# MITRE Privacy Continuous Monitoring Framework

## MITRE Privacy Engineering

8 October 2019

For questions or comments regarding this document, please contact MITRE at privacy@mitre.org

# Agenda

- Purpose and approach
- Privacy continuous monitoring requirements
- Privacy continuous monitoring approach
- Organizational levels for continuous monitoring
- Privacy Continuous Monitoring Considerations for Each Organizational Level
- Identifying and Maturing an Organization’s Privacy Continuous Monitoring Posture
- Privacy Methods and Tools to Use for Systems Privacy Continuous Monitoring Activities
- Additional Privacy Continuous Monitoring Considerations
- Conclusion

# Purpose and Approach

- **OMB Circular A-130,* *Managing Information as a Strategic Resource*, requires every US federal government agency to conduct privacy continuous monitoring and to have a privacy continuous monitoring program and strategy.**
- **This document leverages NIST Special Publication 800-137,** *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* to identify privacy-specific activities to adopt to implement privacy continuous monitoring.**

* Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, July 27, 2016

**NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* September 2011

# Privacy Continuous Monitoring Requirements

- **These concepts as defined in OMB Circular A-130* are now requirements for every agency:**
  - Privacy continuous monitoring: Maintaining ongoing awareness of privacy risks and assessing privacy controls at a frequency sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.
  - Privacy continuous monitoring program: Agency-wide program that implements the agency’s privacy continuous monitoring strategy.
  - Privacy continuous monitoring strategy: Formal document that catalogs the available privacy controls implemented at an agency and ensures that the controls are effectively monitored on an ongoing basis.

*OMB Circular A-130, *Managing Information as a Strategic Resource*, July 27, 2016

# Privacy Continuous Monitoring Approach

- **Privacy continuous monitoring maintains ongoing awareness of privacy risks and assesses administrative, technical, and physical safeguards (privacy controls) employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks.**
- **The privacy continuous monitoring strategy catalogs the available privacy controls and ensures that the controls are effectively *monitored* on an ongoing basis.**
- **The privacy continuous monitoring program conducts *assessments* to determine whether the controls are *implemented correctly*, *operating as intended, and sufficient.***

# Organizational Levels for Continuous Monitoring

- **NIST SP 800-137* uses three levels to address information security continuous monitoring from varying organizational perspectives.**
- **The three organizational levels in NIST SP 800-137 (defined below) can be applied to privacy continuous monitoring as well.**
  - Level 1: Organization
    - Overarching guidance is provided by Senior leaders that frames risk for the particular environment – what is the risk and the risk tolerance level.
    - Advisors should have in mind the risk tolerance level when looking at continuous monitoring approaches.

*NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* September 2011

# Organizational Levels for Continuous Monitoring (cont.)

- Level 2: Mission/Business processes
  - Level 2 criteria for continuous monitoring are defined by how core mission/business processes are prioritized with respect to the overall goals and objectives of the organization, types of information needed to successfully execute the stated mission/business processes, and organization-wide information security program strategy.
  - Controls that address the establishment and management of the organization's information security program are examples of Level 2 security controls.

# Organizational Levels for Continuous Monitoring (cont.)

- Level 3: Information systems
  - Processes identified at Level 2 are decomposed for system-level continuous monitoring.
  - Level 3 includes assessing and monitoring controls implemented at the system level to ensure that they are implemented correctly, operate as intended, produce the desired outcome with respect to meeting security requirements for the system, and continue to be effective over time.
  - Level 3 status reporting includes system security alerts, security incidents, and identified threat activities.
  - Level 3 addresses requirements development, acquisitions, purchasing, sourcing, supply chain management, and system testing.

# Privacy Continuous Monitoring Considerations for Each Organizational Level

# Privacy Continuous Monitoring Considerations Level 1: Organization

- **Level 1 is about framing the risk, identifying what an organization's risk tolerance is, and giving the rationale for what the organization's risk tolerance is**
  - Risk tolerance should be linked to mission/business objectives
- **Risk advisors' recommendations go to an Authorizing Official (AO)**
- **Risk tolerance information should be documented in continuous monitoring strategies**
- **Level 1 privacy continuous monitoring considerations include:**
  - Privacy risk tolerance should be linked to mission/business objectives just as security risk tolerance should be linked to those objectives
  - Privacy risk tolerance information should be documented in the privacy continuous monitoring strategy or in a joint cybersecurity and privacy continuous monitoring strategy

# Privacy Continuous Monitoring Considerations Level 2: Mission/Business Processes

- **Level 2 addresses processes used to help manage risk defined in Level 1**
- **Level 2 privacy continuous monitoring considerations include addressing privacy continuous monitoring within organization-wide policies and procedures on the following topics:**
  - Privacy program organization (including roles and responsibilities of privacy leadership and the workforce)
  - PII inventory
  - Privacy risk management strategy
  - Privacy testing and monitoring
  - Privacy training and threat awareness program
  - Contacts with privacy groups and associations
  - Privacy threat identification and assessment

# Privacy Continuous Monitoring Considerations Level 3: Information Systems

- **Level 3 focuses on system activity**
- **Level 3 privacy continuous monitoring considerations for systems include:**
  - PII inventory
  - Privacy risk assessments
  - Privacy requirements definition and testing
  - Privacy threat identification and monitoring
  - Privacy incident response
  - Privacy metrics and reporting

# Identifying and Maturing an Organization’s Privacy Continuous Monitoring Posture

# Identifying and Maturing an Organization's Privacy Continuous Monitoring Posture

- **MITRE's Privacy Maturity Model* can be used by an organization to identify the location of the different types of privacy continuous monitoring activities within their privacy program.**
- **Organizations can then use the Privacy Maturity Model to identify the current and target maturity level of their privacy continuous monitoring activities for each element of the organization's privacy program.**
- **The organization should discuss plans to mature their privacy continuous monitoring capabilities in their privacy continuous monitoring strategy or another planning document.**
- **The following slides provide information on:**
  - The Privacy Maturity Model structure
  - Types of privacy continuous monitoring activities and their location in privacy programs based on the Privacy Maturity Model structure.

*MITRE Corporation, *MITRE Privacy Maturity Model*, http://www.mitre.org/privacy

# Privacy Maturity Model:* Privacy Program Elements

**Comprehensive government privacy programs consist of seven main elements described in the table below.**

| Privacy Program Element | Description |
|---|---|
| 1.0: Leadership & Organization | Providing organizational support for privacy program priorities and initiatives |
| 2.0: Privacy Risk Management | Using methods and processes to identify, assess, prioritize, and manage privacy risk, including within IT investment, acquisition, and contract management processes. |
| 3.0: Engineering & Information Security | Incorporating privacy into the enterprise systems engineering approach and integrating with cybersecurity |
| 4.0: Incident Response | Managing and responding to privacy incidents, including breaches |
| 5.0: Individual Participation, Transparency & Redress | Informing data subjects and the public regarding information about individuals the agency collects and uses, and how the public may pursue inquiries and complaints |
| 6.0: Privacy Training & Awareness | Establishing and maintaining workforce training and a culture of privacy awareness |
| 7.0: Accountability | Enforcing the responsibility of the organization to implement privacy principles and requirements and to respond to concerns expressed by individuals and the general public |

*MITRE Corporation, *MITRE Privacy Maturity Model*, http://www.mitre.org/privacy. Elements based on Federal CIO Council Privacy Committee White Paper entitled *Best Practices: Elements of a Federal Privacy Program*, June 30, 2010

# Privacy Maturity Model:* Privacy Program Sub-Elements

## The sub-elements for each privacy program element within a comprehensive privacy program are listed in the table below.

| 1.0 Leadership & Organization | 2.0 Privacy Risk Management | | 3.0 Engineering & Information Security | 4.0 Incident Response | 5.0 Individual Participation, Transparency, & Redress | 6.0 Privacy Training & Awareness | 7.0 Accountability |
|---|---|---|---|---|---|---|---|
| 1.1 Program Organizational Structure | 2.1 Regulations Development | 2.9 Data Quality & Integrity | 3.1 Integration into Systems Engineering Process | 4.1 Incident Management Procedures | 5.1 Dissemination of Privacy Program Information | 6.1 Workforce Training | 7.1 Rules of Behavior Acknowledgement |
| 1.2 Program Design and Strategy | 2.2 Privacy Policy, Procedures, and Standards | 2.10 PII Retention, Disposition, & Destruction | 3.2 Cybersecurity Coordination | 4.2 Incident Notification & Reporting | 5.2 Privacy Notices | 6.2 Privacy Awareness Communications | 7.2 Internal & External Reporting |
| 1.3 Program Privacy Principles | 2.3 PII Inventory, Categorization, & Minimization | 2.11 PII Used in Non-Operational Environments & Research | 3.3 Authority to Connect (ATO) Analysis | 4.3 Response Capabilities | 5.3 Consent | 6.3 Internal Online Presence | 7.3 Privacy Monitoring and Auditing |
| 1.4 Privacy Program Governance | 2.4 Project/Initiative Start-Up Consults | 2.12 Internal Use | 3.4 Privacy Control Selection | 4.4 High-Impact Privacy Incident Response Team | 5.4 Manage Complaints & Inquiries | | 7.4 Incorporate Lessons Learned |
| 1.5 Privacy Program Management | 2.5 Privacy Risk & Impact Assessments | 2.13 Information Sharing | 3.5 Privacy in Emerging Technologies | | 5.5 Individual Access | | |
| 1.6 Resource Management | 2.6 System of Records Notice | 2.14 Oversight and Monitoring Planning | | | 5.6 Amendment, Correction, & Redress | | |
| 1.7 Stakeholder Coordination | 2.7 Legal Agreements | 2.15 Government Privacy Changes Monitoring | | | 5.7 Public Facing Online Presence | | |
| 1.8 Outreach and Collaboration | 2.8 Accounting of Disclosures | 2.16 IT Investment, Acquisition, & Contractor Management | | | | | |
| | | 2.17 Privacy Risk & Issue Tracking | | | | | |

*MITRE Corporation, *MITRE Privacy Maturity Model*, http://www.mitre.org/privacy.

# Privacy Continuous Monitoring Activities in the Privacy Program (1 of 3)

**Using the Privacy Maturity Model structure, privacy continuous monitoring activities should be included in the privacy program sub-elements listed in the table below.**

| Level | Privacy Maturity Model Sub-Elements |
|---|---|
| Level 1: Organization's Risk Tolerance | 7.3: Privacy Monitoring and Auditing – Organization risk tolerance is documented in the organization's privacy continuous monitoring strategy |
| Level 2: Mission/ Business Processes That Support Risk Management Across the Organization (continued on next page) | 1.1: Program Organizational Structure<br>1.2: Program Design and Strategy – includes addressing organizational risk tolerance level as part of privacy program strategy<br>1.3: Program Privacy Principles<br>1.4: Privacy Program Governance<br>1.5: Privacy Program Management<br>1.6: Resource Management<br>1.7: Stakeholder Coordination<br>1.8: Outreach and Collaboration -- includes contact with appropriate external organizations to obtain current privacy threat information |

# Privacy Continuous Monitoring Activities in the Privacy Program (2 of 3)

**Using the Privacy Maturity Model structure, privacy continuous monitoring activities should be included in the privacy program sub-elements listed in the table below.**

| Level | Privacy Maturity Model Sub-Elements |
|---|---|
| Level 2: Mission/ Business Processes That Support Risk Management Across the Organization (continued from previous page) | 2.2: Privacy Policy, Procedures, and Standards – includes addressing privacy continuous monitoring in appropriate organization-wide policies, procedures, and standards<br>2.3: PII Inventory, Categorization, & Minimization – includes maintaining an accurate organization-wide PII inventory<br>2.5: Privacy risk and impact assessments – includes organization-wide privacy threat assessment<br>2.14: Oversight and monitoring planning – includes addressing how privacy continuous monitoring is done organization-wide<br>6.1: Workforce Training – includes communicating organization-wide privacy continuous monitoring goals, strategy, policies, and procedures to managers and staff<br>6.2: Privacy Awareness Communications – includes maintaining organization-wide privacy threat awareness<br>7.2: Internal and External Reporting – includes reporting on status of organization-wide privacy continuous monitoring activities<br>7.3: Privacy Monitoring and Auditing – includes identifying and tracking organization-wide privacy metrics for privacy continuous monitoring |

# Privacy Continuous Monitoring Activities in the Privacy Program (3 of 3)

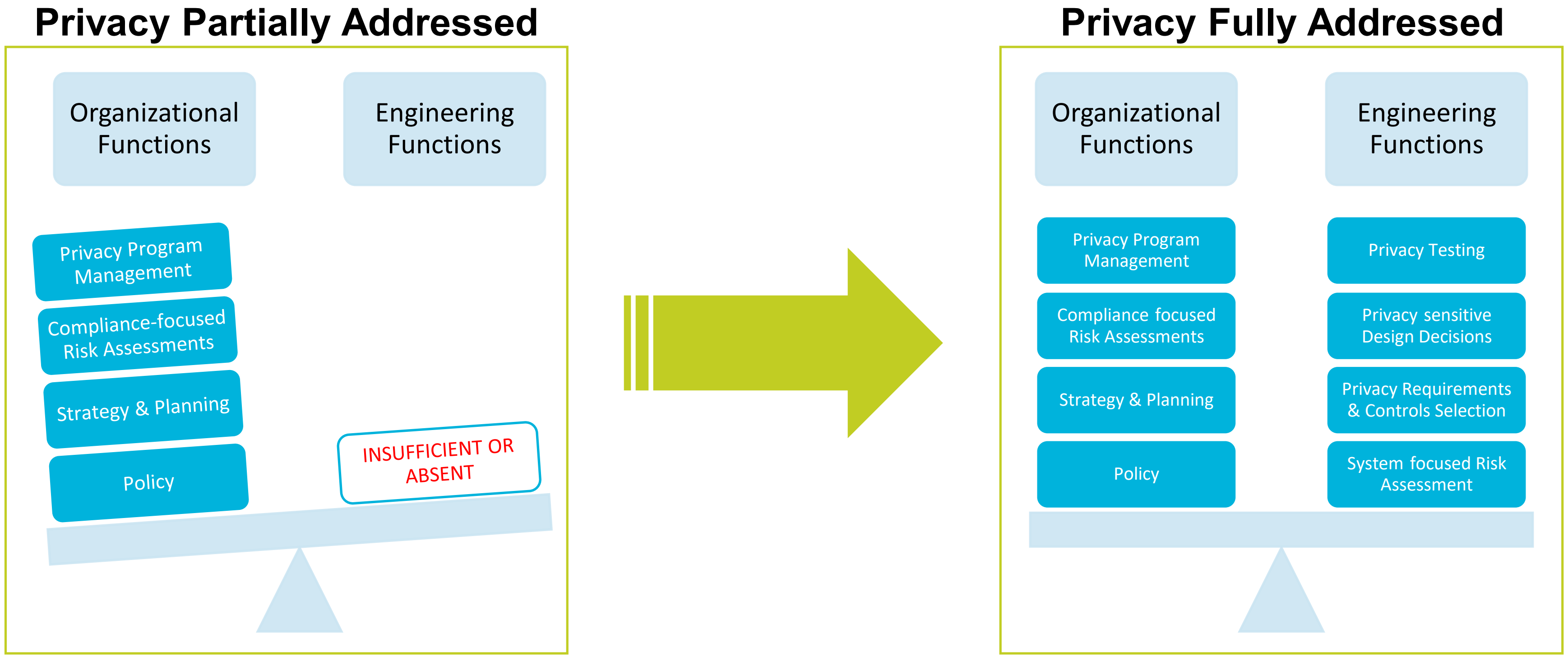
**Using the Privacy Maturity Model structure, privacy continuous monitoring activities should be included in the privacy program sub-elements listed in the table below.**

| Level | Privacy Maturity Model Sub-Elements |
|---|---|
| Level 3: System activity | 2.2: Privacy Policy, Procedures, and Standards – includes addressing privacy continuous monitoring in appropriate system policies, procedures, and standards consistent with organization-wide policies, procedures, and standards<br>2.3: PII Inventory, Categorization, & Minimization – includes maintaining an accurate system PII inventory<br>2.5: Privacy risk and impact assessments – includes system-specific privacy threat assessment<br>3.1: Integration into the Systems Engineering Process (Privacy Engineering) – includes identifying privacy system requirements and conducting systems privacy testing<br>3.2: Cybersecurity coordination – includes coordination with cybersecurity regarding privacy threat identification for systems<br>3.4: Privacy control selection – selecting privacy controls for systems based on risk<br>4.1: Incident Management Procedures -- includes system privacy incident response and linkage to privacy threats<br>7.2: Internal and External Reporting – includes reporting on results of systems testing<br>7.3: Privacy Monitoring and Auditing – includes identifying and tracking privacy metrics for privacy continuous monitoring for systems |

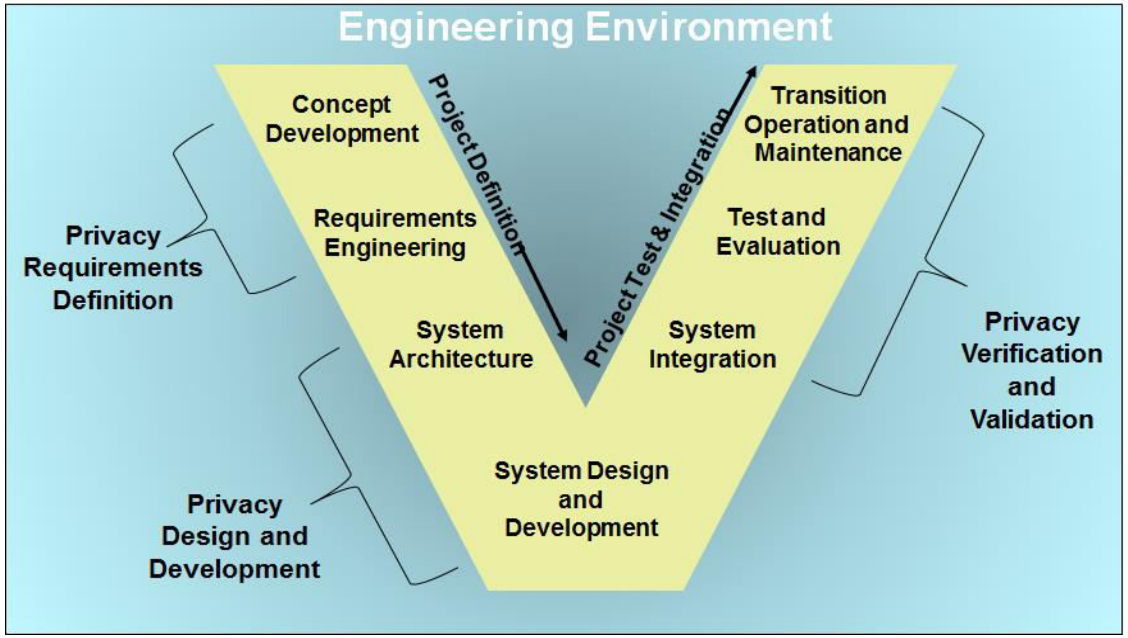
# Privacy Methods and Tools to Use for Systems Privacy Continuous Monitoring Activities

# The Need for Privacy Engineering

- **To adequately address privacy risks, systems that manage PII must behave in a privacy-sensitive manner.**
- **Systems engineering processes are a largely untapped opportunity to embed privacy requirements into organizational activities in a way that provides a major impact and will proactively address privacy risks.**


Privacy Partially Addressed
Organizational Functions
Engineering Functions
Privacy Program Management
Compliance-focused Risk Assessments
Strategy & Planning
Policy
INSUFFICIENT OR ABSENT
Privacy Fully Addressed
Organizational Functions
Engineering Functions
Privacy Program Management
Compliance focused Risk Assessments
Strategy & Planning
Policy
Privacy Testing
Privacy sensitive Design Decisions
Privacy Requirements & Controls Selection
System focused Risk Assessment

# Privacy Engineering


Engineering Environment
Concept Development
Requirements Engineering
System Architecture
System Design and Development
System Integration
Test and Evaluation
Transition Operation and Maintenance
Project Definition
Project Test & Integration
Privacy Requirements Definition
Privacy Design and Development
Privacy Verification and Validation

- **Privacy Engineering integrates privacy into systems as part of systems engineering processes.**
- **This diagram illustrates how the core privacy engineering activities map to stages of the classic systems engineering life cycle.**
- **A mapping exists for every systems engineering life cycle, including agile development, since every life cycle includes the core activities in some form.**
- **MITRE's Privacy Engineering Framework* can be used to integrate privacy into systems engineering processes in support of privacy continuous monitoring activities for systems. The Framework provides guidance on how to:**
  - Integrate privacy into the traditional systems engineering "V" life cycle.
  - Adapt the Framework to other life cycles beyond the traditional systems engineering "V" life cycle such as agile (incremental) and spiral (iterative) life cycles.

*MITRE Corporation, *MITRE Privacy Engineering Framework*, http://www.mitre.org/privacy.

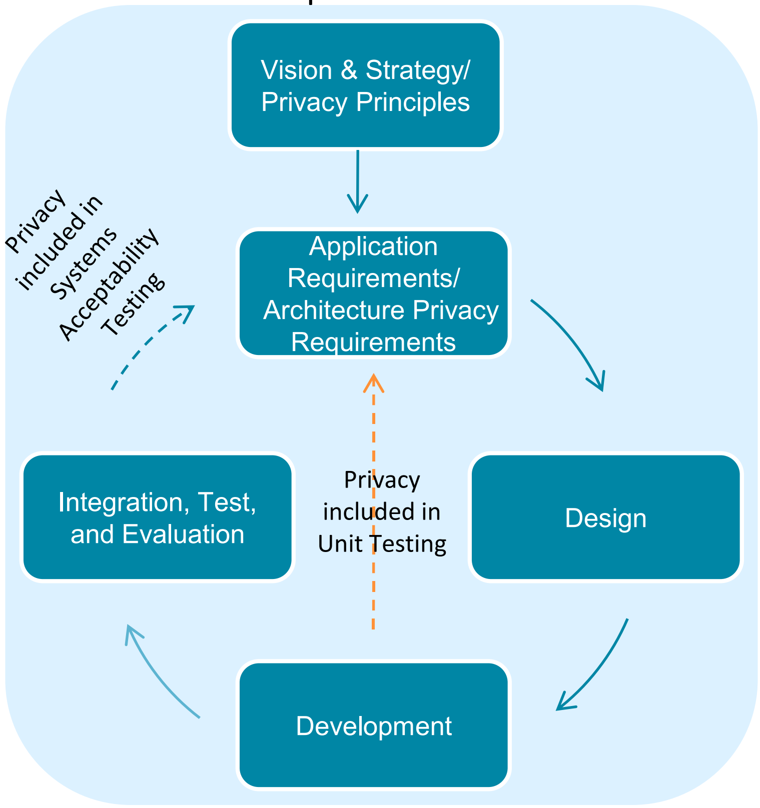
# What is Privacy Testing?

- **Privacy principles and privacy requirements must be built into systems**
- **Privacy testing is the process of verifying that a computer application meets the privacy requirements that were used to help design and develop the application.  The testing helps to ensure that the software works as expected.**
  - For simplicity, the term “privacy testing” is used to refer to a larger set of verification techniques
  - In the absence of testing, other verification techniques (“testing activities”) such as code reviews and document reviews can be used
- **Privacy testing is an important step to ensure systems protect privacy and should be performed as part of privacy continuous monitoring activities.**

# Privacy Testing Approach

- **Privacy testing should not be a separate process -- the privacy testing approach should be to:**
  - Integrate privacy testing activities into the existing system testing process
  - Have privacy testing as a rigorous and explicit activity in the system testing process
- **MITRE's Generic System Privacy Requirements and Tests* document provides a set of generic privacy requirements and tests that can be used to verify that a system works as expected from a privacy perspective as part of privacy continuous monitoring activities.**

Privacy Testing as Part of Overall System Development Process


Vision & Strategy/ Privacy Principles
Application Requirements/ Architecture Privacy Requirements
Design
Development
Integration, Test, and Evaluation
Privacy included in Unit Testing
Privacy included in Systems Acceptability Testing

Objective: Expand testing to ensure privacy is enforced in systems development throughout the system development life cycle

*MITRE Corporation, *MITRE Generic System Privacy Requirements and Tests*, http://www.mitre.org/privacy.

# Privacy Methods and Tools for Privacy Control Selection and Risk Assessment

- **Key federal government documents that address privacy risk management are:**
  - NIST SP 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations* - Privacy Control Catalog (Appendix J), April 2013 with updates through January 2015
  - Committee on National Security Systems Instruction No. 1253 (includes the "Privacy Overlays"), April 20, 2015
  - OMB Circular A-130, *Managing Information as a Strategic Resource*, July 27, 2016
  - NISTIR 8062, *Privacy Risk Management for Federal Information Systems,* January 2017

# Privacy Methods and Tools for Privacy Control Selection and Risk Assessment (cont.)

- **Additional references regarding privacy risk include:**
  - NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management (Preliminary Draft), September 6, 2019, https://www.nist.gov/privacy-framework/working-drafts
  - NIST Privacy Risk Assessment Methodology (PRAM), https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space/browse/risk-assessment-tools
  - System-Theoretic Process Analysis (STPA)-Privacy (STPA-Priv): Analyze system functional control structure for potential control errors that could violate privacy behavioral constraints and identify causal scenarios (http://www.mitre.org/privacy)
  - System-Theoretic Early Concept Analysis (STECA)-Privacy (STECA-Priv): Instrumental method for performing privacy risk management on complex socio-technical systems at early life cycle stages (http://www.mitre.org/privacy)

# Additional Privacy Continuous Monitoring Considerations

# Additional Privacy Continuous Monitoring Considerations

- **Assessment is a major part of privacy continuous monitoring**
  - Continuous monitoring involves doing regular periodic control assessments as well as monitoring in real time
  - Assessments can be done through reviews of documentation and/or via tools configured to look at specific types of activity
- **Sound privacy continuous monitoring goes beyond performing privacy compliance activities such as completing Privacy Impact Assessments (PIAs) and doing privacy program reporting**
  - Privacy needs to be involved in activities beyond compliance such as:
    - Integrating privacy into the systems engineering life cycle, particularly by identifying privacy system requirements and completing privacy system testing
    - Monitoring threat reporting

# Additional Privacy Continuous Monitoring Considerations (cont.)

- **Communication between cyber security and privacy is important since security continuous monitoring activities and tools used may contribute to privacy continuous monitoring efforts**
  - For example, security threat monitoring information may be useful for privacy threat monitoring since security threats may apply to the use of PII

# Conclusion

- **OMB Circular A-130 requires agencies to have a privacy continuous monitoring program and strategy.**
- **NIST SP 800-137 provides a framework for information security continuous monitoring**
  - The framework can be leveraged to identify privacy-specific activities to adopt to implement privacy continuous monitoring.
- **Privacy continuous monitoring activities should occur throughout multiple areas within an organization’s privacy program.**
  - Organizations should identify their privacy continuous monitoring posture and develop plans to mature their posture as part of their privacy continuous monitoring strategy.