NIST 800-53 Rev. 4 Privacy Controls: DHS Implementation Success Story

Debra Danisek, J.D., CIPP/G
Senior Director, Privacy Compliance
DHS Privacy Office

Jeff Gallucci, CISSP, PMP
Director, Authorization Reviews & Monitoring Ongoing Risk (ARMOR)
DHS Office of the CISO
Agenda

• Appendix J Background
• Life before Appendix J
• Engagement Timeline
• Implementation at DHS
Integrating Privacy & Security into a Single Framework

WHY APPENDIX J?
Familiar Territory

FIPPs and Controls may be unfamiliar territory to security staff, but should be familiar to privacy staff.
Life Before Appendix J

- Privacy not viewed as equal partner in risk management discussions
- Confidentiality treated as the sum total of privacy concerns
- Stove piping of privacy and security risk management conversations
Where are Security and Privacy at DHS?

- Secretary of Homeland Security
  - Chief Privacy Officer
  - Undersecretary for Management
    - Chief Information Officer
    - Chief Information Security Officer (CISO)
Compliance and Risk Management
Responsibilities

- Sets DHS Information Security Policy
- Manages DHS FISMA Inventory
- Provides guidance and technology
- Oversees and enforces security through compliance score-carding

• Privacy is a key component in Security Authorization

DHS CISO

- Sets Department privacy policies
- Drafts, reviews, and approves all Department privacy compliance documentation (PIA/SORN)
- Formal determination whether a system/project/program is “privacy sensitive”

- Interaction with CISO during the RMF process

DHS PRIV

Security enabling business: quick, clear, collaborative.
Challenges prior to Appendix J

- CISOs didn’t always see Privacy Documentation as a shared responsibility
- Security Scorecard showed Privacy requirements, but metrics had no teeth
- Privacy Offices and CISO Offices were less collaborative in some cases

DHS CISO

- Confidentiality treated as the sum total of privacy concerns
- Systems granted ATO without complete privacy documentation (PIA, SORN)
- Privacy not included in CISO metrics
- Privacy analysts do not understand the Risk Management Framework

DHS PRIV

- Confidentiality treated as the sum total of privacy concerns
- Systems granted ATO without complete privacy documentation (PIA, SORN)
- Privacy not included in CISO metrics
- Privacy analysts do not understand the Risk Management Framework
These two metrics merge in FY15 making Privacy an embedded part of Security measuring.
Appendix J in Practice

ENGAGEMENT PROCESS AT DHS
Privacy in Partnership with Security

NIST invites the Federal CIO Council Privacy Committee to collaborate on the development of a set of privacy protections for inclusion in Special Publication 800-53, Security Controls for Federal Information Systems and Organizations. Invite stems from recognition that a centralized set of privacy controls is needed for existing and emerging initiatives, such as smart grid and cloud computing.

2009
- CIO Council publishes Best Practices: Elements of a Federal Privacy Program white paper and leverages for App J

2010
- FEA-SPP (V.3) published with a set of Privacy Control Families developed by the Privacy Committee

2011
- July: DRAFT Appendix J Privacy Controls Catalogue released by NIST for public comment. Privacy Committee serves on NIST comment adjudication team.

2012
- February: Second draft of Appendix J integrated into first draft of NIST Special Publication 800-53 (Rev 4), Security and Privacy Controls for Federal Information Systems and Organizations and released for public comment. First time privacy appears in the name of the publication.

2013
- NIST SP 800-53 Rev 4 FINAL
- OMB publishes FY12 FISMA Guidance – Question 53 states that App J is effective upon publication of the final SP 800-53 Rev 4
Key Appendix J Outcomes

- Structured set of privacy controls that are based on Fair Information Practice Principles (FIPPs)
- Tool to support managing organization privacy risk and compliance
- Privacy built into entire lifecycle of personally identifiable information (PII) (paper or electronic)
- Closer cooperation between privacy and security officials
- Comprehensive source of privacy requirements

NIST Special Publication 800-53 (Rev 4), Security and Privacy Controls for Federal Information Systems and Organizations
DHS Engagement Timeline

- **Socialize**
  - June 2013: Socialize Appendix J

- **Assessment Tool**
  - September 2013: CISO launched a new Information Assurance and Compliance tool

- **Authority**
  - New realization on need for Shared Authority

- **Implementation**
  - July 1, 2014
Assessments of privacy controls can be conducted either by the Senior Agency Official for Privacy (SAOP) or Chief Privacy Officer (CPO) alone or jointly with the information security office. (pg. J-4)

SAOPs are responsible for the implementation of Appendix J.
SAOPs may consult with CISOs, but the authority for the selection/assessment of privacy controls rests with SAOP.
SAOP makes determination which controls may be considered “common controls.”
SAOP approval required as a precondition for the issuance of an authority to operate.

2014: New PRIV Authority within Security Authorization Process
Appendix J in Practice

IMPLEMENTATION PLAN AT DHS
DHS Implementation of Privacy Controls

1. Update DHS security policies to reflect new Appendix J controls and PRIV authority
2. Determine which controls are Common, System/Program, and Hybrid
3. Incorporate privacy controls into the security risk management framework
4. Fit privacy controls into the Compliance process
5. Include the Privacy Controls in the Info-Assurance Compliance System tool
Types of Controls

Common Controls
Single implementation leveraged and used uniformly across the organization
- AR-1 Governance and Privacy Program

System Controls
Implementation is unique to the specific system
- May leverage a standard approach
- AP-1 Authority to Collect

Hybrid Controls
Implementation is split between two or more elements of an organization
- AR-5 Privacy Awareness and Training

Capturing the implementation approach in the Privacy Plan promotes uniform understanding and execution and increases compliance.
Using the RMF to assess Privacy Controls

Categorize:
- ISSOs complete PTA as required by DHS policy
- PTAs submitted to DHS PRIV for review
- DHS PRIV makes determination whether system/program is privacy sensitive
Using the RMF to assess Privacy Controls

Select:
- Applicability of privacy controls
- If NOT privacy sensitive:
  - Common Controls apply
- If privacy sensitive:
  - ALL controls (common and system/program) apply
Using the RMF to assess Privacy Controls

Implement:
- What DHS-specific requirements meet the control requirement
- Example:
  - DI-1 data quality control – The organization confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information.
  - Implementation requirement – PIA section 2.4
Using the RMF to assess Privacy Controls

Assess:
- *Has the system/program completed the Implementation Language*
- DHS PRIV analysts will assess each control based on the privacy compliance documentation already submitted
- A complete PIA and SORN will satisfy almost all of the system/program controls
Using the RMF to assess Privacy Controls

Authorize:
- System must have affirmative PRIV assessment of privacy controls *before asking for Authorization to Operate (ATO)*
New challenges...

- POA&Ms and Waivers
- Metrics
- Role of Component Privacy Officers
- Appendix J controls apply beyond FISMA reportable systems
- Ongoing authorization
Privacy and Security Success Story

• Improved coordination and communication between CISO and PRIV
• Privacy embedded in Risk Management Process
• New SAOP Authority