IAPP Practical Privacy Series 2014

New York City
Washington, DC

#PracticalPrivacy
Agenda

- Risk Management Framework (RMF) Overview
- Overlay - Defined
- The Privacy Overlay
  - Privacy Overlay Structure
  - Relationship to the RMF
  - Privacy Overlay Content Overview
  - Privacy Overlay Content Example
  - “Rolodex Exception” and HIPAA
  - Proactive Implementation Considerations
The RMF:
- is an approach to risk management that addresses risk-related concerns at three levels: (i) the organization; (ii) the mission and business process(es); and (iii) the information system(s).
- provides a disciplined and structured process that integrates cyber security and risk management activities into the system development life cycle (SDLC).
- provides a consistent approach for agencies to address cyber security risks to IT systems through the specification and selection of security and privacy controls.
- Personally identifiable information (PII) is an asset of both the individual and the organization. The security and privacy controls protect the privacy of individuals and the assets of the organization.
RMF Overview

Step 1
CATEGORIZED System
- Categorize the system using security objectives: Confidentiality, Integrity, and Availability
- Impact levels: Low, Moderate, High
- Initiate security plan

Step 2
SELECT Security Controls
- Common Control Identification
- Select security and privacy controls.
- Develop system-level continuous monitoring strategy
- Review & approve security plan and continuous monitoring strategy
- Apply overlays and tailor

Step 3
IMPLEMENT Security Controls
- Implement control solutions consistent with organization’s cybersecurity architectures
- Document security control implementation in security plan

Step 4
ASSESS Security Controls
- Develop & approve security assessment plan
- Assess security controls
- Prepare security assessment report
- Conduct initial remediation actions

Step 5
AUTHORIZE System
- Prepare POA&M
- Submit security authorization package to authorizing official (AO)
- AO conducts final risk determination
- AO makes authorization decision

Step 6
MONITOR Security Controls
- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update security documentation
- AO reviews reported status
- Implement system decommissioning strategy

• Determine impact of changes to
the system and environment
• Assess selected controls annually
• Conduct needed remediation
• Update security documentation
• AO reviews reported status
• Implement system decommissioning strategy
An overlay is a specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines.

- NIST SP 800-53, Rev 4

The Privacy Overlay - Introduced

- The Privacy Overlay is a subset of security and privacy controls selected from the NIST SP 800-53 control catalogs, per CNSSI 1253 at Appendix F, applicable to information systems which contain PII and/or PHI
  - Estimated completion - early 2015
  - Will apply to any system that uses CNSSI 1253
  - Can also be applied to any non-NSS system containing PII or PHI
The Privacy Overlay

**Purpose** - Created by the Committee on National Security Systems (CNSS) to:
- Standardize implementation of security and privacy controls for systems containing PII
- Integrate privacy considerations early into the system development life cycle and security processes
- Provide guidance for privacy requirements for protected health information (PHI)

**Benefits** -
- Identifies safeguards necessary to implement the Privacy Act of 1974 in today’s technology-dependent world
- Enables effective communication between privacy and security professionals by clarifying terminology and demonstrating interrelationship of privacy and security controls
- Implements a consistent approach to assess privacy risk from NIST SP 800-122
- Supports OMB M-14-04 (Question 63) in Senior Agency Official for Privacy (SAOP) making sound decisions as an approver during the system authorization process
Privacy Overlay Structure

- Categorizes PII in three subparts as Low, Moderate, or High PII confidentiality impact levels as defined in NIST SP 800-122

- Approaches PHI as a separate, fourth subpart based on the HIPAA Privacy and Security Rules

  - Systems with PHI must apply both the applicable Low, Moderate, or High subpart and the PHI subpart
Privacy Overlay in the RMF

STEP 1
CATEGORIZE System

Categorize Information

Determine Security Category of Each Information Type

- Identify Info Types
- Determine Impact Values

Determine PII Confidentiality Impact Level (NIST 800-122)

Does System Contain PII?

Yes

- Use the 800-122 PII Confidentiality Impact Level as the 1253 confidentiality impact value for the PII information type

No

Privacy Overlay Not Required

STEP 2
SELECT Security Controls

Categorize System

Categorize System

(Determine Impact Values for Each Security Objective)

Select Minimum Controls

Select Security and Privacy Controls (Baseline + Applicable Overlays)

Further Tailor and Supplement (if Required)

Apply Privacy Overlay

- Use the 800-122 PII Confidentiality Impact Level to select the Privacy Overlay PII Sub-Part
- If the system contains PHI, also select the PHI Sub-Part in addition to the applicable PII Sub-Part

KEY:

RMF Process

NIST SP 800-122 Process
Privacy Overlay Content Overview

Table 1 provides summary of each control specified in the overlay:

- Lists every control referenced in the overlay
- Provides “quick view” of the types of specifications for each control by sub-part

<table>
<thead>
<tr>
<th>CONTROL</th>
<th>LOW</th>
<th>MODERATE</th>
<th>HIGH</th>
<th>PHI</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-2(8)</td>
<td></td>
<td>-R</td>
<td>-R</td>
<td>-R</td>
</tr>
<tr>
<td>AC-2(9)</td>
<td>+GR</td>
<td>+GR</td>
<td>+GR</td>
<td>+R</td>
</tr>
<tr>
<td>AC-2(13)</td>
<td>+R</td>
<td>+R</td>
<td>+R</td>
<td>+R</td>
</tr>
<tr>
<td>AC-3</td>
<td>+GR</td>
<td>+GR</td>
<td>+GR</td>
<td>+R</td>
</tr>
<tr>
<td>AC-3(3)</td>
<td>+EGVR</td>
<td>+EGVR</td>
<td>+EGVR</td>
<td>+EGVR</td>
</tr>
<tr>
<td>AC-3(7)</td>
<td></td>
<td>+GVR</td>
<td>+GVR</td>
<td>+GVR</td>
</tr>
<tr>
<td>AC-3(9)</td>
<td></td>
<td>+GR</td>
<td>+GR</td>
<td>+GR</td>
</tr>
<tr>
<td>AC-3(10)</td>
<td>GR</td>
<td>GR</td>
<td>GR</td>
<td></td>
</tr>
<tr>
<td>AC-4</td>
<td></td>
<td></td>
<td></td>
<td>+R</td>
</tr>
<tr>
<td>AC-4(8)</td>
<td></td>
<td></td>
<td></td>
<td>+VR</td>
</tr>
<tr>
<td>AC-4(12)</td>
<td></td>
<td></td>
<td></td>
<td>+GR</td>
</tr>
<tr>
<td>AC-4(15)</td>
<td></td>
<td></td>
<td></td>
<td>+R</td>
</tr>
<tr>
<td>AC-4(17)</td>
<td>+GVR</td>
<td>+GVR</td>
<td>+GVR</td>
<td>+R</td>
</tr>
<tr>
<td>AC-4(18)</td>
<td></td>
<td>+GR</td>
<td>+GR</td>
<td>+GR</td>
</tr>
<tr>
<td>AC-5</td>
<td></td>
<td>+GR</td>
<td>+GR</td>
<td>+GR</td>
</tr>
</tbody>
</table>
Privacy Overlay Content Overview

For each control reference the overlay provides:

- Justification for control inclusion in overlay
- Reference to the applicable statutory, regulatory, or federal standard
- One or more control specifications, depending on the applicable requirement(s):
  - Whether the control must be selected or cannot be selected
  - Supplemental Guidance
  - Parameter Value(s)
  - Control Extensions
AC-2, ACCOUNT MANAGEMENT

**Justification to Select:** Account management is a critical function for developing and implementing an access control framework that is appropriate for the information contained in systems and applications. When implemented effectively, the access control framework provides the necessary constructs for controlling access to PII, limiting disclosure of records about individuals to only those system and application users that have a need for the information to perform their job functions. The purpose of this guidance is to establish requirements for user access to PHI and PII.

**Low PII Confidentiality Impact Level Control Extension:** Prohibit use of guest, anonymous, and shared accounts for providing access to PII. Notify account managers within an *organization-defined timeframe* when temporary accounts are no longer required or when information system users are terminated or transferred or information system usage or need-to-know/need-to-share changes. Prior to granting access to PII, users demonstrate a need for the PII in the performance of the user’s duties.

**Moderate and High PII Confidentiality Impact Level Control Extension:** Apply the Low PII Confidentiality Impact Level Control Extension. Implement access controls within the information system based on users’ or user group’s need for access to PII in the performance of their duties. Organizations should provide access only to the minimum amount of PII necessary for users to perform their duties.

**PHI Control Extension:** Apply the High PII Confidentiality Impact Level Control Extension.

**PHI Supplemental Guidance:** The identification of authorized users and access privileges include considerations of whether the user will need access to PHI and whether such access may be permitted or required under HIPAA. The purpose of this guidance is to establish requirements for user access to PHI.

**Low and Moderate PII Confidentiality Impact Level Parameter Value:** j… at least annually.

**High PII Confidentiality Impact Level Parameter Value:** j… at least quarterly for privileged accounts, at least annually for general user’s accounts.

**Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference(s):** 5 U.S.C. 552a(b), (e)(9), (e)(10); OMB M-07-16

**PHI Regulatory/Statutory Reference(s):** 45 CFR 164.308(a)(3)(ii)(A); 45 CFR 164.308(a)(3)(ii)(B); 45 CFR 164.308(a)(4)(i); 45 CFR 164.308(a)(4)(ii)(B); 45 CFR 164.308(a)(4)(ii)(C); 45 CFR 164.308(a)(5)(ii)(C); 45 CFR 164.312(a)(2)(i); 45 CFR 164.312(a)(2)(ii); 45 CFR 164.502
“Rolodex Exception” and HIPAA

- “Rolodex Exception” - Identifies Business Rolodex Information as a specific context in which the privacy risk for the individuals and/or the respective agency is so low that it does not trigger the Privacy Overlay
  - Business Rolodex Information includes business contact information when used in the limited context of contacting an individual in the normal course of business
  - Aligns with OMB’s Best Judgment Standard from M-07-16, Footnote 6
  - Separate from other types of considerations, such as OPSEC concerns, classification, or labeling

- Health Insurance Portability and Accountability Act (HIPAA)
  - Clarifies that addressable requirements are not optional
  - Implements addressable requirements based on risk analysis:
    - Determines the extent to which each control is “reasonable and appropriate”
Proactive Implementation Considerations

What you can do now to prepare:

- Work with your security counterparts to participate in the CNSS review process.
- Map requirements in the overlay to agency policy and standards to identify traceability and any gaps.
- Determine need for any additional specifications to meet agency-specific requirements.
- Examine the process for categorizing PII in accordance with NIST SP 800-122 and determine your agency’s approach.
- Study the current draft to understand the potential impacts within your agency and necessary policy decisions that govern how it is implemented.
- Identify processes that may require adjustments for implementing the Overlay (e.g., those related to risk management, system design and development, and acquisitions).
- Determine the cognizant officials with security and privacy experience who understand legal requirements necessary to support policy and tailoring determinations.
For More Information

- Lew Oleinick (DLA): lewis.oleinick@dla.mil
- Hillary Fielden (NRO): fielden_hillary@bah.com
- Howard Gill (DHA): gill_howard@bah.com
- Jeremy Miller (DHA): miller_jeremy_1@bah.com
- Julie Snyder (DOD CIO): jsnyder@mitre.org
Backup Slides
CNSS Membership

Members

- The Secretary of State
- The Secretary of the Treasury
- The Secretary of Defense
- The Attorney General
- The Secretary of Commerce
- The Secretary of Transportation
- The Secretary of Energy
- The Secretary of Homeland Security
- Director of the Office of Management and Budget
- Assistant to the President for National Security Affairs
- Director of National Intelligence
- Chairman of the Joint Chiefs of Staff
- Director, Federal Bureau of Investigation
- Administrator, General Services Administration
- The Chief of Staff, United States Army
- The Chief of Naval Operations
- The Chief of Staff, United States Air Force
- Commandant, United States Marine Corps
- Director, Central Intelligence Agency
- Director of the Defense Intelligence Agency
- Director, National Security Agency

Observers

- U.S. Department of Agriculture
- National Geospatial-Intelligence Agency
- Defense Information Systems Agency
- National Institute of Standards and Technology
- Federal Communications Commission
- Nuclear Regulatory Commission
- Information Security Oversight Office
- National Reconnaissance Office
- National Archives and Records Administration
- Office of Science and Technology
- National Aeronautics and Space Administration
- Unified Cross Domain Management Office
- United States Strategic Command
- Program Manager for the Information Sharing Environment