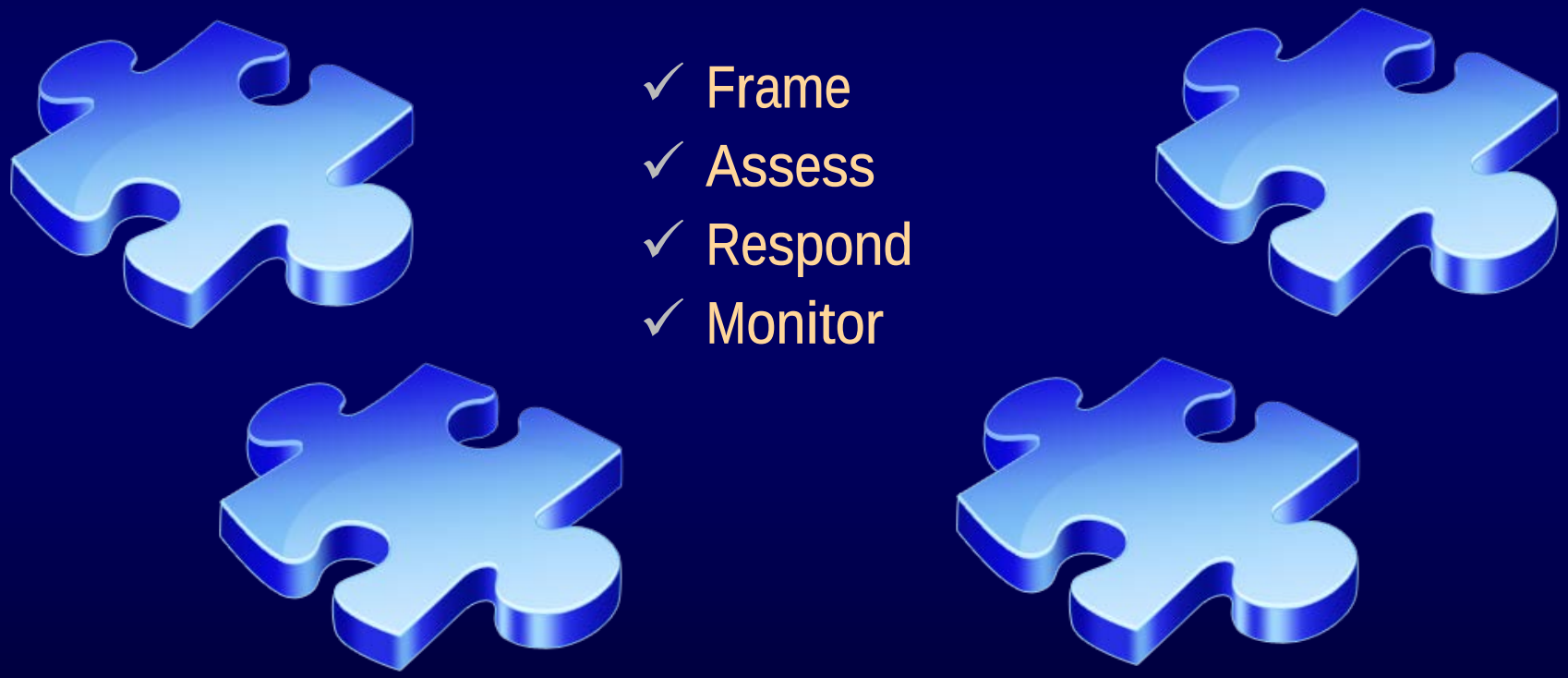
TACTICAL (OPERATIONAL) RISK FOCUS

Risk Management Framework



Managing risk.

Requires having a good framework…



- ✓ Frame
- ✓ Assess
- ✓ Respond
- ✓ Monitor

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.

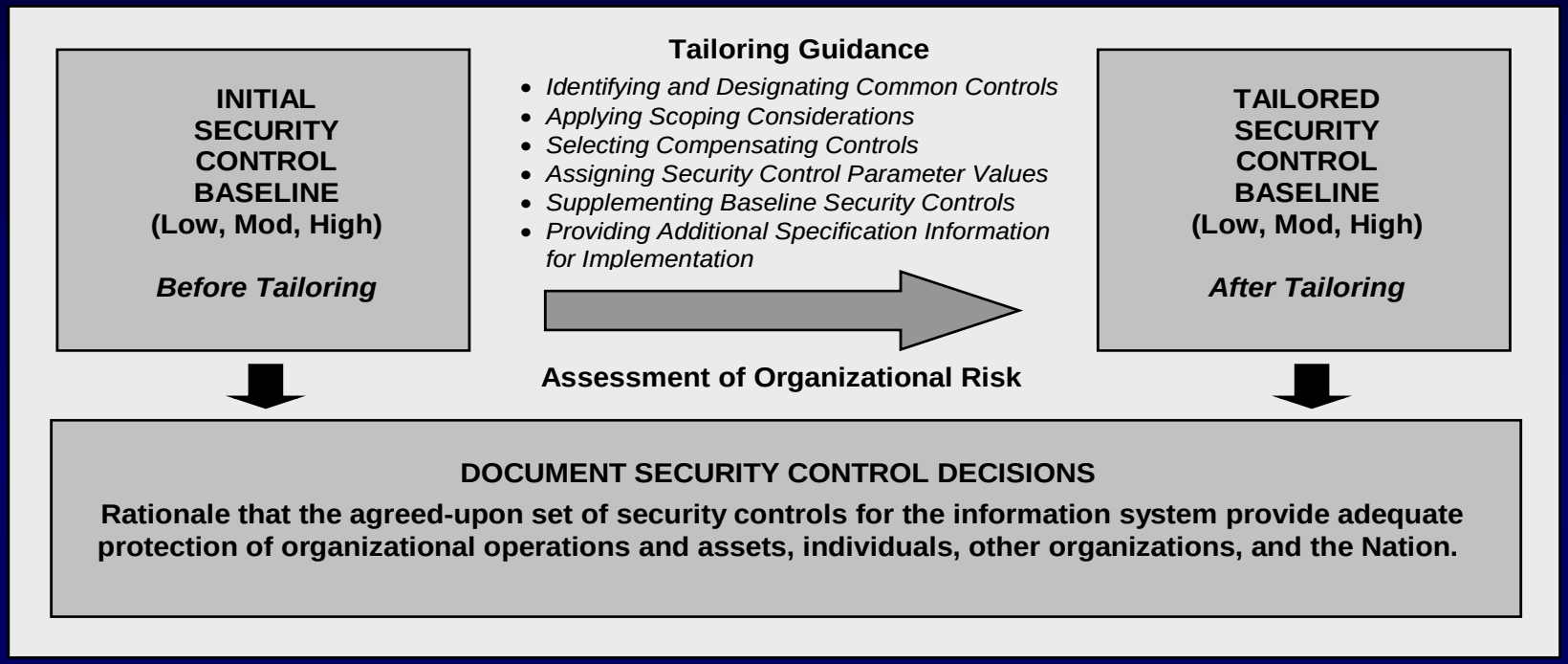
Expanded Tailoring Guidance
(2 of 2)

- 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).

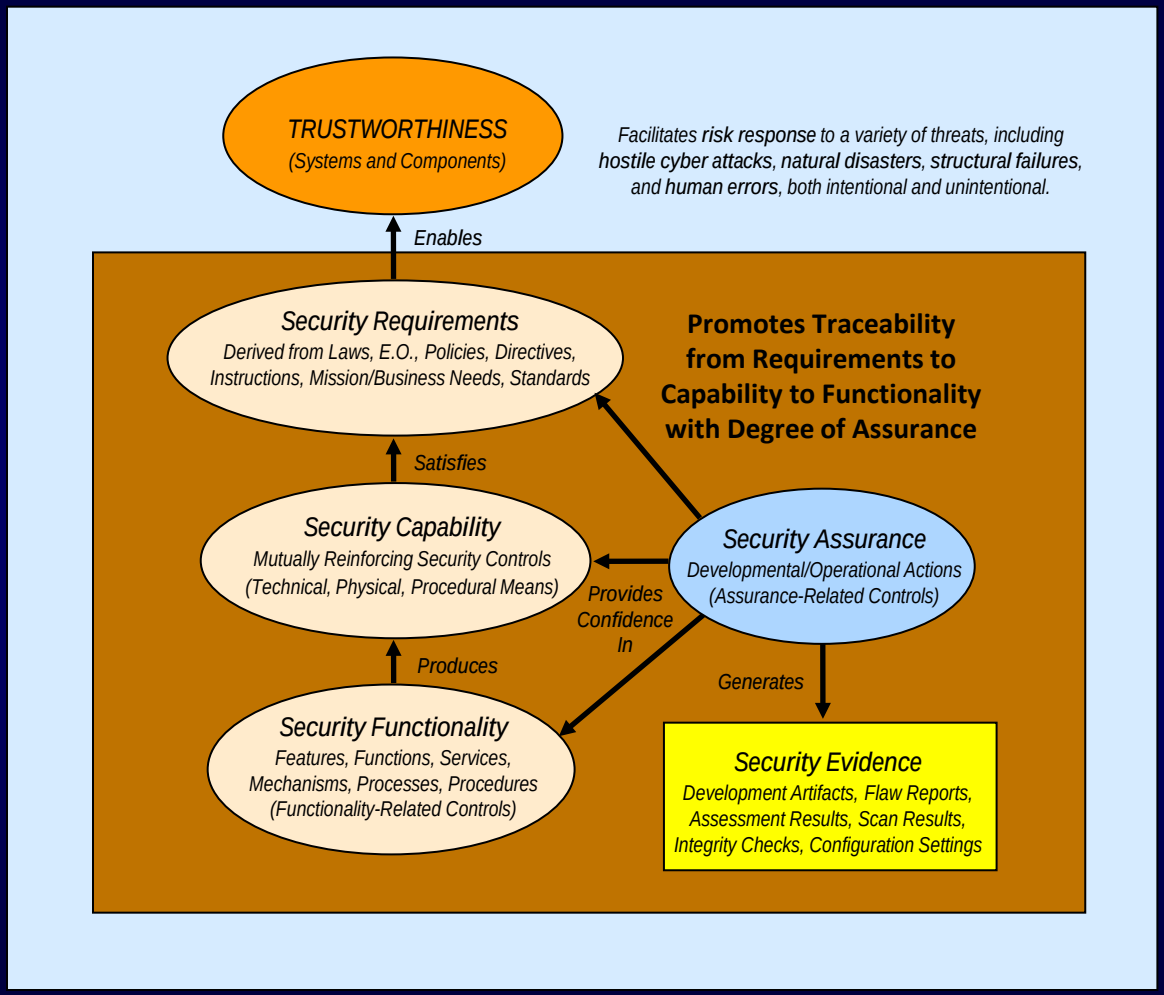
Functionality and Assurance.

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

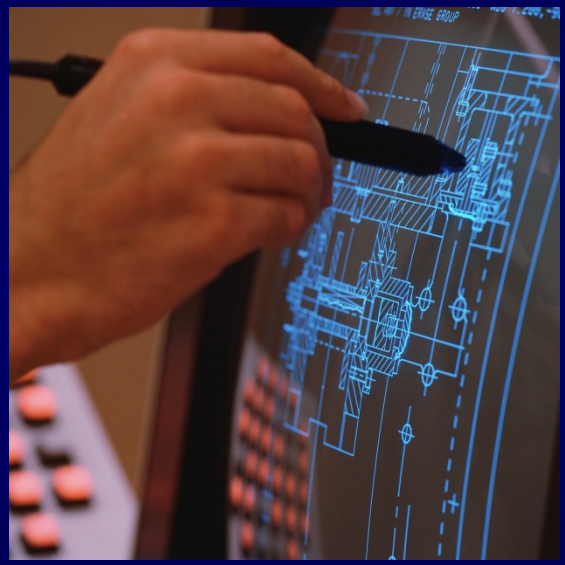
- Appendix E has been completely revised and reworked.
- The *minimum* required assurance is provided by implementation of the appropriate baseline set of controls.
- The *assurance-related* controls for each baseline are provided in tables E-1, E-2, and E-3.
- Additional assurance-related controls are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

New 800-53 Rev 4 Controls

- Cloud-related controls

  SA-9 (5) – External Information Systems | Processing, Storage, and Service Location

- SOA-related controls

  IA-9 – Service Identification and Authentication

- Mobile device-related controls

  AC-19 (8) – Access Control for Mobile Devices | Remote Purging of Information

  AC-19 (7) – Access Control for Mobile Devices | Central Management of Mobile Devices

New 800-53 Rev 4 Controls

- Resiliency-related controls (against the APT)
  - SC-37 (1) – Distributed Processing and Storage | Diversity
  - SI-14 – Non-Persistence
  - SC-44 – Detonation Chambers
  - IR-10 – Integrated Information Security Analysis Team
  - IA-10 – Adaptive Identification and Authentication
  - IA-11 – Reauthentication

Privacy – Appendix J
(1 of 2)

- Privacy and security are complementary and mutually reinforcing.
- Appendix J complements security controls in Appendix F.
- Privacy control families are the same as those in the FEA Security and Privacy Profile, v3, September 2010.
- Appendix J is based on:
  - Fair Information Practice Principles from Privacy Act of 1974;
  - E-Government Act of 2002, Section 208; and
  - Privacy-related OMB guidance.

Privacy – Appendix J
(2 of 2)

- Objective of Appendix J is to promote closer cooperation between privacy and security officials.
- Intended for organizational privacy officials (e.g., CPOs) working with:
  - Program managers;
  - Information system developers;
  - Information technology staff; and
  - Information security personnel.
- Apply each control with respect to organization's distinct mission and operational needs based on legal authorities and obligations.

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.

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

Morning Break.

The Fundamentals of Continuous Monitoring

An Integral Part of Risk Management Strategies

Federal Computer Security Program Manager's Forum

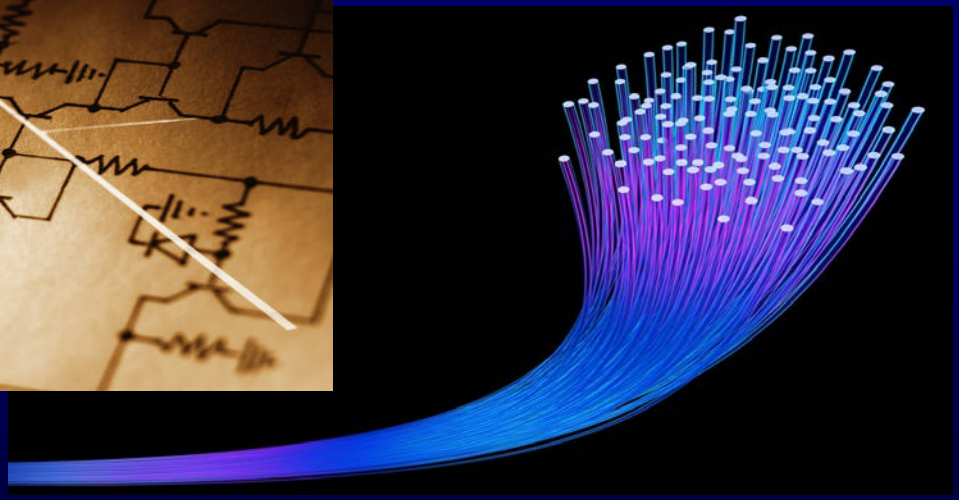
August 8, 2013

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

The federal cyber security strategy…

Build It Right, Continuously Monitor



Before We Monitor – Built It Right

- NIST Special Publication 800-53, Revision 4
  Security and Privacy Controls for Federal Information Systems and Organizations
  April 30, 2013

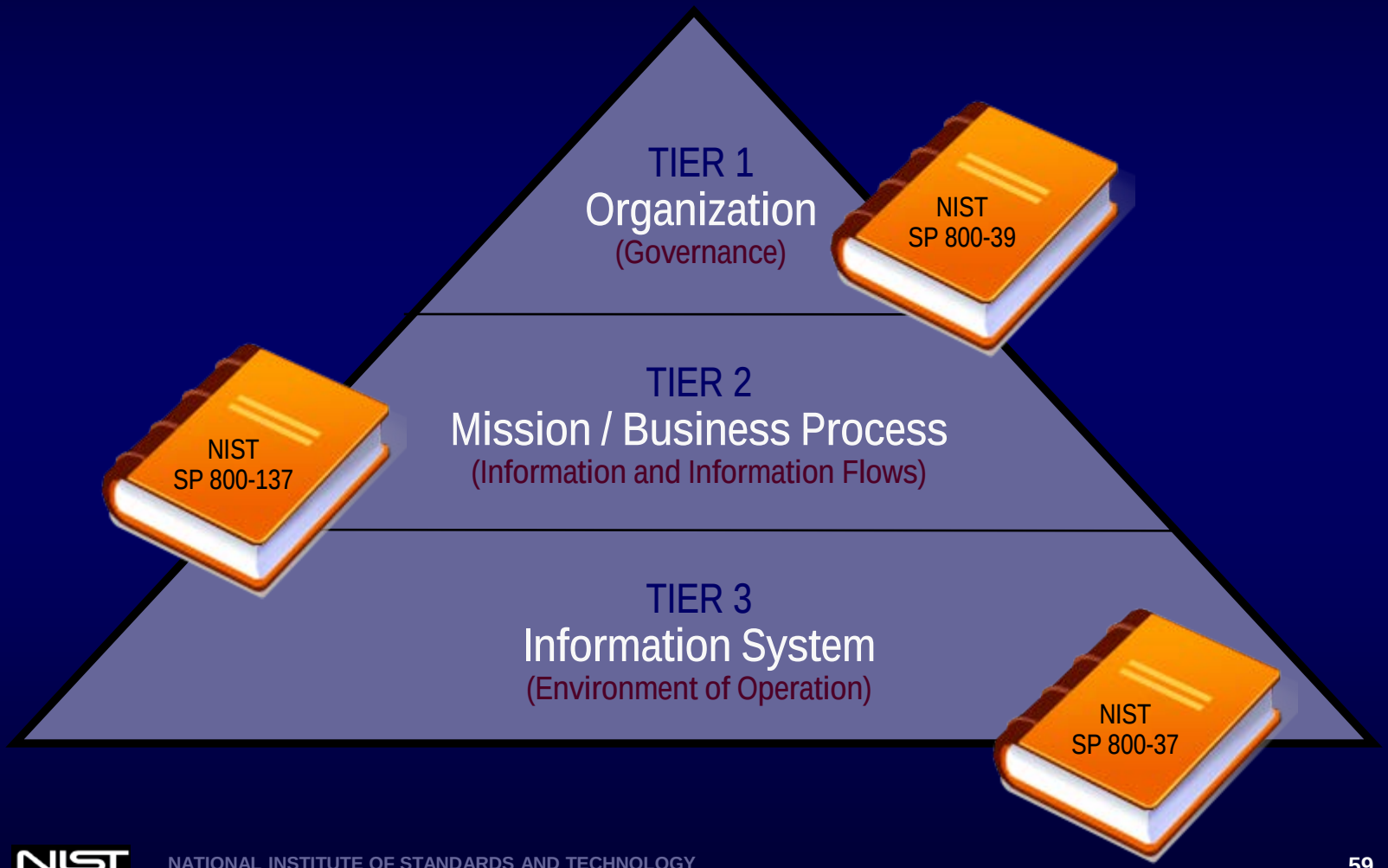
- NIST Special Publication 800-160
  Security Engineering Guideline
  Initial Public Draft – Winter 2013

- NIST Special Publication 800-161
  Supply Chain Risk Management Guideline
  Initial Public Draft – Summer 2013

And after we build it right.

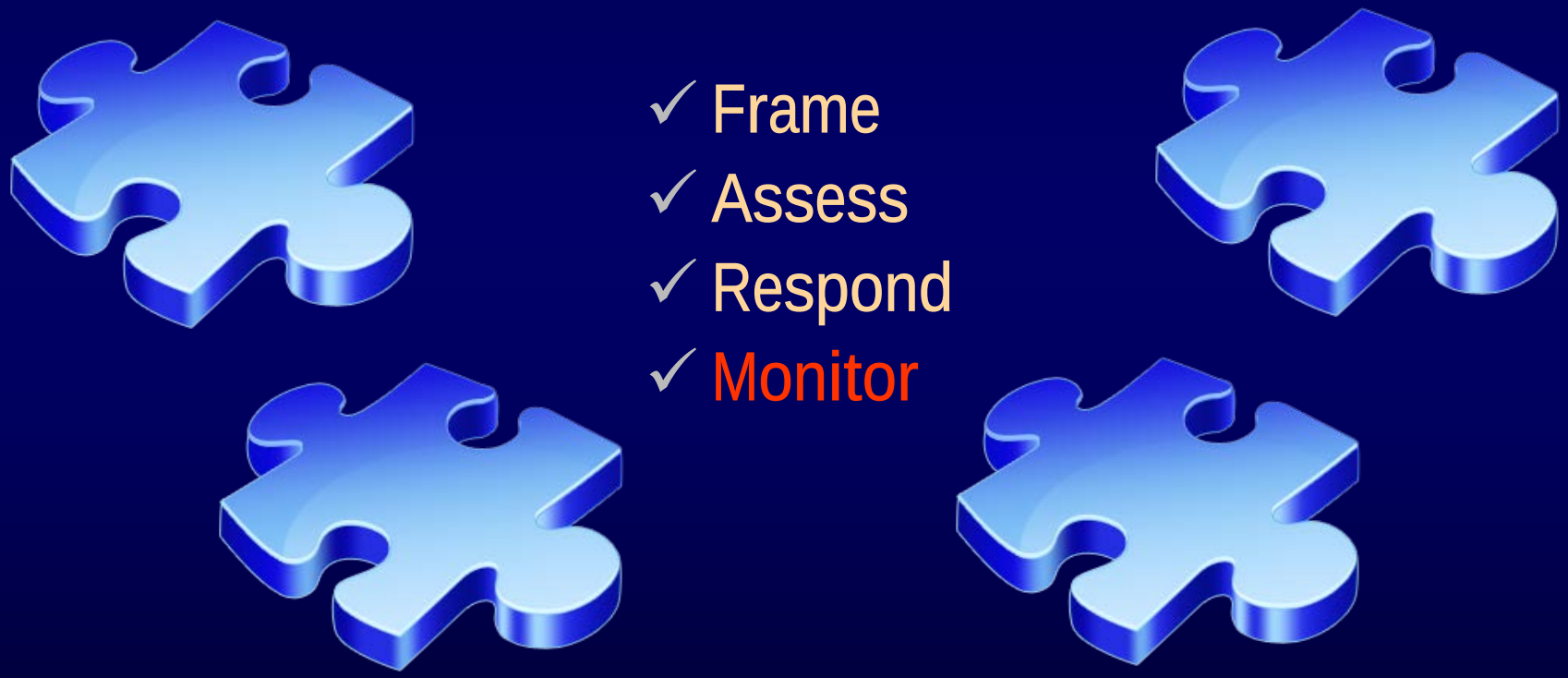
What next?

Enterprise-Wide Risk Monitoring



Continuous Monitoring.

Part of a comprehensive risk management strategy…



- ✓ Frame
- ✓ Assess
- ✓ Respond
- ✓ Monitor

Continuous Monitoring

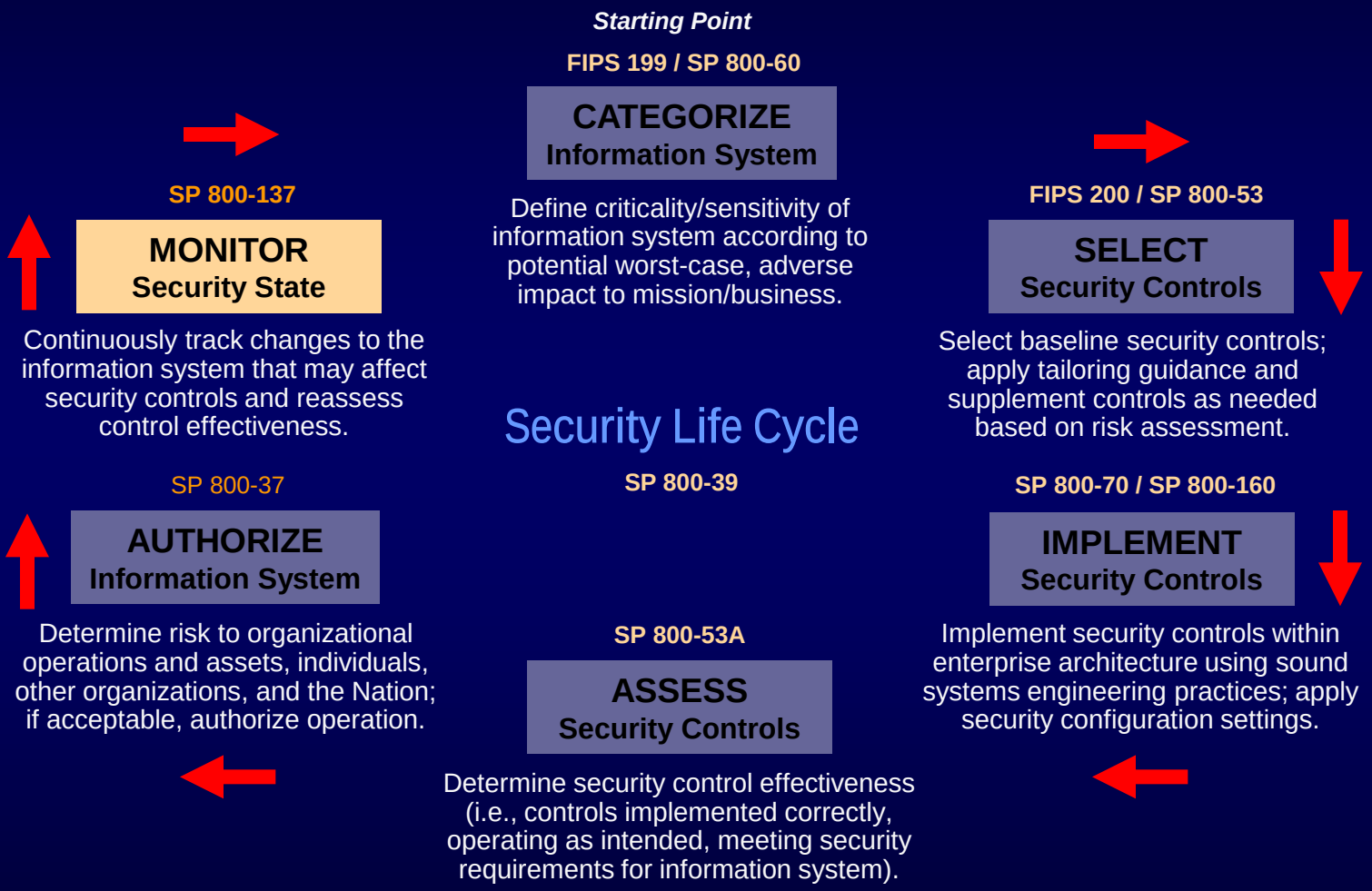
- Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.
- Note: The terms *continuous* and *ongoing* in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information.

Continuous Monitoring

- Determine effectiveness of risk responses.
- Identify changes to information systems and environments of operation.
- Verify compliance to federal legislation, Executive Orders, directives, policies, standards, and guidelines.

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

Continuous Monitoring in the RMF



Continuous Monitoring Core Principles

- Continuous monitoring concepts are applied across all three tiers in the risk management hierarchy defined in NIST Special Publication 800-39.
- Continuous monitoring applies to all security controls implemented in organizational information systems and the environments in which those systems operate.
- Continuous monitoring includes both automated and procedural (manual) methods.

Continuous Monitoring Core Principles

- Continuous monitoring concepts are applied across all three tiers in the risk management hierarchy defined in NIST Special Publication 800-39.
- Continuous monitoring applies to all security controls implemented in organizational information systems and the environments in which those systems operate.
- Continuous monitoring includes both automated and procedural (manual) methods.

Continuous Monitoring Core Principles

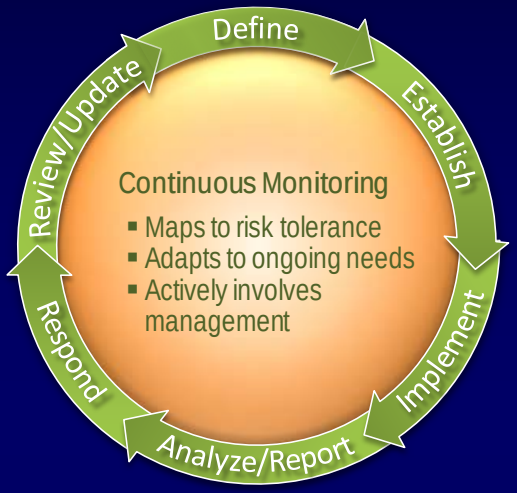
- Organizations define and document in their continuous monitoring strategies, the frequency of security control monitoring and the rigor with which the monitoring is conducted—one size does *not* fit all.
- Continuous monitoring supports the risk management process defined in NIST Special Publication 800-39:
  - Providing information to authorizing officials for a range of potential risk response decisions (i.e., accept, reject, share, transfer, or mitigate risk) in accordance with organizational *risk tolerance* and *mission/business priorities*.

Continuous Monitoring Core Principles

- Continuous monitoring requirements are the same for federal agencies and any external service providers (e.g., cloud service providers) used by the agencies.
- Continuous monitoring programs are more effective if conducted on information technology infrastructures that have been strengthened and are more resilient—

"Build It Right, Continuously Monitor"

Continuous Monitoring Process Steps



- Define CM strategy.
- Establish CM program.
  - Determine metrics.
  - Determine monitoring frequencies.
  - Develop CM architecture.
- Implement the CM program.
- Analyze security-related information and report findings.
- Respond with mitigation actions OR reject, share, transfer, or accept risk.
- Review and update CM strategy and program.

OMB Policy Changes

2012 FISMA Reporting Guidance

OMB Memorandum-12-20

http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-20.pdf

Question #29

- Continuous monitoring programs 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 and Special Publication 800-137.

Bottom Line: Rather than 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 Tips

- Don’t collect too much information during the monitoring process – information collected should be actionable.
- Retain as much information as possible from the monitoring process at the local level – only pass information up the management chain if needed by decision makers.
- Be careful not to over simplify information collected during the monitoring process – dashboards can be deceiving and underestimate mission risk.

What is the DHS Continuous Diagnostics and Mitigation Program?

A subset of a comprehensive continuous monitoring and risk management program.

On The Policy Horizon

- Revision of OMB Circular A-130, Appendix III.
- New OMB Continuous Monitoring Policy.
- Joint Continuous Monitoring Working Group Concept of Operations

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

Question and Answer Session.

Time to hear from you…

Lunch.

Reconvene at 1:15 PM

RMF Case Studies Panel.

Leo Scanlon, NARA (Moderator)
Tim Ruland, Census Bureau
Pete Gouldmann, State Department
Melinda Rogers, Department of Justice
Earl Crane, Promontory
Peter Williams, Booz Allen Hamilton

Afternoon Break.

Ongoing Authorization Case Studies Panel.

Jeff Eisensmith, DHS (Moderator)

Emery Csulak, DHS

Sharon Jurado, TSA

Alex Ruiz, ICE

Concluding remarks.