

# Fundamentals of Continuous Monitoring

An Integral Part of Risk Management Strategies

*and Considerations for*

**SP 800-53 Revision 4**

Federal Computer Security Program Managers' Forum  
Annual Offsite

June 5, 2013

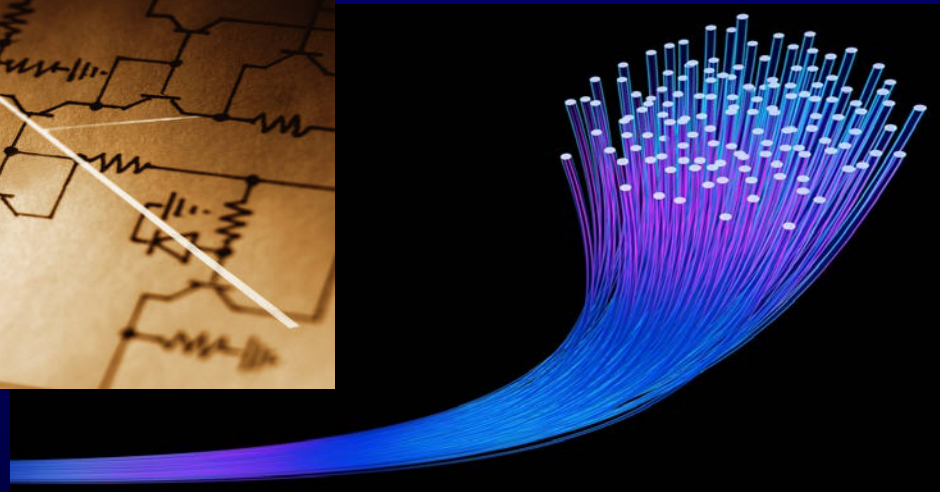
L. Arnold Johnson

*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 – Fall 2013



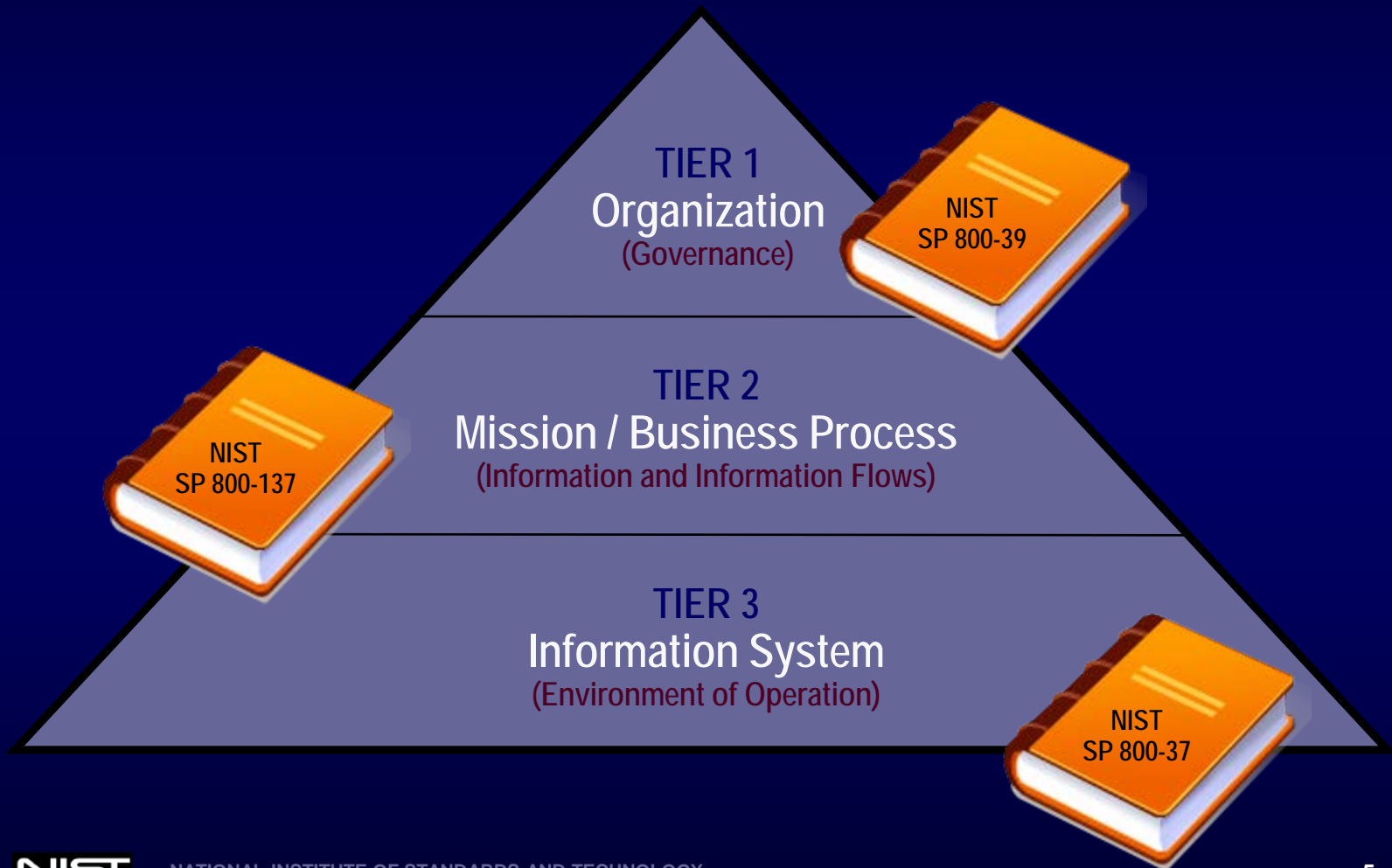
- NIST Special Publication 800-161  
*Supply Chain Risk Management Guideline*  
Initial Public Draft – Summer 2013



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.





# OMB Policy Changes

2012 FISMA Reporting Guidance  
*OMB Memorandum-12-20*

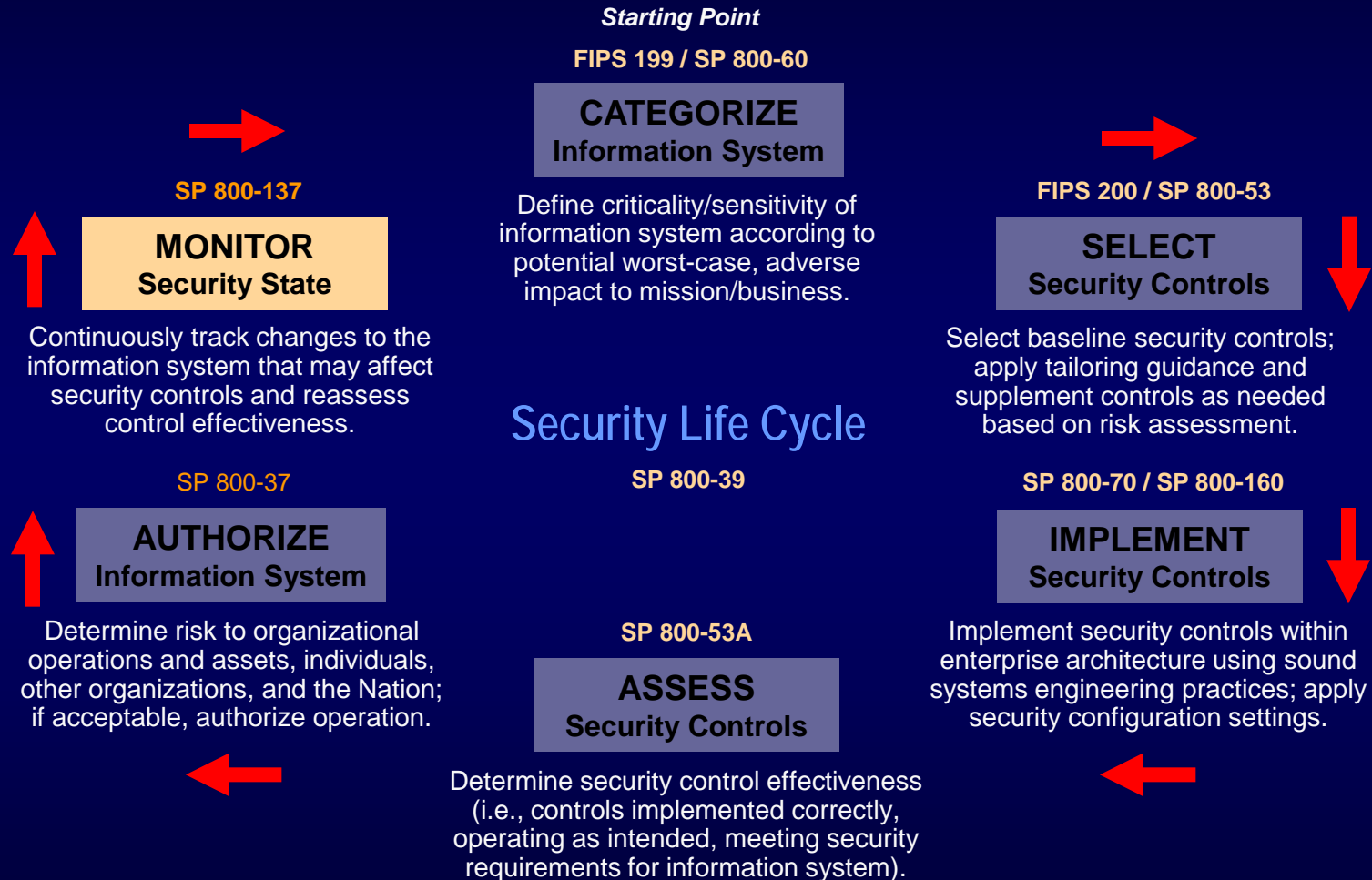
<http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-20.pdf>

## *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 in the RMF



# Continuous Monitoring Publications

- **NIST Special Publication 800-39**  
*Managing Information Security Risk:  
Organization, Mission, and Information System View*
- **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*
- **NIST Special Publication 800-137**  
*Information Security Continuous Monitoring for  
Federal Information Systems and Organizations*



# 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*.

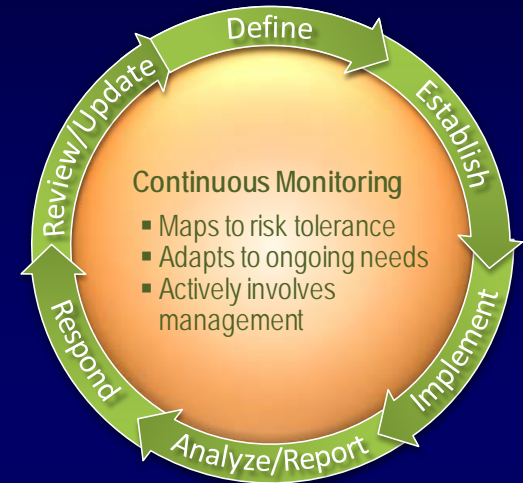
# Continuous Monitoring Core Principles

- 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



# Continuous Monitoring Process

## Develop strategy

- Focus on situational awareness for:
  - Risk management decisions
    - On-going authorization decisions
  - Asset and configuration management
  - Federal and organizational reporting requirements
- In addition to the original objective of monitoring for control effectiveness, the monitoring strategy also supports security posture monitoring (e.g., risk scoring tools)
- The continuous monitoring strategy itself is also monitored to ensure monitoring and reporting frequencies remain aligned with threats and organizational risk tolerance



# Continuous Monitoring Process

## *Establish Measures and Metrics*

- Measures = all the security-related information from assessments and monitoring (manually *and* automatically generated)
- Metrics = measures organized into meaningful information that supports decision making
- Multiple measures may support one metric
- Example: A organization wants to monitor status of authorized and unauthorized components on a network.
  - The organization defines the metric as the % of unauthorized components connected to the network at a specified frequency (hourly, daily, weekly, etc.)
  - Measures to support this metric may include security-related information regarding physical asset locations, logical asset locations (subnets/IP addresses), MAC addresses, system association, policies/procedures for network connectivity, etc.

# Continuous Monitoring Process

## *Establish Monitoring and Assessment Frequencies*

- Monitor metrics/measures and **each** control with varying frequencies based on:
  - Control volatility
  - Organizational and system risk tolerance
  - Current threat and vulnerability information
  - System categorization/impact levels
  - Controls with identified weaknesses
  - Controls or system components providing critical security functions
  - Risk assessment results
  - Output of monitoring strategy reviews
  - Reporting requirements
- Multiple requirements within a control may have to be monitored with differing/varying frequencies.

# Continuous Monitoring Process

## *Implement the Continuous Monitoring Program*

- All controls are monitored and/or assessed (common, system, and hybrid controls)
- Tier 2 - Implement tools and processes associated with common controls and organization-wide monitoring (IDPS, vulnerability scanning, configuration management, asset management, etc.)
  - Organization-wide monitoring will likely pull security-related information from the system level
- Tier 3 – Implement tools and processes pushed down from Tier 2 and fill in any gaps at the system level
- Tiers 2 and 3 – Organize/prepare data for analysis

# Continuous Monitoring Process

## *Analyze Data and Report Findings*

- Data is analyzed in the context of:
  - Stated organizational risk tolerance
  - Potential impact of vulnerabilities on organizational and mission/business processes
  - Potential impact/costs of mitigation options
- Tier 3
  - Conducts initial analysis
  - Reports findings/provides recommendations to Tiers 2 and/or 1
- Tiers 1 and 2
  - Determine aggregate security status of effectiveness of controls (including common controls) for all systems in meeting organizational information security requirements

# Continuous Monitoring Process

## *Respond to Findings*

- Determine if the organization will take remediation action, accept the risk, avoid/reject the risk, or transfer the risk (all tiers)
- Tier 1 Specific Response - Changes to strategy or policies
- Tier 2 Specific Response
  - Request additional information
  - Changes in procedures
  - Changes in common control implementations
- Tier 3 Specific Response
  - Implementation of additional controls/changes in existing control implementations
  - Additional/more detailed analysis of security-related information
- Suspension or removal of authorization to operation

# Continuous Monitoring Automation:

## The Need for Caution

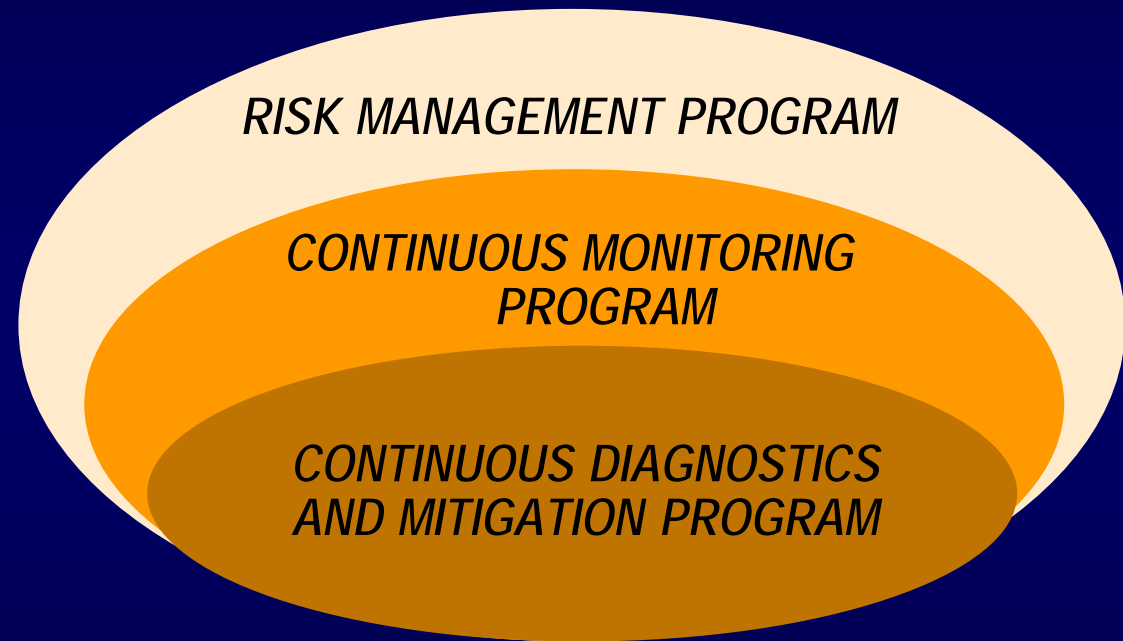
Automated tools may lead to a false sense of security:

- If all controls are **not** taken into account when monitoring, an **incomplete picture of overall security posture** and risk is presented:
  - Risk scores may not be comprehensive, i.e., an automated tool cannot score risks about which it has no information
  - Risk scoring is often based solely on automation of technical controls and thus is **not a substitute for monitoring other essential operational and management controls** nor can it determine how security failures will affect organization functions and mission
- Whether or not monitoring of a control can be automated is **NOT** a criterion for determining the frequency of monitoring

# 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.



# Continuous Monitoring Process

## *Review/Update the Monitoring Strategy/Program*

- Organizations establish a process for reviewing and modifying the strategy
  - Accuracy in reflecting organizational risk tolerance
  - Accuracy of measurements
  - Applicability of metrics
  - Applicability of monitoring frequencies and reporting requirements
- Factors precipitating changes to the strategy may include:
  - Changes to core missions or business processes
  - Significant changes in the enterprise architecture
  - Changes in organizational risk tolerance
  - Changes in threat and/or vulnerability information
  - Increase/decrease in POA&Ms related to specific controls or metrics
  - Trend analyses of status reporting output

# Reviewing and upgrading to SP800-53R4?

*Good time to simultaneously...*

*Review/update the*

*Continuous Monitoring Strategy/Program!*

# Continuous Monitoring Considerations

## 53R4 Changes – CA-2

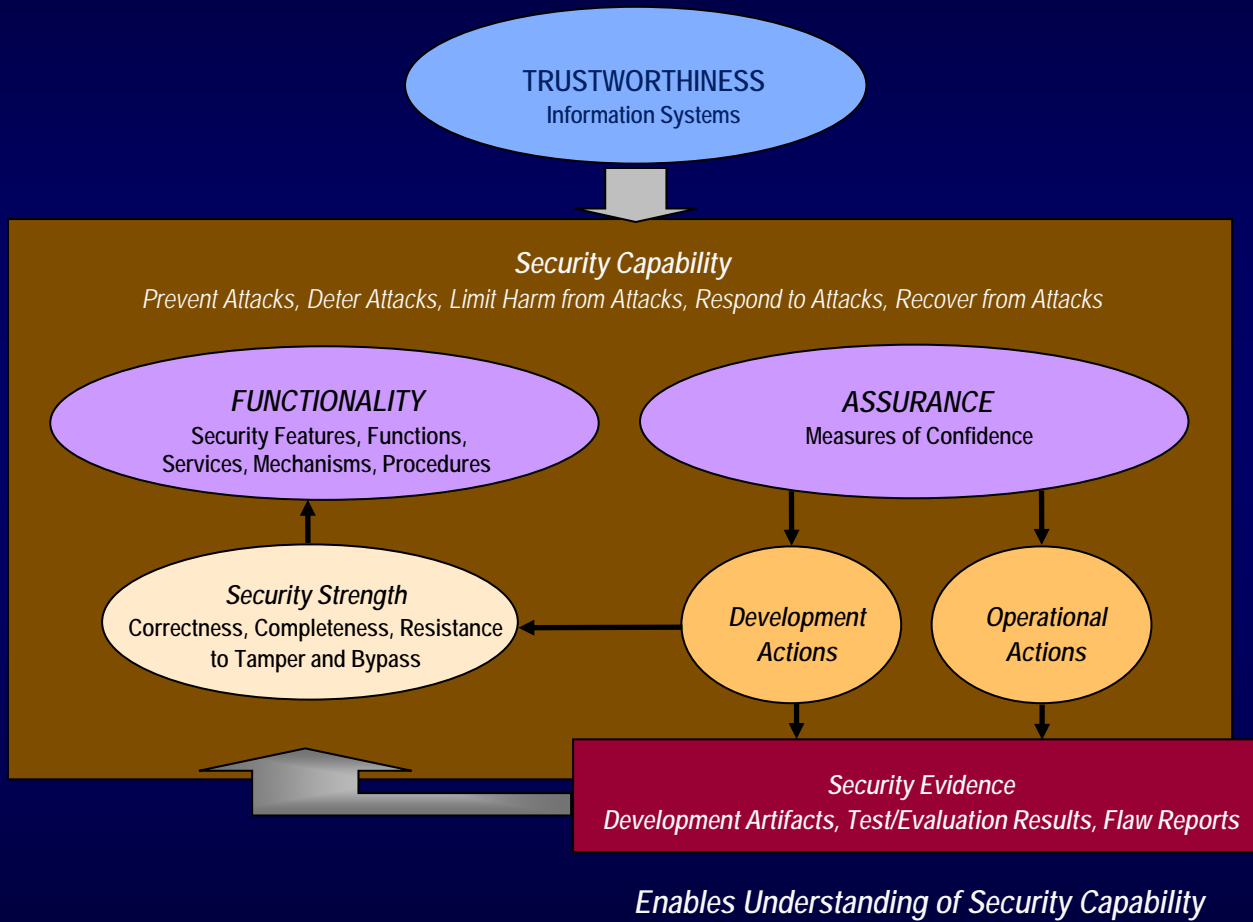
- CA-2 Security Assessments SG specifies:
  - Reasons to assess security controls include “initial and ongoing authorizations” and “continuous monitoring;”
  - Security assessments “provide essential information needed to make risk-based decisions as part of security authorization processes;” and
  - Assessment results from ongoing authorizations and from continuous monitoring may be used to satisfy FISMA annual assessment requirements.
- CA-2 “References” now include SP 800-137

# Continuous Monitoring Considerations

## 53R4 Changes – CA-7...

- CA-7 Continuous Monitoring revised to be consistent with continuous monitoring steps from SP 800-137
  - CE (1) Independent Assessment
  - CE(3) Trend Analysis
- Continuous monitoring-related guidance and “References” added to controls CP-10, SA-4, SI-4, PM-10, PM-15 and many other controls where appropriate

# Assurance and Trustworthiness (53R4)



# Continuous Monitoring Considerations

## 53R4 – Trustworthiness and Assurance

- Continuous monitoring tie-in to Assurance and Trustworthiness in SP 800-53R4 Section 2.6 and Appendix E
- Significant changes to security controls and control enhancements—
- 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.*

# Continuous Monitoring Considerations

## 53R4 – Assurance

- Updated Appendix E discussion on Assurance
  - Revised minimum assurance requirements
  - Identification of minimum assurance controls/CEs in catalog
  - Identification of all assurance controls/CEs in catalog (regardless of whether they are in any 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		

Minimum Assurance Controls for Low Impact Systems

# Continuous Monitoring Considerations

## 53R4 – Security Enhanced Areas

- Insider Threats
- Application Security
- Service Oriented Architectures
- Mobile Devices
- Cloud Computing
- Supply Chain Security
- Software and System Assurance
- Advanced Persistent Threats
- Cross Domain Solutions
- Industrial/Process Control Systems
- Privacy



# Continuous Monitoring Considerations

## 53R4 – New Controls and Enhancements (Examples)

- SOA oriented controls
  - E.g., IA-9 - SERVICE IDENTIFICATION AND AUTHENTICATION
- Mobile device oriented controls
  - E.g., 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*
- Cloud oriented controls
  - E.g., SA-9 (5) - *EXTERNAL INFORMATION SYSTEMS | PROCESSING, STORAGE, AND SERVICE LOCATION*

# Continuous Monitoring Considerations

## 53R4 – Supply Chain Protection

### ■ SA-12 Supply Chain Protection (Base Control)

Control: The organization protects against supply chain threats to the information system, system component, or information system service by employing [*Assignment: organization-defined security safeguards*] as part of a comprehensive, defense-in-breadth information security strategy.

*(Control Enhancements)*

- ACQUISITION STRATEGIES / TOOLS / METHODS
- SUPPLIER REVIEWS
- LIMITATION OF HARM
- ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE
- USE OF ALL-SOURCE INTELLIGENCE
- OPERATIONS SECURITY

# Continuous Monitoring Considerations

## 53R4 – Software and System Assurance

- SA-15 Development Process, Standards, Tools
- SA-16 Developer-Provided Training
- SA-17 Developer Security Architecture / Design
- SA-18 Tamper Resistance and Detection
- SA-19 Component Authenticity
- SA-20 Customized Development of Critical Components
- SA-21 Developer Screening

# Continuous Monitoring Considerations

## 53R4 – APT and Resiliency Controls

- SC-27 Platform-Independent Applications
- SC-29 Heterogeneity
- SC-30 Concealment and Misdirection
- SC-34 Non-Modifiable Executable Programs
- SC-36 Distributed Processing and Storage
- SC-37 Out-of-Band Channels
- SC-38 Operations Security
- SC-44 Detonation Chambers

# Built It Right *and* Continuously Monitor...



Strengthening  
IT Infrastructure

*ARCHITECTURE, ENGINEERING,  
SYSTEM RESILIENCY*



Monitoring  
IT Infrastructure

*AUTOMATED AND PROCEDURAL  
TECHNIQUES AND METHODS*

Has your organization achieved the appropriate balance?

# 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*

Kevin Stine  
(301) 975-4483  
kevin.stine@nist.gov

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

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

Web: [csrc.nist.gov/sec-cert](http://csrc.nist.gov/sec-cert)

Comments: [sec-cert@nist.gov](mailto:sec-cert@nist.gov)