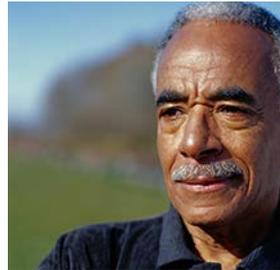


**2015 VA Privacy Matters
Symposium**

*Session 1:
Understanding Appendix J*



June 9, 2015



Office of Information Security
Privacy and Records Management

Administrative Items

- Do not use your computer microphone to participate in this meeting. Lync will be used only as a display. Please dial in using the following information:
 - Phone number: 1-800-767-1750
 - Conference ID: 08388
- Please mute your computer microphone and speakers. This will eliminate feedback on the line and make it easier for you and your colleagues to hear the presentation.
- The presenters will address questions at the end of the presentation. For those online, please feel free to type your questions into the Lync Instant Messenger.
- Send technical issues to VACOPrivacySpeakers@va.gov.



Panel Moderator

Miles Windsor

Privacy Compliance Lead

VA Privacy Service

U.S. Department of Veterans Affairs



Guest Panelists

Chris Brannigan

Privacy Officer

IT Security & Privacy

Office of the Chief Information Officer

U.S. Office of Personnel Management

Jonathan Cantor

Deputy Chief Privacy Officer

U.S. Department of Homeland Security

Claire Barrett

Chief Privacy Officer

U.S. Department of Transportation



Chris Brannigan

Privacy Officer

IT Security & Privacy

Office of the Chief Information Officer

U.S. Office of Personnel Management

QUICK START GUIDE
to a
GAP ANALYSIS
between the requirements of an
AGENCY PRIVACY POLICY
and
NIST SP 800-53 Rev 4
Appendix J

QUICK START GUIDE
to a
GAP ANALYSIS
between the requirements of an
AGENCY PRIVACY POLICY
and
NIST SP 800-53 Rev 4
Appendix J

Christopher J. Brannigan, CIPP/US, CIPP/G
Privacy Officer, IT Security & Privacy
Office of the Chief Information Officer
US Office of Personnel Management

So, what should privacy heads at government agencies do now?
What's the first order of business in complying with the new 800-53? Will there be a scramble?

Essentially, this is a great time to do a gap analysis, said NIST's Ross.

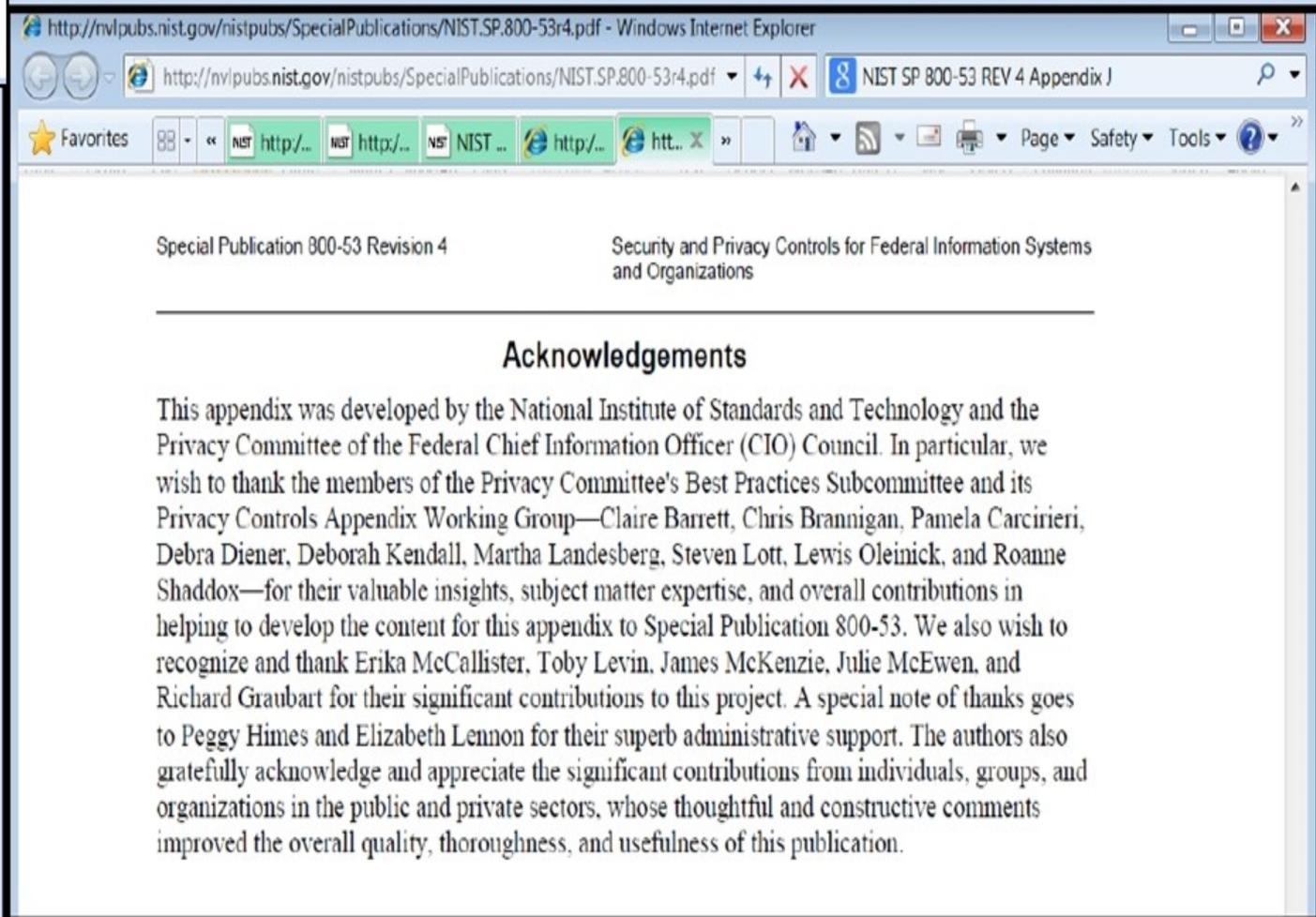
"That's exactly what I would do," he said.

"Go look at what's in Appendix J and then do a gap analysis to see if they're missing anything or if they need to change anything that they're already doing.

And then they'll look at those things routinely after that."

NIST Appendix J - Quick-Start Gap Analysis of Your Privacy Policy & Appendix J Controls

QUICK START GUIDE
to a
GAP ANALYSIS
between the requirements of an
AGENCY PRIVACY POLICY
and
NIST SP 800-53 Rev 4
Appendix J



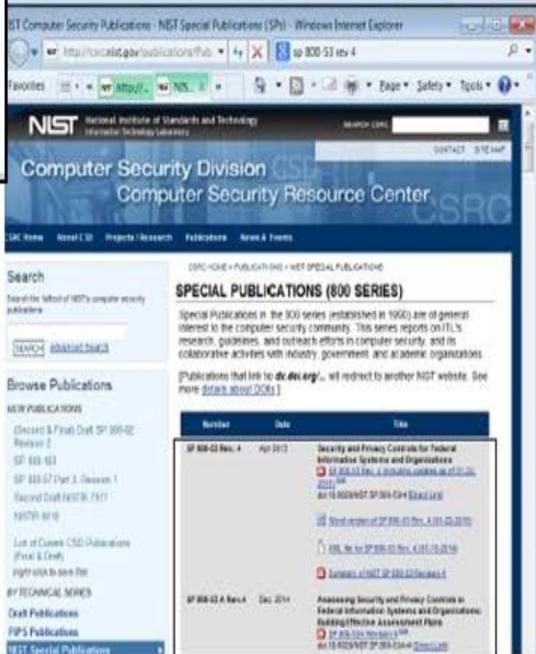
The screenshot shows a Windows Internet Explorer browser window. The address bar contains the URL <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>. The page title is "NIST SP 800-53 REV 4 Appendix J". The browser's Favorites bar shows several bookmarks, including "http://...", "NIST http://...", "NIST http://...", "NIST http://...", and "http://...". The main content area of the browser displays the following text:

Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations

Acknowledgements

This appendix was developed by the National Institute of Standards and Technology and the Privacy Committee of the Federal Chief Information Officer (CIO) Council. In particular, we wish to thank the members of the Privacy Committee's Best Practices Subcommittee and its Privacy Controls Appendix Working Group—Claire Barrett, Chris Brannigan, Pamela Carcirieri, Debra Diener, Deborah Kendall, Martha Landesberg, Steven Lott, Lewis Oleinick, and Roanne Shaddox—for their valuable insights, subject matter expertise, and overall contributions in helping to develop the content for this appendix to Special Publication 800-53. We also wish to recognize and thank Erika McCallister, Toby Levin, James McKenzie, Julie McEwen, and Richard Graubart for their significant contributions to this project. A special note of thanks goes to Peggy Himes and Elizabeth Lennon for their superb administrative support. The authors also gratefully acknowledge and appreciate the significant contributions from individuals, groups, and organizations in the public and private sectors, whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication.

NIST Appendix J - Quick-Start Gap Analysis of Your Privacy Policy & Appendix J Controls



NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from
<http://dx.doi.org/10.6028/NIST.SP.800-53x>

Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations

APPENDIX J

PRIVACY CONTROL CATALOG

PRIVACY CONTROLS, ENHANCEMENTS, AND SUPPLEMENTAL GUIDANCE

The need to protect an individual's privacy in the digital age has become a central theme in the Privacy Act first sought to balance the government's need to collect, maintain, and dispose of information with a citizen's right to be notified of the collection, maintenance, and disposal of information. In the private sector, where healthcare, financial services, and social media are increasingly higher level, the need to protect personal information is becoming more acute. Smart Grid, mobile, and cloud computing have created new data and metadata environments, which present challenges for federal organizations in safeguarding information beyond the traditional information technology security challenges. Now there are challenges for federal organizations in safeguarding information integrity of an individual's information in a world where information is available on demand. The challenge is to expand their view of privacy, in order to meet citizens' expectations for information security.

Privacy, with respect to personally identifiable information, is obtained only with appropriate legislation, policy, and compliance with requirements. Protecting the privacy of information is a responsibility of federal organizations. Privacy is not when and whether to share personal information, but rather, the particular circumstances under which that information is processed, stored, and transmitted. Organizations cannot have effective information security if they do not have effective privacy. Privacy is more than security; it is a principle of transparency, notice, and choice.

This appendix provides a structured set of controls for organizations to use in identifying and implementing a privacy program, whether in paper or electronic form, as a value distinct from, but highly interrelated with, information security.

¹¹⁰ OMB Memorandum 07-15 defines PII as information that identifies such as their name, social security number, business or personal identifying information, which is linked or linkable to another's unique name, etc. OMB Memorandum 16-12 further defines a category of information or technology. Rather, if an individual can be identified by examining the content of one or more records, it is important for agencies to recognize that one or more records be used to identify an individual. ¹¹¹ NIST Special Publication 800-53 Rev. 4 focuses on the security of information. Organizational definitions of PII may vary based on the context of the privacy controls in this appendix apply regardless of the definition.

APPENDIX J

Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations

The administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of PII. ¹¹⁰ Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.

The privacy controls in this appendix are based on the Fair Information Practice Principles (FIPPs) ¹¹¹ embodied in the Privacy Act of 1974, Section 208 of the E-Government Act of 2002, and Office of Management and Budget (OMB) policies. The FIPPs are designed to build public trust in the privacy practices of organizations and to help organizations avoid tangible costs and intangible damages from privacy incidents. There are eight privacy control families, each aligning with one of the FIPPs. The privacy families can be implemented at the organization, department, agency, component office, program, or information system level, under the leadership and oversight of the Senior Agency Official for Privacy (SAOP) Chief Privacy Officer (CPO) ¹¹² and in coordination with the Chief Information Security Officer, Chief Information Officer, program officers, legal counsel, and others as appropriate. Table J-1 provides a summary of the privacy controls by family in the privacy control catalog.

TABLE J-1: SUMMARY OF PRIVACY CONTROLS BY FAMILY

ID	PRIVACY CONTROLS
AP	Authority and Purpose
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	Accountability, Audit, and Risk Management
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-6	Privacy Reporting
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	Data Quality and Integrity
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	Data Minimization and Retention
DM-1	Minimization of Sensitive Identifiable Information
DM-2	Data Retention and Disposal

¹¹⁰ In 2010, the Federal CIO Council Privacy Committee issued a framework for designing and implementing a privacy program entitled *Best Practices: Elements of a Federal Privacy Program (Silver White Paper)*. The privacy controls in this appendix mirror a number of the elements included in the paper. Organizations can use the privacy controls and the guidance in the paper to develop an organization-wide privacy program or enhance an already existing program.

¹¹¹ The FIPPs are widely accepted in the United States and internationally as a general framework for privacy and are reflected in other federal and international laws and policies. In a number of organizations, FIPPs serve as the basis for analyzing privacy risks and determining appropriate mitigation strategies. The Federal Enterprise Architecture Security and Privacy Profile (FEA-SP) also provided information and materials in development of the privacy controls.

¹¹² All federal agencies and departments designate in SAOP CPO as the senior organizational official with the overall organization-wide responsibility for information privacy issues. OMB Memorandum 05-08 provides guidance for the designation of SAOP/CPOs. The term SAOP/CPO as used in this appendix means an organization's senior privacy leader, whose job title may vary from organization to organization.

QUICK START GUIDE
to a
GAP ANALYSIS
between the requirements of an
AGENCY PRIVACY POLICY
and
NIST SP 800-53 Rev 4
Appendix J

NIST Appendix J - Quick-Start Gap Analysis of Your Privacy Policy & Appendix J Controls

Q&A: NIST's Ron Ross on the fourth revision of SP 800-53 - FierceGovernmentIT - Windows

http://www.fierce... ron ross nist appendix gap analysis

FierceGovernmentIT NEWS TOPICS

Topics: Cybersecurity

Q&A: NIST's Ron Ross on the fourth revision of SP 800-53

April 30, 2013 | By David Perera

SHARE

Email

Tweet

18

Show



Ron Ross, Image: NIST

The National Institute of Standards and Technology released April 30 its fourth version of Special Publication 800-53 (pdf), the catalog of controls most agencies utilize in their cybersecurity programs. We spoke that day with Ron Ross, NIST Federal Information Security Management Act implementation project leader and leader of the joint task force that put together the new revision.

FierceGovernmentIT: I want to ask about the new privacy appendix, but before that can you highlight some of the more significant changes to the security

The ability to develop those controls gives more consistency. Everybody knows now when you're dealing with transparency, or whatever the FIPPs requirement might be, there's a specific set of controls, the language is specified in the words of the privacy folks who understand the business, and they can now be applied uniformly across the agencies.

We also plan to develop some assessment procedures. We'll have uniform ways to assess those privacy controls, to see if they're actually effective in what they're trying to do. His main wanted to bring together - and it's very hard to do this, since the privacy officer and the security officer are totally separate, obviously, and have different legislative derivations-but yet, they have a lot of overlap.

In other words, if you want to have good privacy, you have to have a good foundation of security, especially in the area of confidentiality. It's kind of like a Venn diagram. There's a lot of things that privacy folks do to protect things from nondisclosure that are overlapping the security space.

The whole purpose was to develop a set of controls that were developed on the order of our security controls, same type of structure. It would allow more consistency as these controls were implemented across the different federal agencies. When you have the FIPPs, there were eight of those. And each of those principles drove a different family of policy controls.

The ability to develop those controls gives more consistency. Everybody knows now when you're dealing with transparency, or whatever the FIPPs requirement might be, there's a specific set of controls, the language is specified in the words of the privacy folks who understand the business, and they can now be applied uniformly across the agencies.

We also plan to develop some assessment procedures. We'll have uniform ways to assess those privacy controls, to see if they're actually effective in what they're trying to do. His main wanted to bring together - and it's very hard to do this, since the privacy officer and the security officer are totally separate, obviously, and have different legislative derivations-but yet, they have a lot of overlap.

In other words, if you want to have good privacy, you have to have a good foundation of security, especially in the area of confidentiality. It's kind of like a Venn diagram. There's a lot of things that privacy folks do to protect things from nondisclosure that are overlapping the security space.

FGIT: Changing subjects, I wonder if I can ask you about the privacy appendix [Appendix J].

Ross: That's brand new.

FGIT: Everybody knows that FISMA, through FIPS, leads to 800-53. How do privacy requirements get to 800-53?

Ross: The motivation to put the privacy controls came largely from our working with the CIO Council and the privacy subcommittee. There is legislation going back to the Privacy Act of 1974, kind of the equivalent of FISMA. There is also OMB policies that deal with privacy issues, and then there's the Fair Information Practice Principles--the FIPPs with two P's. That whole body of work, all three of those, motivated the development of the privacy controls.

The whole purpose was to develop a set of controls that were developed on the order of our security controls, same type of structure. It would allow more consistency as these controls were implemented across the different federal agencies. When you have the FIPPs, there were eight of those. And each of those principles drove a different family of privacy controls.

The ability to develop those controls gives more consistency. Everybody knows now when you're dealing with transparency, or whatever the FIPPs requirement might be, there's a specific set of controls, the language is specified in the words of the privacy folks who understand the business, and they can now be applied uniformly across the agencies.

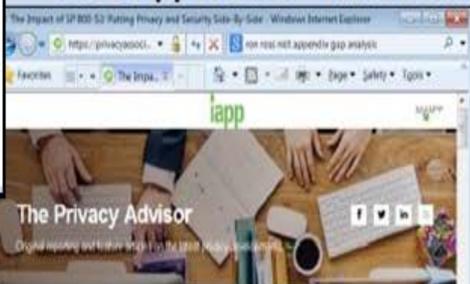
On the other hand, the privacy requirements go well beyond what security folks would ever be concerned about--how much data you can you collect on somebody, what can you use it for, how long can you retain it--all of those things are partnered with the larger Fair Information Practice Principles that our CIO Council, the privacy subcommittee, worked on.

We want to bring the worlds together, because they do depend on each other for success, and they have discipline and structure like we do with our security controls and make it a little bit easier for folks to plug the controls in and assess those controls to see if they're effective.

FGIT: The security community pretty much has to look at 800-53 for the controls they're going to implement. But the privacy community doesn't have to look at 800-53.

Ross: I guess the real answer to your question is it's a policy decision. A lot of this will depend on OMB and how they want to enforce those controls. I think just having them in the catalog now, and having that consistency--there was a lot of enthusiastic support for Appendix J, because it really gives them an anchor now in a fairly important publication. How those are actually implemented within every agency, I think that will be up to every agency, how they want to do that. We'll see what happens on the longer term on that one.

NIST Appendix J - Quick-Start Gap Analysis of Your Privacy Policy & Appendix J Controls



The Impact of SP 800-53: Putting Privacy and Security Side-By-Side



The Privacy Advisor | Jun 1, 2012

Already, 800-53 was the guidebook by which IT professionals in the federal government made sure they were complying with best practices established by NIST. Now, in the same kind of language and side-by-side with their security controls, they have Appendix J, which outlines the privacy controls by which everyone working with federal systems needs to comply. Appendix J was put together by the CIO Council Privacy Committee Best Practices Subcommittee, which Shaddox co-chairs with DHS Senior Director, Privacy Oversight, Martha Landesberg, and Claire Barrett, CPO at the Department of Transportation.

"By putting the privacy controls into this document, which has been around for a long time, we really wanted to elevate the privacy area to where security is," said Ron Ross, project leader of the FISMA Implementation Project at NIST. Even simply putting privacy in the name was a significant milestone.

"Security grabs a lot of the headlines," Ross said, "but privacy is very, very important, and it's getting more important all the time. With the increase in mobile devices and cloud computing and all of the digital information technology, we really wanted to make sure that privacy stands shoulder-to-shoulder with security to make sure they're equally important things that deserve attention."

It certainly resonates with Chris Brannigan, CIPP/US, CIPP/G, senior privacy analyst at the FAA. "That whole idea that you can't have security without privacy, that interaction has been building for a decade. Putting the word in the title makes it official...It recognizes that federal privacy professionals have some comparable standing to the certified IT security professionals, and even more important, that they have specialized knowledge, that they are subject matter experts that the IT security experts need."

Further, Brannigan feels the tone and language of the appendix are more important than you might think. "What these FISMA controls do is give the IT security group that's responsible some real language and rules that are written in their vocabulary," he said. "Everything that was written for the privacy policy in the past was written for attorneys. Now everything that was written for attorneys has been translated for IT."

There's a general recognition that these two groups need to come together more for the betterment of their organizations, and these new controls might be a practical way to bring them closer, said Ross. "Because of how we're organized, the security office and the privacy office are largely separate," he said. "They have different legislative mandates. There are OMB policies on both sides, but they're largely stove-piped...There are a lot of things you can do to fix that, and this was our contribution so that the organizations can benefit and get on with their missions."

So, what should privacy heads at government agencies do now?

What's the first order of business in complying with the new 800-53? Will there be a scramble?

Essentially, this is a great time to do a gap analysis, said NIST's Ross. "That's exactly what I would do," he said. "Go look at what's in Appendix J and then do a gap analysis to see if they're missing anything or if they need to change anything that they're already doing. And then they'll look at those things routinely after that."

He doesn't feel that most organizations will have to buy any new software or invest in much technology to meet the Appendix J controls. "I think a lot of the technology-related controls are on the security side," he said, "and the privacy controls will take advantage of that."

Essentially, this is a great time to do a gap analysis, said NIST's Ross.

"That's exactly what I would do," he said.

"Go look at what's in Appendix J and then do a gap analysis to see if they're missing anything or if they need to change anything that they're already doing.

And then they'll look at those things routinely after that."

NIST Appendix J - Quick-Start Gap Analysis of Your Privacy Policy & Appendix J Controls

QUICK START GUIDE
to a
GAP ANALYSIS
between the requirements of an
AGENCY PRIVACY POLICY
and
NIST SP 800-53 Rev 4
Appendix J

NIST Appendix J - Quick Start Gap Analysis of A Privacy Policy & Appendix J Controls

#	Control Family Name	Control Name	Control Number	DESCRIPTION - "The organization..."	Policy Includes (Y/N or Part?)	Policy Clauses (Y/N or Part, clause?)	IF Partial, Note what is needed for full inclusion
1	Authority & Purpose	Authority To Collect	AP-1	Determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PI), either generally or in support of a specific program or information system need.			
2	Authority & Purpose	Purpose Specification	AP-2	Describes the purposes for which personally identifiable information (PI) is collected, used, maintained, and shared in its privacy notices.			
3	Accountability, Audit, & Risk Management	Governance & Privacy	AR-1	Appoints a Senior Agency official for Privacy (SAC/PI) or Privacy officer (CPO), accountable for developing, implementing, and maintaining an organization-wide privacy program and oversees compliance with all applicable laws and			

NIST Appendix J - Quick Start Gap Analysis of A Privacy Policy & Appendix J Controls

#	Control Family Name	Control Name	Control Number	DESCRIPTION - "The organization..."	Policy Includes (Y/N or Part?)	Policy Clauses (Y/N or Part, clause?)	IF Partial, Note what is needed for full inclusion
4	Accountability, Audit, & Risk Management	Govt Privacy	AR-2	Includes privacy requirements in contracts and other agreement-related documents.			
5	Accountability, Audit, & Risk Management	Govt Privacy	AR-3	AR-3.b			
6	Accountability, Audit, & Risk Management	Govt Privacy	AR-4	Monitors and audits privacy controls and internal privacy policy (management organization-defined frequency) to ensure effective implementation.			

NIST Appendix J - Quick Start Gap Analysis of A Privacy Policy & Appendix J Controls

#	Control Family Name	Control Name	Control Number	DESCRIPTION - "The organization..."	Policy Includes (Y/N or Part?)	Policy Clauses (Y/N or Part, clause?)	IF Partial, Note what is needed for full inclusion
7	Accountability, Audit, & Risk Management	Govt Privacy	AR-5	AR-5.a			
8	Accountability, Audit, & Risk Management	Govt Privacy	AR-6	AR-6.a			
9	Accountability, Audit, & Risk Management	Privacy Risk A	AR-7	AR-7.a			
10	Accountability, Audit, & Risk Management	Privacy Risk A	AR-8	AR-8.a			
11	Accountability, Audit, & Risk Management	Privacy Risk A	AR-9	AR-9.a			

NIST Appendix J - Quick Start Gap Analysis of A Privacy Policy & Appendix J Controls

#	Control Family Name	Control Name	Control Number	DESCRIPTION - "The organization..."	Policy Includes (Y/N or Part?)	Policy Clauses (Y/N or Part, clause?)	IF Partial, Note what is needed for full inclusion
12	Data Quality & Integrity	Data Quality	DI-1.b	Collects PI directly from the individual to the greatest extent practicable.			
13	Data Quality & Integrity	Data Quality	DI-1.c	Checks for, and corrects as necessary, any inaccurate or outdated PI used by its programs or systems (management organization-defined frequency), and issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.			
14	Data Quality & Integrity	Data Integrity & Data Retention	DI-2	Documents processes to ensure the integrity of personally identifiable information (PI) through routine security controls and			

NIST Appendix J - Quick Start Gap Analysis of A Privacy Policy & Appendix J Controls

#	Control Family Name	Control Name	Control Number	DESCRIPTION - "The organization..."	Policy Includes (Y/N or Part?)	Policy Clauses (Y/N or Part, clause?)	IF Partial, Note what is needed for full inclusion
15	Data Quality & Integrity	Data Data	DI-3	Develops policies and procedures that minimize the use of personally identifiable information (PI) for testing, training, and research, and			
16	Data Quality & Integrity	Data Minimization & Retention	DI-3	Implements controls to protect PI used for testing, training, and research.			
17	Data Quality & Integrity	Data Minimization & Retention	DI-3	DI-3.b			
18	Data Quality & Integrity	Data Minimization & Retention	DI-3	DI-3.c			
19	Data Quality & Integrity	Data Minimization & Retention	DI-3	DI-3.d			
20	Data Quality & Integrity	Data Minimization & Retention	DI-3	DI-3.e			

NIST Appendix J - Quick Start Gap Analysis of A Privacy Policy & Appendix J Controls

#	Control Family Name	Control Name	Control Number	DESCRIPTION - "The organization..."	Policy Includes (Y/N or Part?)	Policy Clauses (Y/N or Part, clause?)	IF Partial, Note what is needed for full inclusion
21	Data Quality & Integrity	Data Minimization & Retention	DI-3	DI-3.f			
22	Data Quality & Integrity	Data Minimization & Retention	DI-3	DI-3.g			

NIST Appendix J - Quick Start Gap Analysis of A Privacy Policy & Appendix J Controls

#	Control Family Name	Control Name	Control Number	DESCRIPTION - "The organization..."	Policy Includes (Y/N or Part?)	Policy Clauses (Y/N or Part, clause?)	IF Partial, Note what is needed for full inclusion
23	Individual Participation & Redress	Individual Participation & Redress	IP-3.b	Establishes a process for disseminating corrections or amendments of the PI to other authorized users of the PI, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.			
24	Individual Participation & Redress	Complaint Management	IP-4	Implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.			

NIST Appendix J - Quick Start Gap Analysis of A Privacy Policy & Appendix J Controls

#	Control Family Name	Control Name	Control Number	DESCRIPTION - "The organization..."	Policy Includes (Y/N or Part?)	Policy Clauses (Y/N or Part, clause?)	IF Partial, Note what is needed for full inclusion
25	Security	Individual Participation & Redress	IP-4	Establishes, maintains, and updates management organization-defined processes to			
26	Security	Records Notices & Privacy Act Statements	TR-2.a	Publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PI).			
27	Transparency	Records Notices & Privacy Act Statements	TR-2.b	Keeps SORNs current, and			
28	Transparency	Records Notices & Privacy Act Statements	TR-2.c	Includes Privacy Act statements on its forms that collect PI, or on separate forms that can be related by individuals, to provide additional formal notice to individuals from whom the information is being collected.			
29	Transparency	Dissemination of Privacy Program Information	TR-3.a	Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency official for Privacy (SAC/PI) or Privacy officer (CPO), and			
30	Transparency	Dissemination of Privacy Program Information	TR-3.b	Ensures that its privacy practices are publicly available through organizational websites or otherwise.			
31	Use Limitation	Internal Use	UL-1	Uses personally identifiable information (PI) internally only for the authorized purposes identified in the Privacy Act and/or in public notices.			
32	Use Limitation	Information Sharing With Third Parties	UL-2.a	Shares personally identifiable information (PI) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notices, or for a purpose that is compatible with those purposes.			
33	Use Limitation	Information Sharing With Third Parties	UL-2.b	Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements with third parties that specifically describe the PI covered and specifically enumerate the purposes for which the PI may be used.			
34	Use Limitation	Information Sharing With Third Parties	UL-2.c	Monitors, audits, and trains its staff on the authorized sharing of PI with third parties and on the consequences of unauthorized use or sharing of PI, and			
35	Use Limitation	Information Sharing With Third Parties	UL-2.d	Evaluates any proposed new instances of sharing PI with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.			

NIST Appendix J - Quick-Start Gap Analysis of A Privacy Policy & Appendix J Controls

#	Control Family Name	Control Name	Control Number	DESCRIPTION – “The organization...	Policy includes: Y/N/ or Partial?	Policy Citation (If Y or Partial, citation)?	If Partial; Note what is needed for full inclusion:
1	Authority & Purpose	Authority To Collect	AP-1	Determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need.			
2	Authority & Purpose	Purpose Specification	AP-2	Describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.			
3	Accountability, Audit, & Risk Management	Governance & Privacy Program	AR-1 a.	Appoints a Senior Agency official for Privacy (SAOP)/Chief Privacy officer (CPO) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems;			
4	Accountability, Audit, & Risk Management	Governance & Privacy Program	AR-1 b.	Monitors federal privacy laws and policy for changes that affect the privacy program;			
5	Accountability, Audit, & Risk Management	Governance & Privacy Program	AR-1 c.	Allocates [Assignment: organization-defined allocation of budget and staffing] sufficient resources to implement and operate the organization-wide privacy program;			
6	Accountability, Audit, & Risk Management	Governance & Privacy Program	AR-1 d.	Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures;			
7	Accountability, Audit, & Risk Management	Governance & Privacy Program	AR-1 e.	Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and			
8	Accountability, Audit, & Risk Management	Governance & Privacy Program	AR-1 f.	Updates privacy plan, policies, and procedures [Assignment: organization-defined frequency, at least biennially].			
9	Accountability, Audit, & Risk Management	Privacy Impact & Risk Assessment	AR-2 a.	Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and			
10	Accountability, Audit, & Risk Management	Privacy Impact & Risk Assessment	AR-2 b.	Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.			
11	Accountability, Audit, & Risk Management	Privacy Requirements For Contractors & Service Providers	AR-3 a.	Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and			

NIST Appendix J - Quick-Start Gap Analysis of A Privacy Policy & Appendix J Controls

#	Control Family Name	Control Name	Control Number	DESCRIPTION – “The organization...	Policy includes: Y/N/ or Partial?	Policy Citation (if Y or Partial, citation)?	If Partial; Note what is needed for full inclusion:
12	Accountability, Audit, & Risk Management	Privacy Requirements For Contractors & Service Providers	AR-3 b.	Includes privacy requirements in contracts and other acquisition-related documents.			
13	Accountability, Audit, & Risk Management	Privacy Monitoring & Auditing	AR-4	Monitors and audits privacy controls and internal privacy policy [Assignment: organization-defined frequency] to ensure effective implementation.			
14	Accountability, Audit, & Risk Management	Privacy Awareness & Training	AR-5 a.	Develops, implements, & updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;			
15	Accountability, Audit, & Risk Management	Privacy Awareness & Training	AR-5 b.	Administers basic privacy training [Assignment: organization-defined frequency, at least annually] and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII [Assignment: organization-defined frequency, at least annually]; and			
16	Accountability, Audit, & Risk Management	Privacy Awareness & Training	AR-5 c.	Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements [Assignment: organization-defined frequency, at least annually].			
17	Accountability, Audit, & Risk Management	Privacy Reporting	AR-6	Develops, disseminates, and updates reports to the office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.			
18	Accountability, Audit, & Risk Management	Privacy-Enhanced System Design & Development	AR-7	Designs information systems to support privacy by automating privacy controls.			
19	Accountability, Audit, & Risk Management	Accounting of Disclosures	AR-8 a.	Keeps an accurate accounting of disclosures of information held in each system of records under its control, including:			
20	Accountability, Audit, & Risk Management	Accounting of Disclosures	AR-8 b.	Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and			
21	Accountability, Audit, & Risk Management	Accounting of Disclosures	AR-8 c.	Makes the accounting of disclosures available to the person named in the record upon request.			
22	Data Quality & Integrity	Data Quality	DI-1 a.	Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information;			

NIST Appendix J - Quick-Start Gap Analysis of A Privacy Policy & Appendix J Controls

#	Control Family Name	Control Name	Control Number	DESCRIPTION – “The organization...	Policy includes: Y/N/ or Partial?	Policy Citation (If Y or Partial, citation)?	If Partial; Note what is needed for full inclusion:
23	Data Quality & Integrity	Data Quality	DI-1 b.	Collects PII directly from the individual to the greatest extent practicable;			
24	Data Quality & Integrity	Data Quality	DI-1 c.	Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems [Assignment: organization-defined frequency]; and			
25	Data Quality & Integrity	Data Quality	DI-1 d.	Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.			
26	Data Quality & Integrity	Data Integrity & Data Integrity Board	DI-2	Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and			
27	Data Quality & Integrity	Data Integrity & Data Integrity Board	DI-2	Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements[1] and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.			
28	Data Minimization & Retention	Minimization of Personally Identifiable Information	DM-1 a.	Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection;			
29	Data Minimization & Retention	Minimization of Personally Identifiable Information	DM-1 b.	Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice & for which the individual has provided consent; and			
30	Data Minimization & Retention	Minimization of Personally Identifiable Information	DM-1 c.	Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings [Assignment: organization-defined frequency, at least annually] to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.			
31	Data Minimization & Retention	Data Retention & Disposal	DM-2 a.	Retains each collection of personally identifiable information (PII) for [Assignment: organization-defined time period] to fulfill the purpose(s) identified in the notice or as required by law;			
32	Data Minimization & Retention	Data Retention & Disposal	DM-2 b.	Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and			
33	Data Minimization & Retention	Data Retention & Disposal	DM-2 c.	Uses [Assignment: organization-defined techniques or methods] to ensure secure deletion or destruction of PII (including originals, copies, and archived records).			

NIST Appendix J - Quick-Start Gap Analysis of A Privacy Policy & Appendix J Controls

#	Control Family Name	Control Name	Control Number	DESCRIPTION – “The organization...	Policy includes: Y/N/ or Partial?	Policy Citation (If Y or Partial, citation)?	If Partial; Note what is needed for full inclusion:
34	Data Minimization & Retention	Minimization of PII Used In Testing, Training, & Research	DM-3	Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and			
35	Data Minimization & Retention	Minimization of PII Used In Testing, Training, & Research	DM-3	Implements controls to protect PII used for testing, training, and research.			
36	Individual Participation & Redress	Consent	IP-1 a.	Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection;			
37	Individual Participation & Redress	Consent	IP-1 b.	Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;			
38	Individual Participation & Redress	Consent	IP-1 c.	Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and			
39	Individual Participation & Redress	Consent	IP-1 d.	Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.			
40	Individual Participation & Redress	Individual Access	IP-2 a.	Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records;			
41	Individual Participation & Redress	Individual Access	IP-2 b.	Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records;			
42	Individual Participation & Redress	Individual Access	IP-2 c.	Publishes access procedures in System of Records Notices (SORNs); and			
43	Individual Participation & Redress	Individual Access	IP-2 d.	Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.			
44	Individual Participation & Redress	Redress	IP-3 a.	Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and			

NIST Appendix J - Quick-Start Gap Analysis of A Privacy Policy & Appendix J Controls

#	Control Family Name	Control Name	Control Number	DESCRIPTION – “The organization...	Policy includes: Y/N/ or Partial?	Policy Citation (If Y or Partial, citation)?	If Partial; Note what is needed for full inclusion:
45	Individual Participation & Redress	Redress	IP-3 b.	Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.			
46	Individual Participation & Redress	Complaint Management	IP-4	Implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.			
47	Security	Inventory of Personally Identifiable Information	SE-1 a.	Establishes, maintains, and updates [Assignment: organization-defined frequency] an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and			
48	Security	Inventory of Personally Identifiable Information	SE-1 b.	Provides each update of the PII inventory to the CIO or information security official [Assignment: organization-defined frequency] to support the establishment of information security requirements for all new or modified information systems containing PII.			
49	Security	Privacy Incident Response	SE-2 a.	Develops and implements a Privacy Incident Response Plan; and			
50	Security	Privacy Incident Response	SE-2 b.	Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.			
51	Transparency	Privacy Notice	TR-1 a.	Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary;			
52	Transparency	Privacy Notice	TR-1 b.	Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and			
53	Transparency	Privacy Notice	TR-1 c.	Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.			

NIST Appendix J - Quick-Start Gap Analysis of A Privacy Policy & Appendix J Controls

#	Control Family Name	Control Name	Control Number	DESCRIPTION – “The organization...	Policy includes: Y/N/ or Partial?	Policy Citation (If Y or Partial, citation)?	If Partial; Note what is needed for full inclusion:
54	Transparency	System of Records Notices & Privacy Act Statements	TR-2 a.	Publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII);			
55	Transparency	SORNs & Privacy Act Statements	TR-2 b.	Keeps SORNs current; and			
56	Transparency	System of Records Notices & Privacy Act Statements	TR-2 c.	Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.			
57	Transparency	Dissemination of Privacy Program Information	TR-3 a.	Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency official for Privacy (SAOP)/Chief Privacy officer (CPO); and			
58	Transparency	Dissemination of Privacy Program Information	TR-3 b.	Ensures that its privacy practices are publicly available through organizational websites or otherwise.			
59	Use Limitation	Internal Use	UL-1	Uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.			
60	Use Limitation	Information Sharing With Third Parties	UL-2 a.	Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes;			
61	Use Limitation	Information Sharing With Third Parties	UL-2 b.	Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used;			
62	Use Limitation	Information Sharing With Third Parties	UL-2 c.	Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and			
63	Use Limitation	Information Sharing With Third Parties	UL-2 d.	Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.			

*To Adapt the Gap Analysis Template
to a survey of Metrics and Roles & Responsibilities.....*

Replace the provided Gap Analysis Headings

Policy Includes? Y/N	Policy Citation if Y?	If Partial, what is needed for inclusion?
-------------------------------------	----------------------------------	--

With Appropriate Categories as applicable...

Policy Gap	Metric	R&R
Policy Citation?	Existing Metric?	Responsible Party?

NIST Appendix J - Quick-Start Gap Analysis of A Privacy Policy & Appendix J Controls

#	Control Family Name	Control Name	Control Number	DESCRIPTION – “The organization...	Policy Citation?	Existing Metric?	Responsible Party?
1	Authority & Purpose	Authority To Collect	AP-1	Determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need.			
2	Authority & Purpose	Purpose Specification	AP-2	Describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.			
3	Accountability, Audit, & Risk Management	Governance & Privacy Program	AR-1 a.	Appoints a Senior Agency official for Privacy (SAOP)/Chief Privacy officer (CPO) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems;			
4	Accountability, Audit, & Risk Management	Governance & Privacy Program	AR-1 b.	Monitors federal privacy laws and policy for changes that affect the privacy program;			
5	Accountability, Audit, & Risk Management	Governance & Privacy Program	AR-1 c.	Allocates [Assignment: organization-defined allocation of budget and staffing] sufficient resources to implement and operate the organization-wide privacy program;			
6	Accountability, Audit, & Risk Management	Governance & Privacy Program	AR-1 d.	Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures;			
7	Accountability, Audit, & Risk Management	Governance & Privacy Program	AR-1 e.	Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and			
8	Accountability, Audit, & Risk Management	Governance & Privacy Program	AR-1 f.	Updates privacy plan, policies, and procedures [Assignment: organization-defined frequency, at least biennially].			
9	Accountability, Audit, & Risk Management	Privacy Impact & Risk Assessment	AR-2 a.	Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and			
10	Accountability, Audit, & Risk Management	Privacy Impact & Risk Assessment	AR-2 b.	Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.			
11	Accountability, Audit, & Risk Management	Privacy Requirements For Contractors & Service Providers	AR-3 a.	Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and			

**Policy
Citation?**

**Existing
Metric?**

**Responsible
Party?**

**Yes - Citation:
(agency Privacy
Policy 3.2.a)**

**Yes - Citation:
(PIAs in FISMA
SAOP Report)**

**Yes - Citation:
(Privacy Policy 1.2.b
assigns to CPO)**

**Yes - Citation:
(IT Security
Policy 5.2.2.c)**

NO

**Yes - Citation:
(Privacy Policy 1.5.d
to System Owner)**

Thank you!
and
Good Luck with your Gap Analysis!

Christopher J. Brannigan, CIPP/US, CIPP/G
Privacy Officer, IT Security & Privacy
Office of the Chief Information Officer
US Office of Personnel Management



Claire Barrett

Chief Privacy Officer

U.S. Department of Transportation



Jonathan Cantor

Deputy Chief Privacy Officer

U.S. Department of Homeland Security

NIST 800-53 Rev. 4 Privacy Controls

Jonathan Cantor
Deputy Chief Privacy Officer
DHS Privacy Office
June 9, 2015



Appendix J Basics

**ALL YOU EVER WANTED
TO KNOW AND THEN
SOME!**



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*

Familiar Territory



FIPPs and Controls may be unfamiliar territory to security staff, but **should be familiar to privacy staff**

DHS Privacy Impact Assessment – Based on FIPPs

1. Authorities and Other Requirements
2. Characterization of the Information
3. Uses of the Information
4. Notice
5. Data Retention by the project
6. Information Sharing
7. Redress
8. Auditing and Accountability



**Privacy Impact Assessment
for the
Performance and Learning Management System
(PALMS)**

DHS/ALL/PIA-049

January 23, 2015

Privacy Controls Based on FIPPs

FIPPs = Privacy Controls

Privacy Controls = FIPPs



Privacy Controls	
AP	Authority & Purpose
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	Accountability, Audit, & Risk Management
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-6	Privacy Reporting
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	Data Quality & Integrity
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Review Board
DM	Data Minimization
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	Individual Participation and Redress
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	Security
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	Transparency
TR-1	Privacy Notice
TR-2	System of Records Notice and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	Use Limitation
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Why Do We Need Privacy Controls?

The government is reading your tweets

By Dean Obeidallah, Special to CNN



... event? Catch our live blog

CNET › News › Technically Incorrect › Court to TSA: Hey, what about your nude ...

Court to TSA: Hey, what about your nude scanners?

A federal court wonders why the TSA hasn't held public hearings or issued rules about its nude scanners, even though it was ordered to a year ago.



ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

HOME

ABOUT

OUR WORK

DEEPLINKS BLOG

PRESS ROOM

DECEMBER 21, 2011 | BY MARK M. JAYCOX



New Agreement Between the United States and Europe Will Compromise the Privacy Rights of International Travelers

Understanding Controls



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

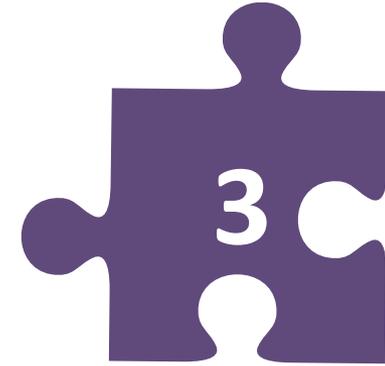
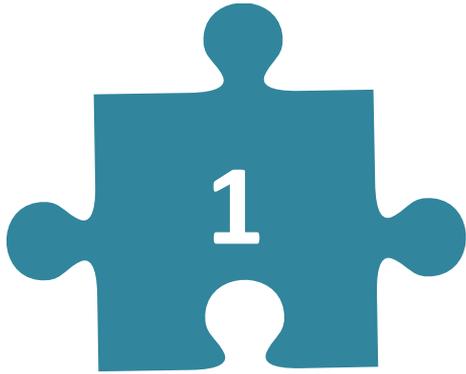
Hybrid Controls

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.

Implementation Planning by SAOP



Establish Organization Approach

- Determine “common” controls
 - Set assignment parameters where applicable
- Determine system/program controls
- Document and Approve Plan
- Disseminate and Educate
- Implement “common” controls

System/Program Implementation

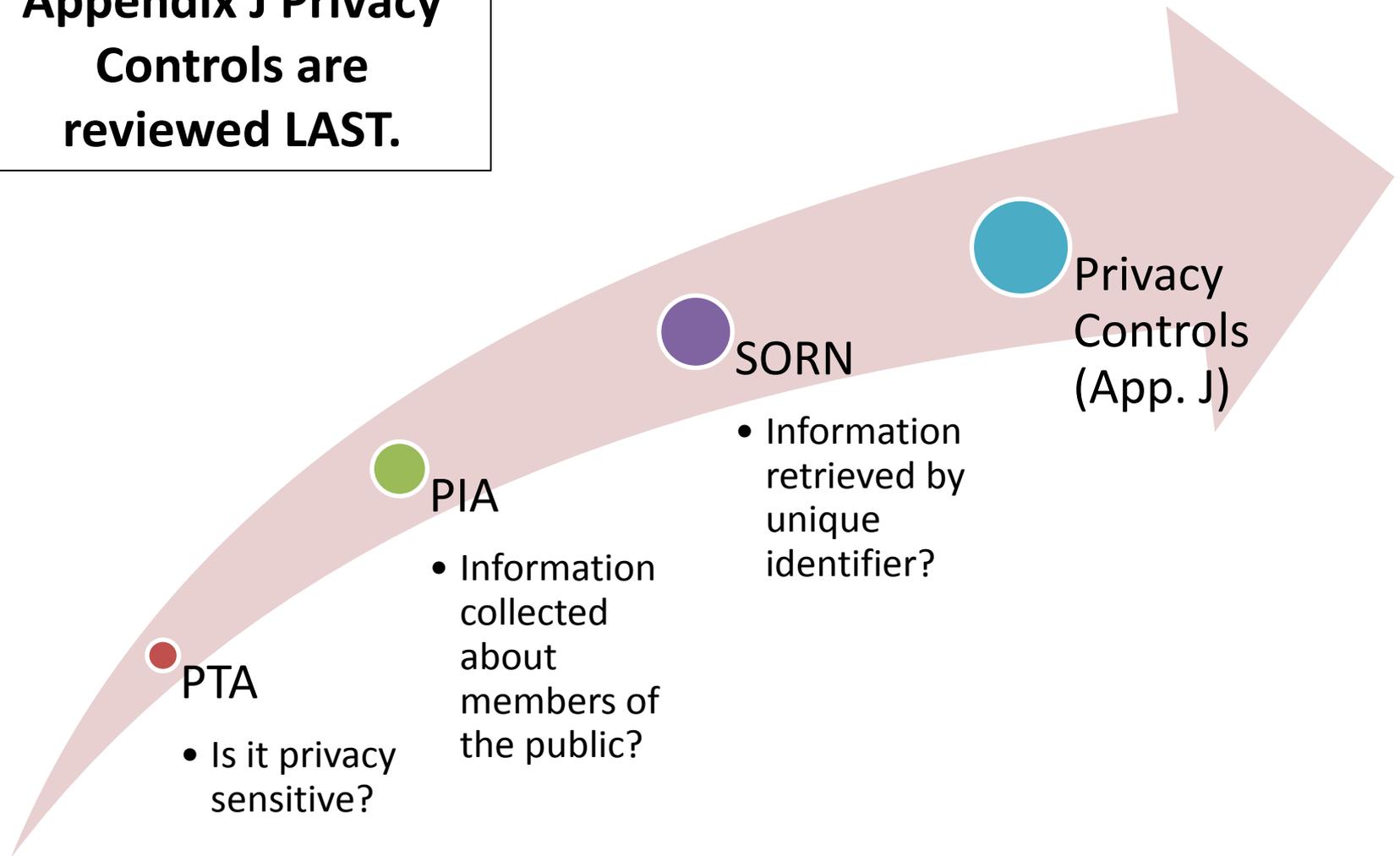
- Select and implement privacy controls based on organization’s privacy requirements and the need to protect PII
 - PTA
- May coordinate privacy control selection and implementation with mission/business owners, CISO, CIO
- Implement the optional control enhancements when there is a demonstrated need for additional protection
- Document outcomes
 - PIA
 - SORN

Assess Compliance

- Develop Assessment Plan
 - 800-53A (under development)
- Conduct Assessment
 - Are controls implemented?
 - Do the controls reduce risk as intended?
- Remediate

Privacy Compliance Analysis Process

Appendix J Privacy Controls are reviewed LAST.



When does Appendix J apply to me?

- Now 😊
- New systems:
 - Privacy Controls included as of April 1, 2014
- Legacy systems are moving or already have moved into compliance with NIST SP 800-53 Rev. 4 .



Implementation of Privacy Controls

1. **Update security policies to reflect new Appendix J controls and SAOP 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 FISMA compliance tool**



2014: New SAOP Authority in Security Authorization Process

NIST 800-53 Rev. 4 Appendix J

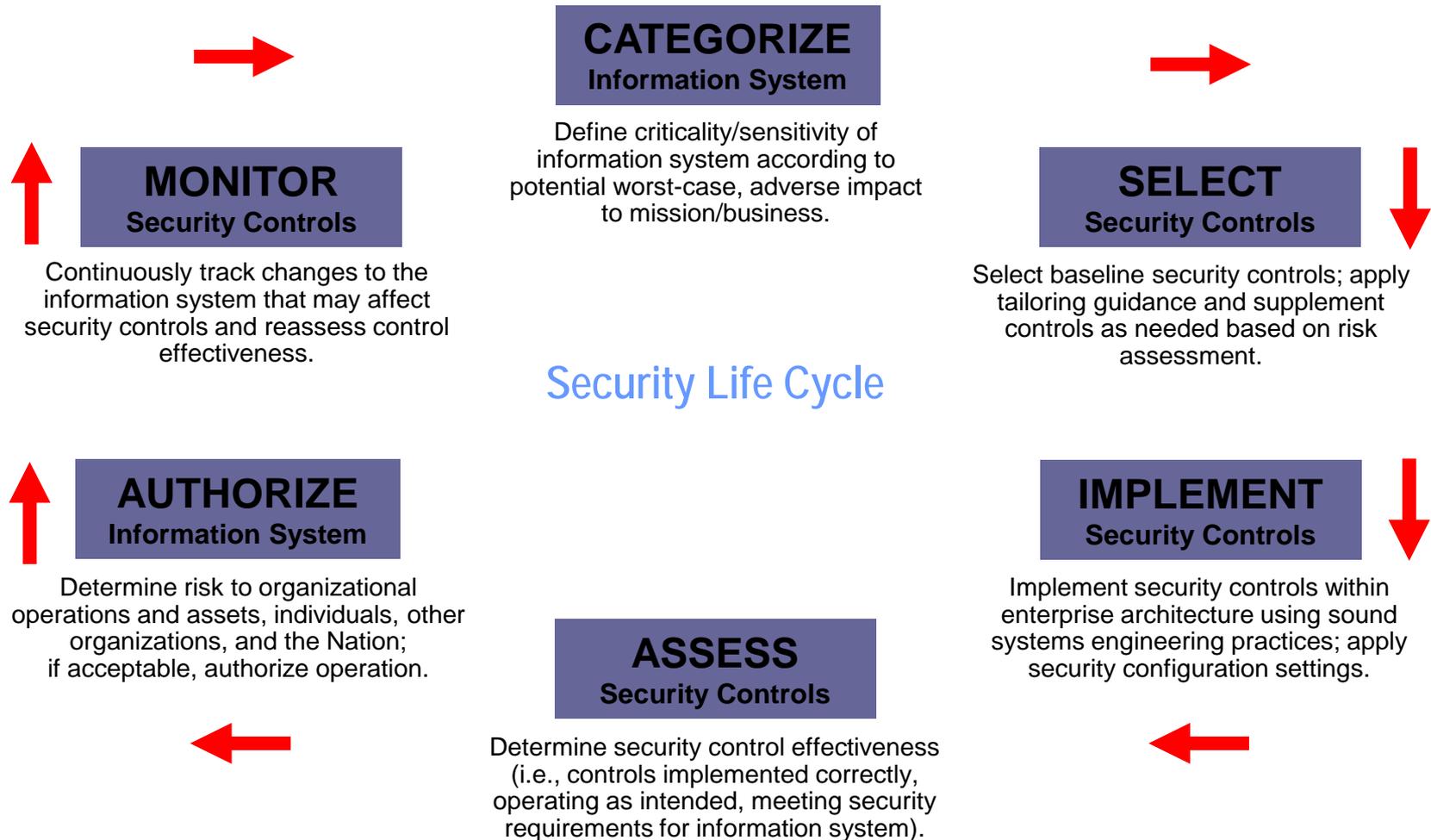
- Assessments of privacy controls can be conducted either by the Senior Agency Official for Privacy (SAOP) or Chief Privacy Officer (CPO) *alone or jointly* with ...the information security office. (pg. J-4)

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

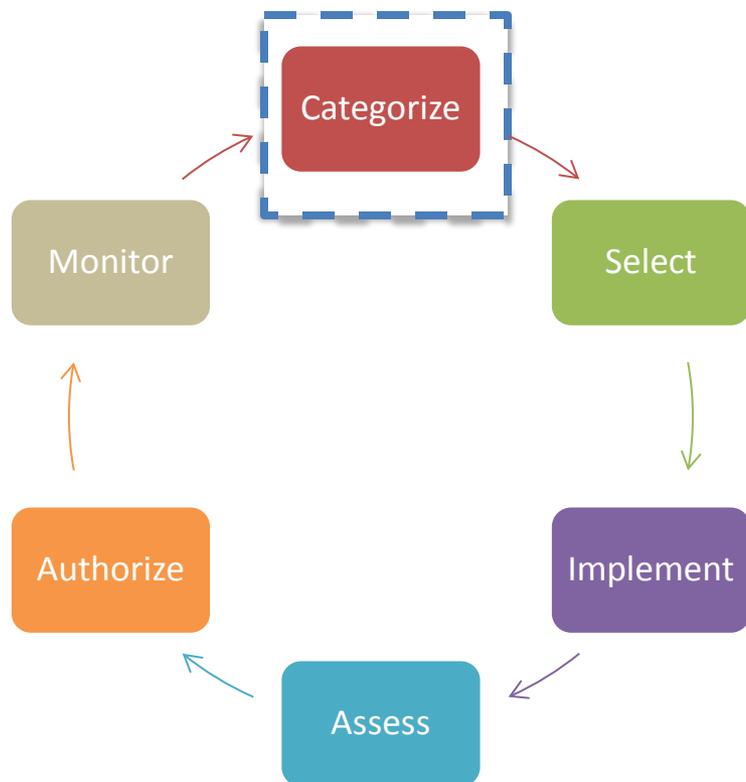
- **SAOPs are responsible for the implementation of Appendix J.**
- SAOPs may consult with CISOs, but the authority for the selection/ assessment of privacy controls rests with SAOP.
- SAOP makes determination which controls may be considered “common controls.”
- **SAOP approval required as a precondition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

Risk Management Framework (RMF)

Starting Point



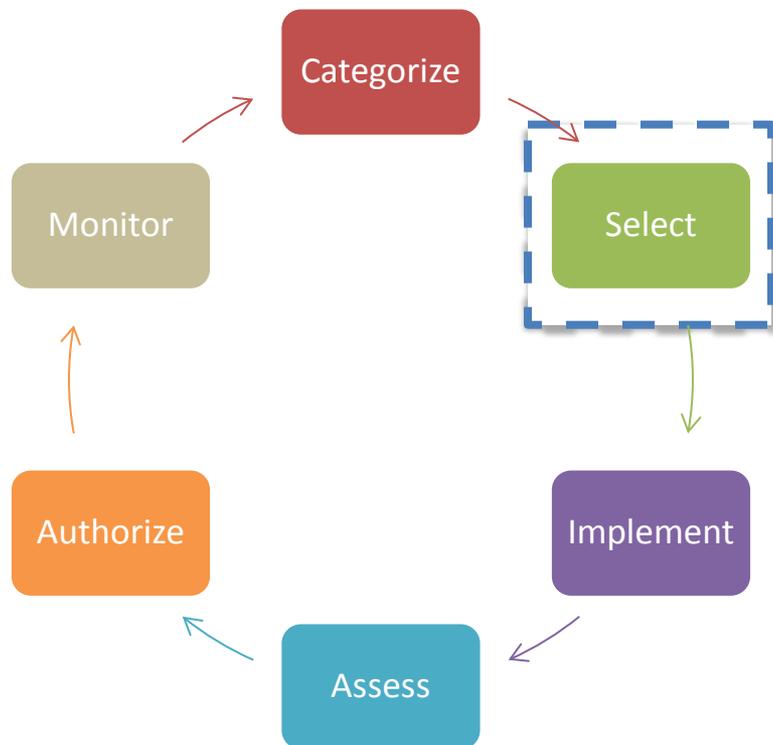
Using the RMF to assess Privacy Controls



Categorize:

- ISSOs complete PTA
- PTAs submitted to Privacy Office for review
- Privacy Office makes determination whether system/program is **privacy sensitive**

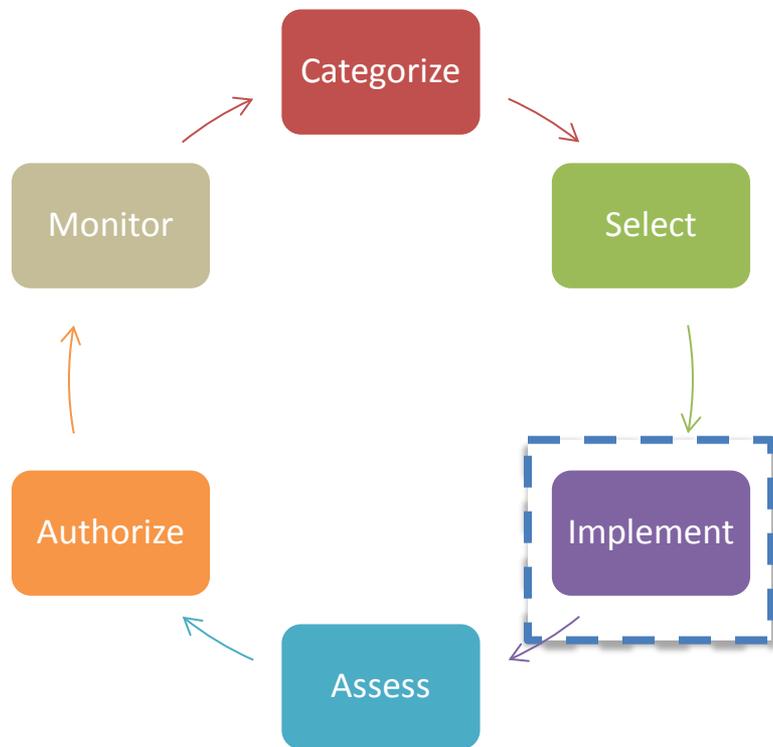
Using the RMF to assess Privacy Controls



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

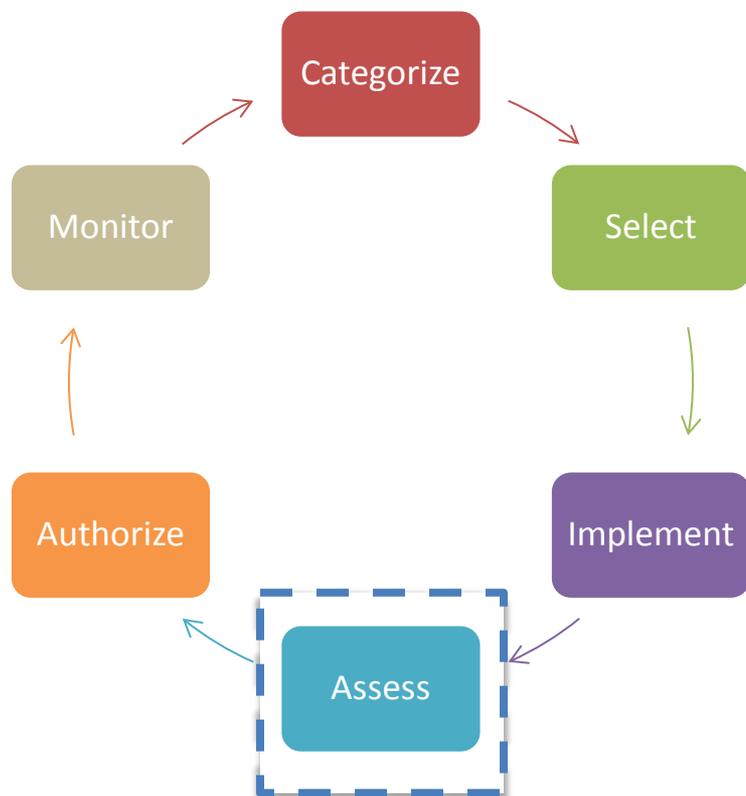


Implement:

- 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:

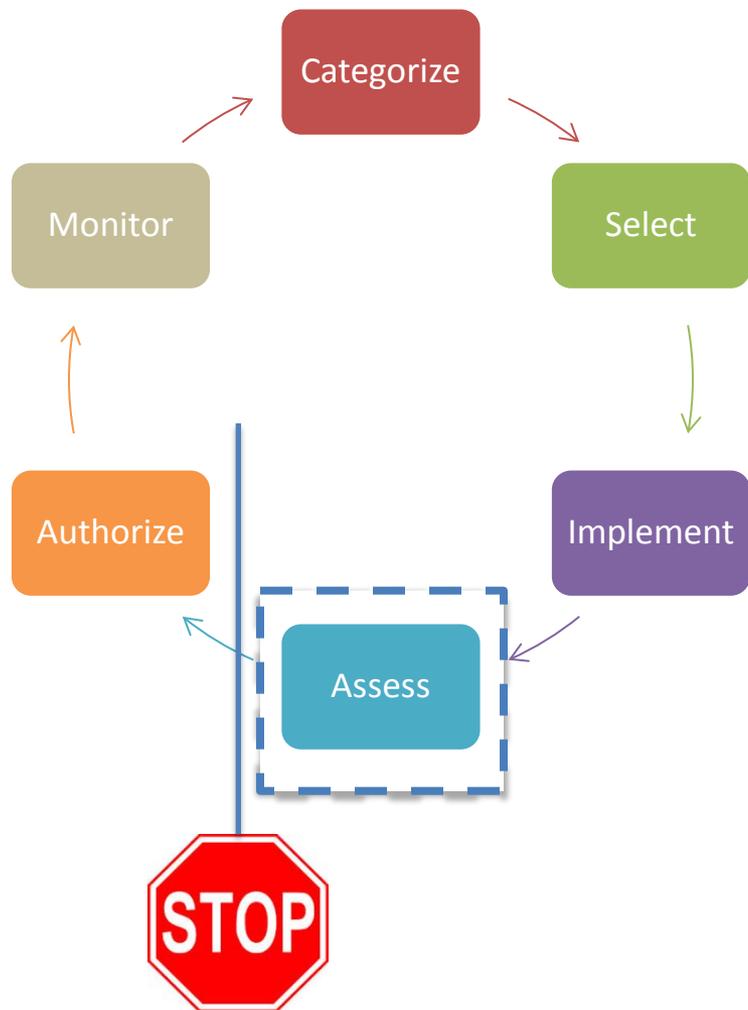
- *Has the system/program completed the Implementation Language*
- Privacy analysts will assess each control based on the privacy compliance documentation already submitted
- **A complete PIA and SORN will satisfy almost all of the system/program controls**

Tricky controls

- **Most controls are met by a complete PIA/SORN**
- **However, three are not captured in most PIAs:**
 - AR-3: Contracts
 - AR-5: Certification of Training
 - AR-8: Accounting of Disclosures
- **Reach out to Privacy Officer for answers to these controls if not identifiable from compliance documents**



Using the RMF to assess Privacy Controls



Authorize:

- System must have affirmative SAOP assessment of privacy controls ***before*** asking for **Authorization to Operation (ATO)**

Adjudicating Controls

- Who adjudicates the privacy controls for your systems? Your Privacy Office!
- PIA and/or SORN required?
 - PIA and/or SORN completed?
 - All controls should pass.
 - PIA and/or SORN **NOT** completed?
 - All controls should **FAIL**.



POA&Ms and Waivers

- What if your system needs an ATO but hasn't met the Appendix J requirements?
- Plan ahead
- **Cannot** waive legal requirements
 - PIA and SORN are both legally required by Privacy Act and E-Government Act

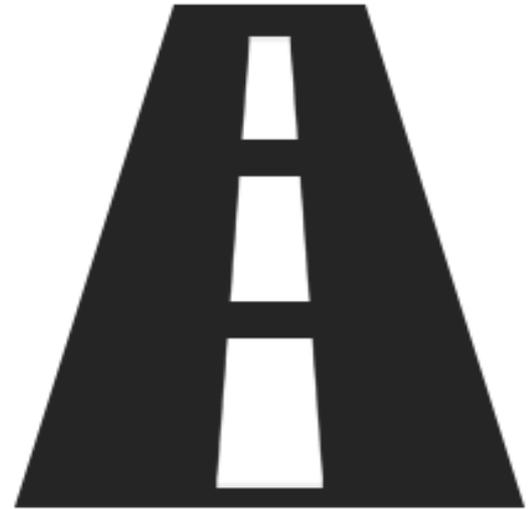
Bottom Line for ISSOs

- Privacy Office has the sole authority for assessing and adjudicating privacy controls.
- Privacy Office selects, implements, and assesses ALL privacy controls.
 - Privacy Plans document analyst selections/notes
- No ATO unless privacy controls are complete.



New challenges...

- POA&Ms and Waivers
- Metrics
- Appendix J controls apply beyond FISMA reportable systems
- Ongoing authorization
- Shared services
- New technologies (Agile, etc.)



Privacy and Security Success Story

- Improved coordination and communication between CISO and SAOP
- Privacy embedded in Risk Management Process





Jonathan Cantor

jonathan.cantor@hq.dhs.gov

Privacy Office: 202-343-1717



Guest Panelists Q&A

Chris Brannigan

Privacy Officer
IT Security & Privacy
Office of the Chief Information Officer
U.S. Office of Personnel Management

Jonathan Cantor

Deputy Chief Privacy Officer
U.S. Department of Homeland Security

Claire Barrett

Chief Privacy Officer
U.S. Department of Transportation

Thanks for Attending!

- Thank you for attending the 2015 VA Privacy Service “Privacy Matters” Symposium.
 - We value your feedback, opinions and comments!
 - After this session, you will receive a short questionnaire via email. Please take a moment to complete upon receipt.
- To self-certify Lync Meeting attendance in the Talent Management System (TMS), search:
 - **Item Title:** VA Privacy Symposium 2015: Session I - Understanding NIST 800-53 Rev 4, Appendix J Privacy Control Cat
 - **TMS ID:** VA 3941837
- Visit the new VA Privacy Service website at <http://www.oprm.va.gov> to learn more about Privacy within VA.