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**

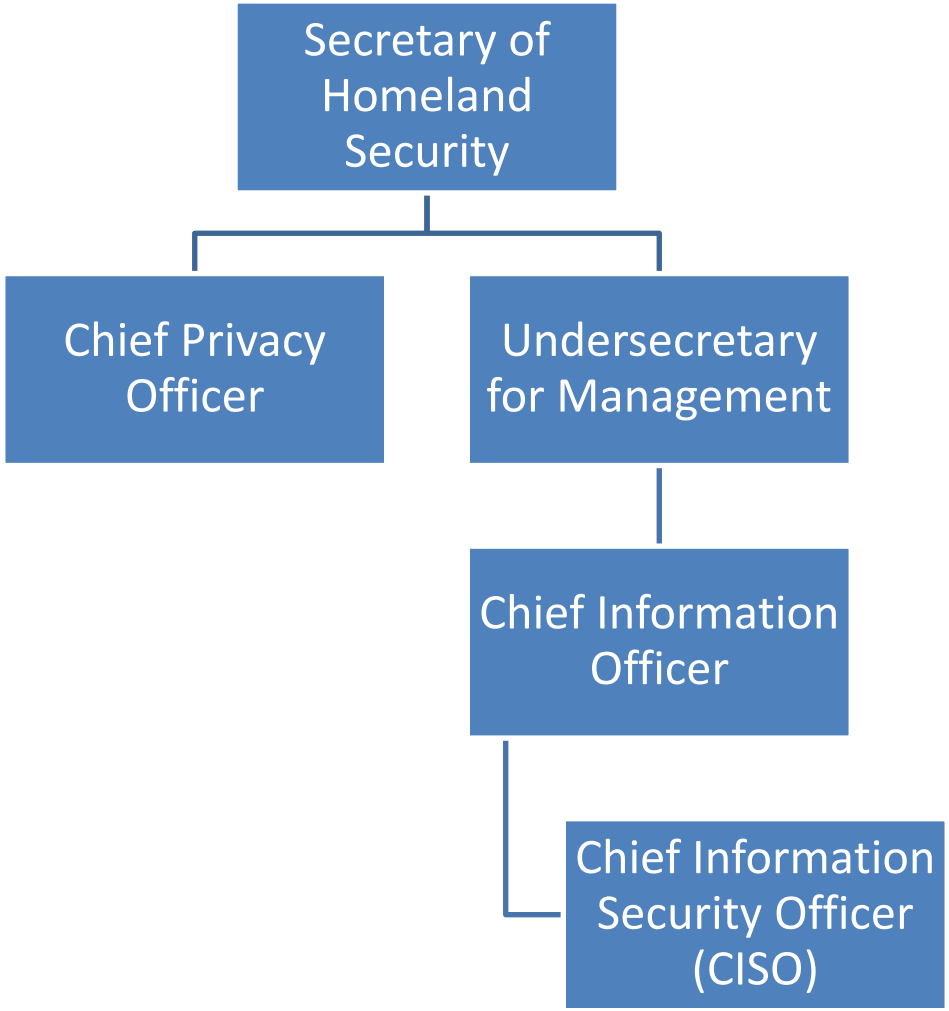
Privacy and Security

LIFE BEFORE APPENDIX J

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?



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

DHS FISMA Scorecard

Department of Homeland Security

FY14 Information Security Scorecard
– Security Processes (SPM)
September 2014

	ABC	HIJ	GHI	DEF	Target	DHS
FISMA Systems	89	57	87	12	N/A	189
Mission Essential Systems	35	18	25	0	N/A	67
Authorization	97%	93%	56%	83%	90%	78%
Ongoing Authorization (I)	Y	2%	N	17%	N/A	12%
Privacy (I)	53%	93%	35%	63%	90%	56%
Weakness Remediation	85%	97%	73%	97%	90%	88%
Training	99%	98%	100%	90%	95%	91%
Event Management	99%	100%	77%	100%	90%	93%
TIC Consolidation	100%	98%	90%	96%	95%	97%
Mandatory Access – PIV	80%	86%	95%	76%	75%	84%
Overall SPM Score	96%	96%	75%	91%	90%	88%

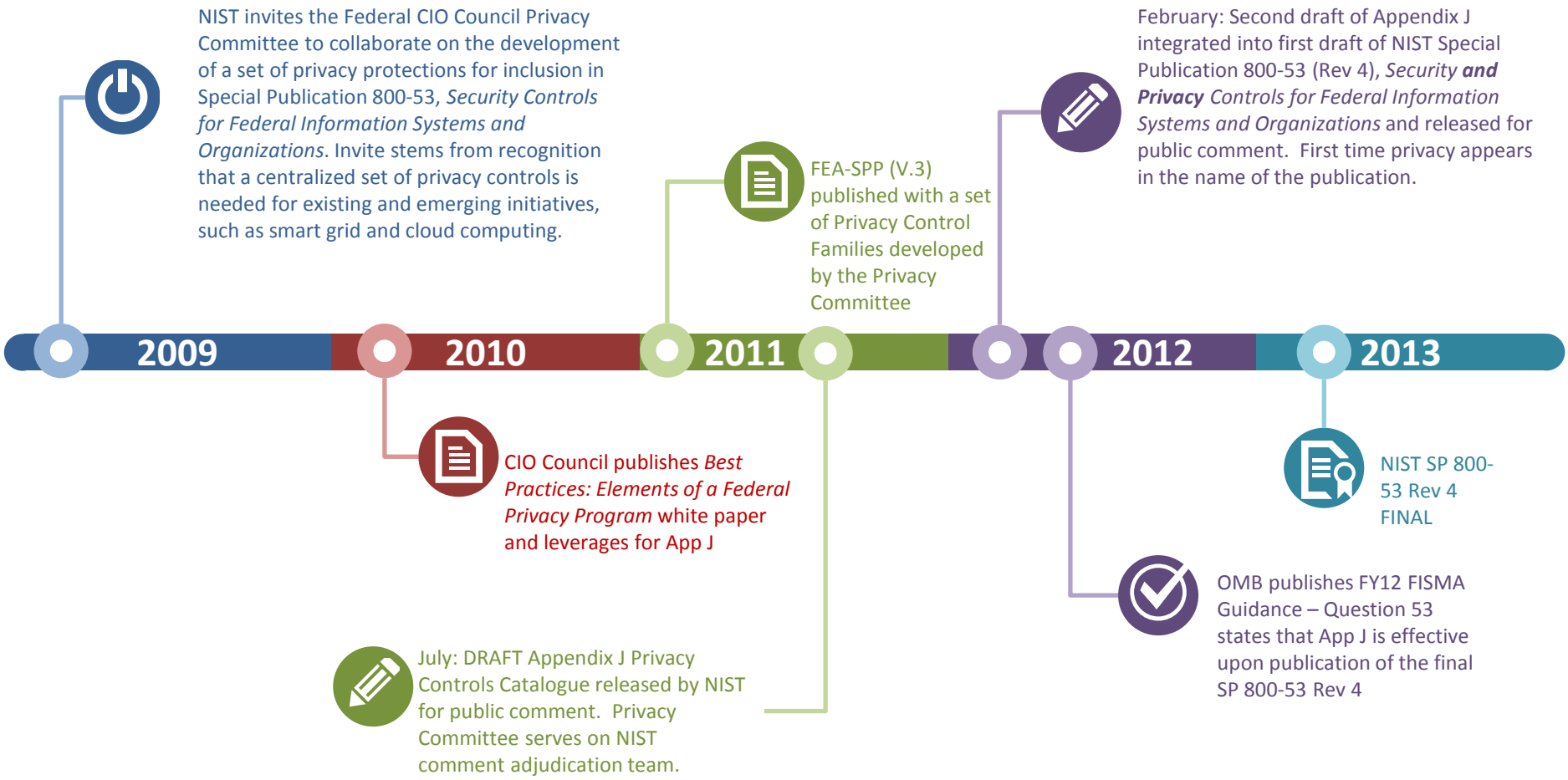
(I) Informational Metrics do not contribute to the Overall SPM Score

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

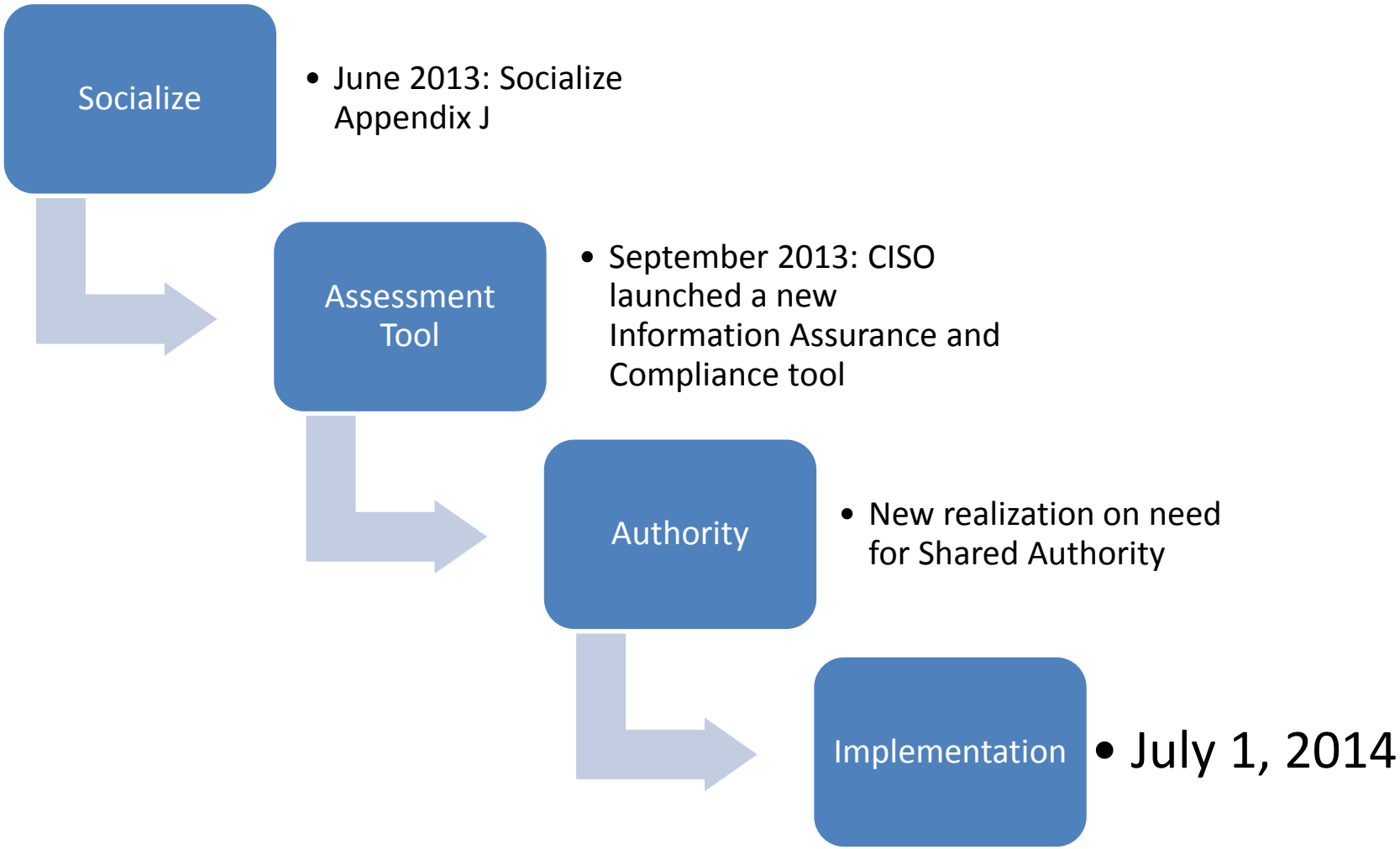


Key Appendix J Outcomes

- **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



2014: New PRIV Authority within Security Authorization Process

NIST 800-53 Rev. 4 Appendix J

- 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)

OMB M-14-04 (pg. 23-24)

- **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.**

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

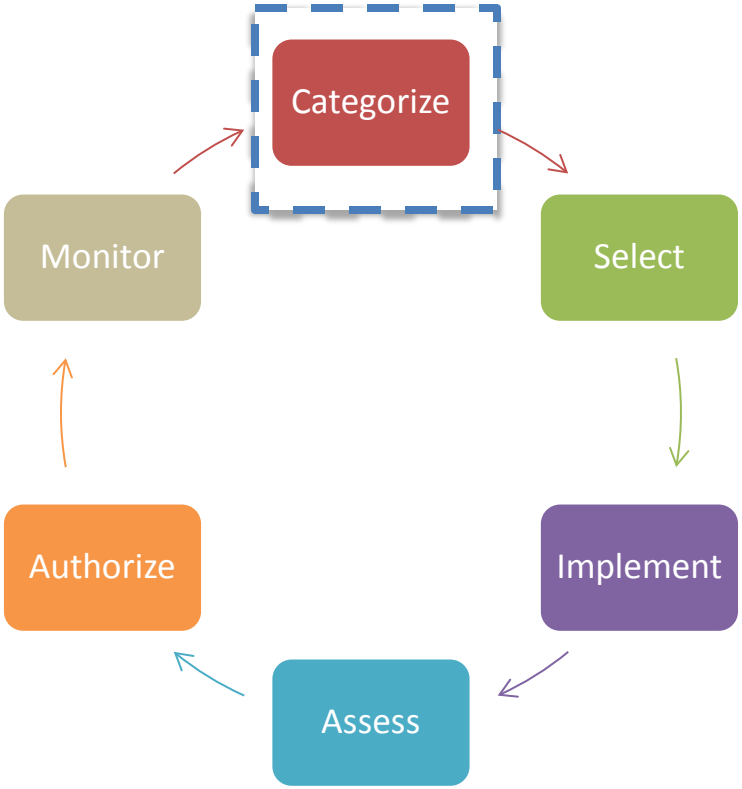
Hybrid Controls

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.

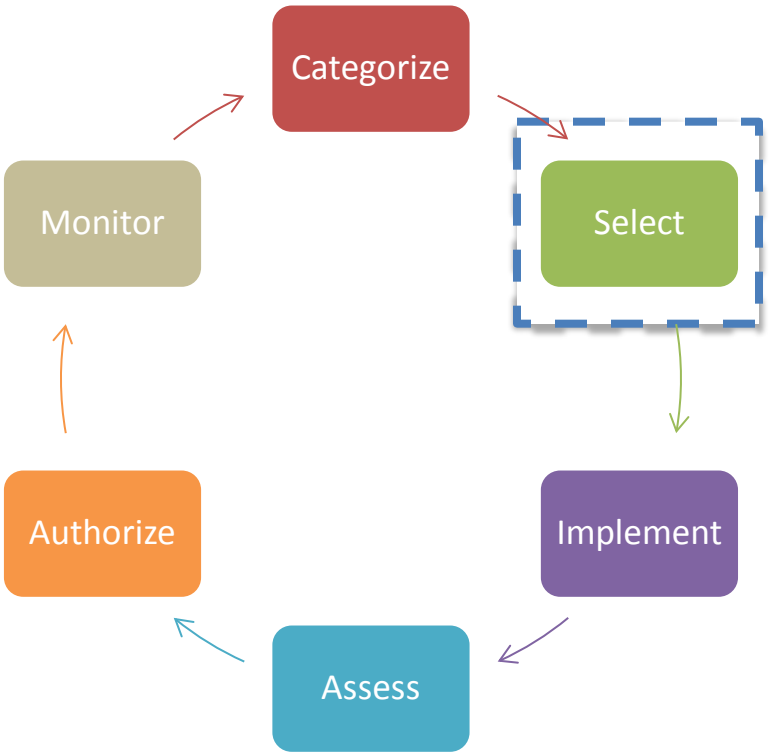
Using the RMF to assess Privacy Controls



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**

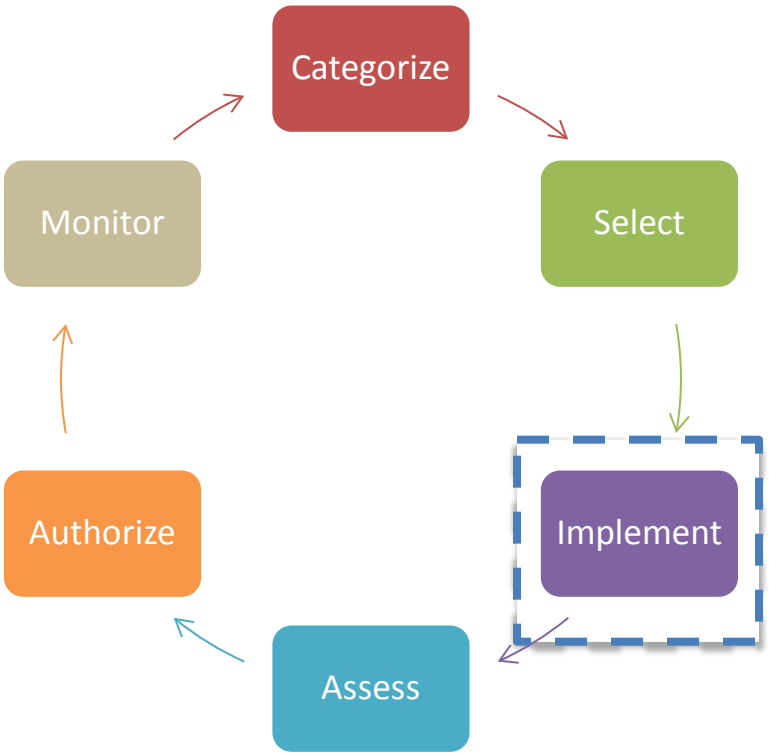
Using the RMF to assess Privacy Controls



Select:

- *Applicability of privacy controls*
- If NOT privacy sensitive:
  - Common Controls apply
- If privacy sensitive:
  - ALL controls (common and system/program) apply)

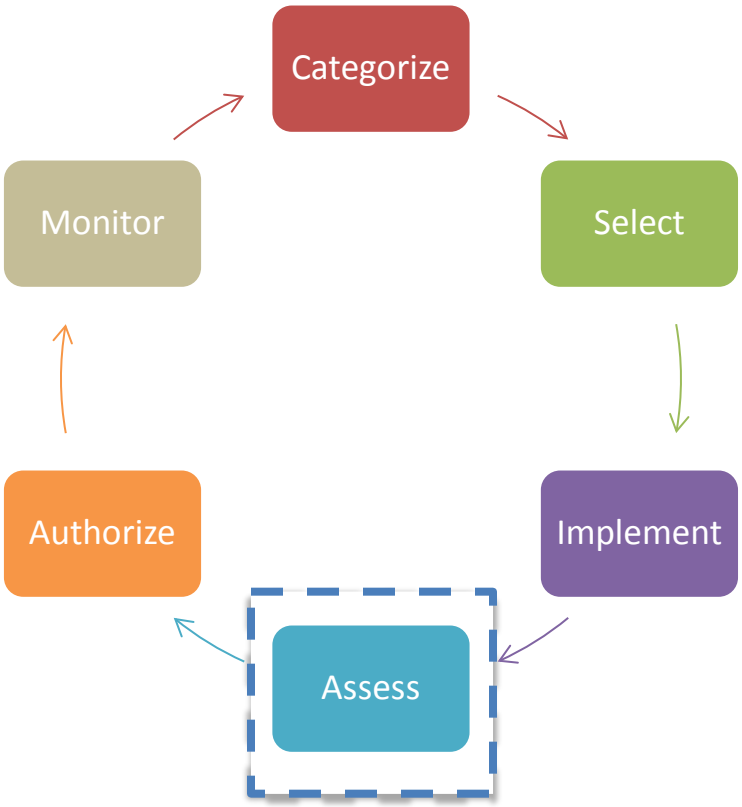
Using the RMF to assess Privacy Controls



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

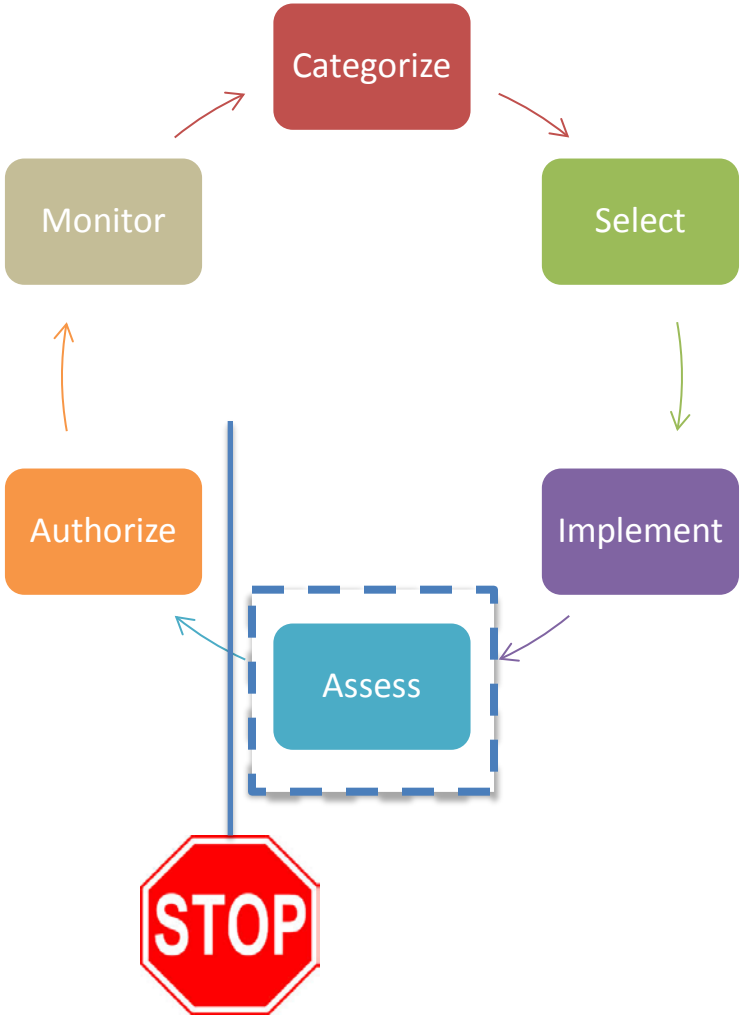
Using the RMF to assess Privacy Controls



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

Debra Danisek

Debra.Danisek@hq.dhs.gov

Jeff Gallucci

Jeffrey.Gallucci@hq.dhs.gov