

MITRE PRODUCT



Privacy Maturity Model

Version 1

MITRE Privacy Engineering Capability

October 20, 2019

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

©2019 The MITRE Corporation.
All rights reserved.

McLean, VA

Approved for Public Release; Distribution Unlimited. 19-3384

Table of Contents

1	Introduction	3
2	How to Use This Document	3
3	Elements of a Privacy Program	3
3.1	Sub-Elements of a Privacy Program	4
4	Steps for Completing and Documenting a Privacy Program Analysis	6
5	References	7
	Appendix A: Privacy Program Analysis Matrix	8
5.1.1	Element 1.0: Leadership & Organization	8
5.1.2	Element 2.0: Privacy Risk Management.....	15
5.1.3	Element 3.0: Engineering & Information Security	29
5.1.4	Element 4.0: Incident Response.....	32
5.1.5	Element 5.0: Individual Participation, Transparency, & Redress.....	35
5.1.6	Element 6.0: Privacy Training & Awareness	41
5.1.7	Element 7.0: Accountability	44
	Appendix B: Summary of Privacy Program Analysis Results	47

1 Introduction

This document provides a framework for developing, implementing, maintaining, and evaluating privacy programs within organizations. Privacy programs must be comprehensive enough to address all requirements established by authoritative sources (e.g., laws, regulations, guidance), and must be supported by written policies, appropriate training, ongoing practices, and appropriate assessment. This document may be used to assess both the *completeness* (whether an organization has identified and implemented all elements of a privacy program), and *maturity level* (an evaluation of to what degree practices supporting each element are effective in achieving their intended purpose) of a privacy program. The framework was developed based not only on comprehensive research of relevant laws and guidance, but on practices that have been assessed as effective in many organizations.

This document was developed by members of MITRE’s privacy engineering capability. For questions or comments regarding the document, please send a message to privacy@mitre.org.

2 How to Use This Document

Privacy professionals will use this document in support of organizations, including executives charged with creating or assessing privacy programs, as a guide for developing, implementing, and maintaining such programs and for assessing the implementation, effectiveness, and sustainability of all components of a privacy program.

3 Elements of a Privacy Program

This document enables strategic planning by providing a framework of core privacy program capabilities and criteria that can be used to measure progress toward achieving a program’s target state. The model is based on concepts in foundational laws and guidance applicable to U.S. federal government organizations and also usable by non-federal organizations, including in the private sector, given that the foundational privacy principles are the same across sectors. The core foundation for the framework is a set of seven privacy elements of a privacy program.¹ These elements are provided in the table below.

Element	Description
1.0: Leadership & Organization	Providing organizational support for privacy program priorities and initiatives
2.0: Privacy Risk Management	Using methods and processes to identify, assess, prioritize, and manage privacy risk, including within IT investment, acquisition, and contract management processes.
3.0: Engineering & Information Security	Incorporating privacy into the enterprise systems engineering approach and integrating with cybersecurity
4.0: Incident Response	Managing and responding to privacy incidents, including breaches
5.0: Individual Participation, Transparency & Redress	Informing data subjects and the public regarding information about individuals the organization collects and uses, and how the public may pursue inquiries and complaints

¹ Based on a Federal CIO Council Privacy Committee White Paper entitled *Best Practices: Elements of a Federal Privacy Program*, June 30, 2010

6.0: Privacy Training & Awareness	Establishing and maintaining workforce training and a culture of privacy awareness
7.0: Accountability	Enforcing the responsibility of the organization to implement privacy principles and requirements and to respond to concerns expressed by individuals and the general public

Table 1. Elements of a Privacy Program.

3.1 Sub-Elements of a Privacy Program

The sub-elements of a privacy program are identified in the table below.

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

		2.17 Privacy Risk & Issue Tracking					
--	--	---	--	--	--	--	--

Table 2. Sub-Elements of a Privacy Program

4 Steps for Completing and Documenting a Privacy Program Analysis

In order to complete a privacy program analysis, the privacy program must complete the following steps:

Step 1: Review the table in Appendix A, Privacy Program Analysis Matrix. The sub-element descriptions describe two kinds of program requirements. Most of the sub-elements are requirements listed in laws and guidance for U.S. federal government agencies, e.g., Office of Management and Budget (OMB) Memoranda or National Institute of Standards and Technology (NIST) standards and guidance. The concepts represented are usable by private sector and other non-federal organizations as well since foundational privacy concepts are the same across sectors. Other sub-elements identify actions taken by various organizations that have been necessary to meet and sustain compliance with requirements. This document uses the term “effective practices” for sub-elements that are necessary but not explicitly required by external authorities. While, theoretically, organizations may be able to address most requirements without explicitly addressing or assessing their effective practices, they will find implementing these practices useful and in most cases critical to effectively managing privacy.

Step 2. For each sub-element listed in the Privacy Program Analysis Matrix in Appendix A, identify the organization’s current and target levels of maturity. A maturity level is a characterization of the degree to which a privacy protection has been integrated into the organization’s infrastructure. The definitions of the five maturity levels used in this Privacy Maturity Model are provided in Table 3, Privacy Maturity Level Descriptions, below. The maturity levels are consistent with the Capability Maturity Model Integration (CMMI)² approach that is used to create a structure for encouraging productive, efficient behavior throughout an organization. Document the current and target maturity levels in Appendix A for each sub-element. Important considerations include:

- For target maturity level, the assessor must select the target level that is as high as the organization may reasonably be expected to achieve, given its size, resources, the criticality of its functions, and the risks associated with deficiencies in each sub-element.
- When the privacy program and other organizations share responsibility for a sub-element of the privacy program, the assessor should record the name of the entity or entities with which the privacy program shares responsibility in the “Comments” column of the matrix in Appendix A.
- The “Comments” column should also be used to document any steps taken towards the next maturity level and any implementation decisions that have been made regarding a sub-element.

²Capability Maturity Model Institute, <https://cmmiinstitute.com/>.

Level No.	Title	Description
1	Ad Hoc	<ul style="list-style-type: none"> The program requirement is new, not yet reliably implemented, or undocumented.
2	Defined	<ul style="list-style-type: none"> The program requirement is at least documented but may not always be implemented consistently.
3	Consistently Implemented	<ul style="list-style-type: none"> The program requirement is established as a standard business practice and its use is enforced by the organization.
4	Managed & Measurable	<ul style="list-style-type: none"> The program requirement is quantitatively managed with agreed upon metrics. The effectiveness of the process used to meet the program requirement is monitored.
5	Optimized	<ul style="list-style-type: none"> Program requirement management includes deliberate and continuous process improvement. Automation is used to continuously monitor and improve effectiveness.

Table 3. Privacy Maturity Level Descriptions

Step 3: The Privacy Maturity Model provides a process to use to identify existing, immediate risk as well as lower levels of risk. Use the current and target privacy maturity levels recorded in Appendix A for each sub-element as input for completing the table in Appendix B, Summary of Privacy Program Analysis Results, to summarize the results of the assessment and provide priority action items. Instructions for completing the table can be found in Appendix B. Organizations are advised to address their High Priority items immediately. They may choose to make a careful, risk-based decision to address other more mature items later in the current year or in a subsequent year by integrating them into a longer-term plan.

5 References

- Federal CIO Council Privacy Committee White Paper, *Best Practices: Elements of a Federal Privacy Program*, June 30, 2010
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations, NIST 800-53 v4, Appendix J, Privacy Controls Catalog*, April 2013
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010
- OMB Circular A-130, *Managing Information as a Strategic Resource*, July 27, 2016

Appendix A: Privacy Program Analysis Matrix

Use the table below to document the status of each of the sub-elements of a privacy program.

5.1.1 Element 1.0: Leadership & Organization

Table A-1. Leadership & Organization Program Requirements.

Sub-Element No.	Privacy Program Requirements	References	Current Maturity Level 1: Ad Hoc 2: Defined 3: Consistently Implemented 4: Managed & Measurable 5: Optimized	Target Maturity Level 1: Ad Hoc 2: Defined 3: Consistently Implemented 4: Managed & Measurable 5: Optimized	Comments <ul style="list-style-type: none">Organization or Role ResponsibleSteps taken towards next maturity levelImplementation decisions
1.1	Program Organizational Structure				
1.1.1	Appoints a senior privacy official (e.g., Chief Privacy Officer) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to manage privacy risk, including addressing all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems, delegating these duties to appropriate staff as necessary	NIST 800-53 v4, Appendix J, AR-1(a); OMB A-130: Main Body § 5(f)(1)(b); Appendix I § 4(e)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	

1.1.2	Establishes “top down” executive-level leadership support for the privacy program from the head of the organization.	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
1.2.3	Aligns privacy program placement within the organization and leadership in accordance with the program strategy	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
1.2	Program Design and Strategy				
1.2.1	Maintains a comprehensive privacy program.	OMB A-130: Main Body § 5(f)(1)(a); Appendix I § 3(b), 3(f), and § 4(e)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
1.2.2	Determines and documents the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or information system need	NIST 800-53 v4, Appendix J, AP-1	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
1.2.3	Defines program vision, mission, goals, objectives, and metrics to meet statutory and regulatory privacy requirements as well as unique mission needs	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	

1.2.4	Determines privacy protections that will be implemented to protect individuals that are not covered under the laws, regulations, and directives that govern the organization's operations	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
1.3	Program Privacy Principles				
1.3.1	Defines organization-specific information privacy principles that address privacy requirements in the context of its mission	OMB A-130: Appendix II § 3	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
1.3.2	Incorporates privacy requirements into enterprise architecture.	OMB A-130: Appendix I § 4(b)(5)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
1.3.3	Integrates privacy principles with enterprise architecture, policies, business processes, procedures, and standards	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
1.3.4	Reviews and updates privacy principles periodically	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
1.4	Privacy Program Governance				

1.4.1	Develops, disseminates, and implements operational privacy policies and procedures that implement the organization’s privacy principles and govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII	NIST 800-53 v4, Appendix J, AR-1(e)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
1.4.2	Updates privacy plan,policies, and procedures periodically	NIST 800-53 v4, Appendix J, AR-1(f)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
1.4.3	Establishes a framework, approach, and priority for developing privacy policies, procedures, and other resources	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
1.4.4	Communicates changes to personnel adequately in advance of compliance dates	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
1.5	Privacy Program Management				
1.5.1	Develops a strategic organizational privacy plan that provides an overview of the organization’s’s privacy program, for implementing applicable privacy controls, policies, and procedures	NIST 800-53 v4, Appendix J, AR-1(d); OMB A-130: Appendix I § 4(c)(2) and 4(e)(1)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4	

			<input type="checkbox"/> Level 5	<input type="checkbox"/> Level 5	
1.6	Resource Management				
1.6.1	Ensures that employee performance plans include privacy considerations	OMB A-130: Appendix I § 3(b)(9)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
1.6.2	Ensures that the senior privacy official is involved in assessing and addressing privacy hiring, training, and professional development needs	OMB A-130: Main Body § 5(c)(6)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
1.6.3	Maintains a workforce planning process	OMB A-130: Main Body § 5(c)(1)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
1.6.4	Develops a set of privacy competency requirements	OMB A-130: Main Body § 5(c)(1)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
1.6.5	Ensures that the workforce has the appropriate knowledge and skill	OMB A-130: Main Body § 5(c)(2)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4	

			<input type="checkbox"/> Level 5	<input type="checkbox"/> Level 5	
1.6.6	Allocates] sufficient budget and staffing and qualified resources to implement and operate the organization-wide privacy program in accordance with the program strategy	NIST 800-53 v4, Appendix J, AR-1(c)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
1.6.8	Defines, assigns, and communicates privacy roles and responsibilities for all members of the workforce, including members of the privacy program and other stakeholders throughout the organization	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
1.7	Stakeholder Coordination				
1.7.1	Ensures coordination between privacy and other programs	OMB A-130: Main Body § 5(f)(1)(k); Appendix I § 3(b)(11)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
1.7.2	Develops a structured approach to managing stakeholder communications, including identification of relevant stakeholders, definition of appropriate messaging, and coordination of communications	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
1.7.3	Leadership shares information with Privacy Program regarding activities that impact the program’s initiatives	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4	

			<input type="checkbox"/> Level 5	<input type="checkbox"/> Level 5	
1.8	Outreach & Collaboration				
1.8.1	Develops formal and informal relationships with internal and external groups that support the privacy program's activities	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	

5.1.2 Element 2.0: Privacy Risk Management

Table A-2. Privacy Risk Management Program Requirements.

Sub-Element No.	Privacy Program Requirements	References	Current Maturity Level 1: Ad Hoc 2: Defined 3: Consistently Implemented 4: Managed & Measurable 5: Optimized	Target Maturity Level 1: Ad Hoc 2: Defined 3: Consistently Implemented 4: Managed & Measurable 5: Optimized	Comments • Organization or Role Responsible • Steps taken towards next maturity level • Implementation decisions
2.1	Regulations Development				
2.1.1	For U.S. federal government organizations: Publishes required regulations in the Federal Register to support privacy requirements and program operations	As required by federal government laws and guidance	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.2	Privacy Policy, Procedures, and Standards				
2.2.1	Develops a risk-based approach to developing and implementing internal standards that support consistent implementation of privacy requirements	CIO Council Best Practices White Paper, Element 2	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.2.2	Establishes rules of behavior for employees with access to PII and consequences for violating them	OMB A-130: Appendix I § 4(h)(7)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4	

			<input type="checkbox"/> Level 5	<input type="checkbox"/> Level 5	
2.2.3	Provides resources, such as manuals, guides, and handbooks, to support consistent implementation of privacy policies, procedures, and standards	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.2.4	Conducts periodic reviews of privacy policy, procedures, and standards documentation to ensure they remain current and revises documentation as needed	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.3	PII Inventory, Categorization, & Minimization				
2.3.1	Describes the purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices and requires approval by the privacy program when changes to the identified purpose occur	NIST 800-53 v4, Appendix J, AP-2	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.3.2	Reviews and approves the categorization of information systems that involve PII	OMB A-130: Appendix I § 4(a)(2) and 4(e)(7)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.3.3	Implements a standardized process to assess whether information is PII and categorize PII based on associated privacy risks	NIST SP 800-122, § 2.1, 3.2 Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	

2.3.4	Balances the need for information collection with the privacy risks	OMB A-130: Main Body § 4(g), 4(i), 4(j)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.3.5	Identifies the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection	NIST 800-53 v4, Appendix J, DM-1(a)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.3.6	Limits the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII	OMB A-130: Main Body § 5(f)(1)(d)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.3.7	Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent	NIST 800-53 v4, Appendix J, DM-1(b)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.3.8	Eliminates unnecessary collection, maintenance, and use of Social Security numbers	OMB A-130: Main Body § 5(f)(1)(f)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.3.9	Establishes, maintains, and periodically updates an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing	NIST 800-53 v4, Appendix J, SE-1(a) OMB A-130: Main Body § 5(a)(1)(a) and 5(f)(1)(e)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	

	PII, and reduces PII holdings where possible				
2.3.10	Provides each update of the PII inventory to the CIO, information security official, or other appropriate senior official periodically to support the establishment of information security requirements for all new or modified information systems containing PII	NIST 800-53 v4, Appendix J, SE-1(b))	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.4	Project/Initiative Start-Up Consults				
2.4.1	Evaluates new programs, projects, technologies, systems, processes, activities, contracts and other initiatives for privacy implications	CIO Council White Paper on Best Practices, Element 2	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.5	Privacy Risk & Impact Assessments				
2.5.1	Ensures compliance with privacy requirements and manages privacy risks	OMB A-130: Main Body § 5(e)(1)-5(e)(2), 5(e)(7), 5(f)(1)(g)-5(f)(1)(i); and Appendix I § 3 (a), 3(b)(4), and 3(f)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.5.2	Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing	NIST 800-53 v4, OMB A-130: Appendix I § 3(b)(5) Appendix J, AR-2(a)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	

	(including for the purposes of matching), storing, transmitting, use, and disposal of PII				
2.5.3	For U.S. federal government organizations: Conducts Privacy Impact Assessments (PIAs) under section 208(b) of the E-Government Act of 2002, absent an applicable exception under that section, 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	NIST 800-53 v4, Appendix J, AR-2(b) OMB A-130; Main Body § 5(f)(1)(i) and Appendix I § 3(f)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.5.4	For U.S. federal government organizations: Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act	NIST 800-53 v4, Appendix J, DI-2(b)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.5.5	Strategically integrates privacy documentation, including risk assessments, into privacy risk management processes	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.5.6	Integrates privacy risk management into the enterprise risk management function	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4	

			<input type="checkbox"/> Level 5	<input type="checkbox"/> Level 5	
2.6	System of Records Notice				
2.6.1	For U.S. federal government organizations: Publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing PII	NIST 800-53 v4, Appendix J, TR-2(a)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.6.2	For U.S. federal government organizations: Keeps SORNs current and publishes deletion notices when systems are retired	NIST 800-53 v4, Appendix J, TR-2(b)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.7	Legal Agreements				
2.7.1	Works with business owners and legal stakeholders to include privacy considerations in legal agreements when they involve PII	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.8	Accounting of Disclosures				
2.8.1	Keeps an accurate accounting of disclosures of information	NIST 800-53 v4, Appendix J, AR-8(a)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.8.2	Makes the accounting of disclosures available to the person named in the record upon request	NIST 800-53 v4, Appendix J, AR-8(c)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4	

			<input type="checkbox"/> Level 5	<input type="checkbox"/> Level 5	
2.9	Data Quality & Integrity				
2.9.1	Confirms to the greatest extent practicable upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information	NIST 800-53 v4, Appendix J, DI-1(a)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.9.2	Collects PII directly from the individual to the greatest extent practicable	NIST 800-53 v4, Appendix J, DI-1(b)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.9.3	Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems in accordance with organizational standards	NIST 800-53 v4, Appendix J, DI-1(c)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.9.4	Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information	NIST 800-53 v4, Appendix J, DI-1(d)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.9.5	Documents processes to ensure the integrity of PII through existing security controls	NIST 800-53 v4, Appendix J, DI-2(a)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.9.6	Develops data quality standards that meet the	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2	

	organization's statutory and regulatory privacy requirements as well as unique mission needs and privacy principles		<input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.10	PII Retention, Disposition, & Destruction				
2.10.1	Retains each collection of PII for an appropriate amount of time to fulfill the purpose(s) identified in the notice, in accordance with the applicable retention schedule, and as required by law	OMB A-130: Main Body § 5(e)(1)(c), 5(f)(1)(h) NIST 800-53 v4, Appendix J, DM-2(a)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.10.2	Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with the official record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access	NIST 800-53 v4, Appendix J, DM-2(b)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.10.3	Uses pre-approved techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).	NIST 800-53 v4, Appendix J, DM-2(c)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.10.4	Destroys information from individuals upon request when practicable	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.11	PII Used in Non-Operational Environments & Research				

2.11.1	Develops policies and procedures that minimize the use of PII for testing, training, or research; and for developing software or programs; piloting software of programs; and for use in any other non-operational environments	NIST 800-53 v4, Appendix J, DM-3(a)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.11.2	Implements controls to protect PII used for testing, training, or research; and for developing software or programs; piloting software of programs; and for use in any other non-operational environments	NIST 800-53 v4, Appendix J, DM-3(b)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.11.3	Implements privacy protections consistent with human subjects research protocols	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.12	Internal Use				
2.12.1	Uses PII internally only for the authorized purpose(s) identified in applicable authorities and/or in public notices	NIST 800-53 v4, Appendix J, UL-1	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.13	Information Sharing				
2.13.1	Evaluates any proposed new instances of sharing PII, including ad hoc requests, with third parties to assess whether the sharing is authorized and	NIST 800-53 v4, Appendix J, UL-2(d)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	

	whether additional or new public notice is required				
2.13.2	Where appropriate, enters into agreements with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used as well as allowable disclosures (if any) and retention conditions	NIST 800-53 v4, Appendix J, UL-2(b) OMB A-130: Appendix I § 3(d)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.13.3	Shares PII externally, only for the authorized purposes identified in applicable authorities and/or described in its notice(s) or for a purpose that is compatible with those purposes	NIST 800-53 v4, Appendix J, UL-2(a)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.13.4	Requires organizations receiving PII to maintain the PII in an information system with a particular categorization level	OMB A-130: Appendix I § 3(c)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.13.5	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	NIST 800-53 v4, Appendix J, UL-2(c)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.13.6	Implements a process to evaluate ad hoc requests for sharing	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	

2.14	Oversight and Monitoring Planning				
2.14.1	Implements procedures to coordinate across the organization to address privacy requirements at all levels of the organization and in all locations	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.15	Government Privacy Changes Monitoring				
2.15.1	Monitors privacy laws and policy for changes that affect the privacy program	NIST 800-53 v4, Appendix J, AR-1(b) OMB A-130: Main Body § 5(f)(1)(c)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.15.2	Reviews regulations and reports from other entities to identify trends and best practices that may benefit the organization	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.16	IT Investment, Acquisition, & Contractor Management				
2.16.1	Supports identification and management of privacy risks through the acquisition life cycle	CIO Council White Paper on Best Practices, Element 2	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.16.2	Establishes privacy roles, responsibilities, and access	NIST 800-53 v4, Appendix J, AR-3(a)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3	

	requirements for contractors and service providers		<input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.16.3	Includes privacy requirements in Requests for Proposal	OMB A-130: Appendix I § 5(d)(j)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.16.4	Establishes a process to evaluate privacy risks for IT investments	OMB A-130: Main Body § 5(d)(3) and 5(d)(4)(c)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.16.5	Ensures that privacy risks are addressed and costs are included in IT capital investment plans and budgetary requests	OMB A-130: Main Body § 5(a)(3)(e)(ii) and 5(d)(3)(e); Appendix I § 4(b)(2) and 4(e)(6)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.16.6	Ensures that investment plans meet the privacy requirements appropriate for the life cycle stage of the investment	OMB A-130: Appendix I § 4(b)(4)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.16.7	Upgrades, replaces, or retires unprotected information systems	OMB A-130: Appendix I § 4(b)(3)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.16.8	Ensures that senior privacy officials are made aware of information systems and	OMB A-130: Main Body § 5(d)(2)(h);	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4	

	components that cannot be protected	Appendix I § 3(b)(11)	<input type="checkbox"/> Level 5	<input type="checkbox"/> Level 5	
2.16.9	Includes privacy requirements in contracts and other acquisition-related documents	NIST 800-53 v4, Appendix J, AR-3(b) OMB A-130: Appendix I § 3(d), 4(j)(1)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.16.10	Ensures that entities comply with law and other applicable privacy-related requirements	OMB A-130: Appendix I § 4(j)(1)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.16.11	Ensures that privacy-related authorities apply to contractors where required	OMB A-130: Appendix I § 4(j)(3)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.16.12	Oversees information systems operated by contractors	OMB A-130: Appendix I § 4(j)(2)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.16.13	Maintains an inventory of contractor information systems	OMB A-130: Appendix I § 4(j)(2)(c)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.16.14	Ensures that incident response procedures are in place for contractor information systems	OMB A-130: Appendix I § 4(j)(2)(e)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3	

			<input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.16.15	Modifies contracts as needed to address new privacy requirements	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
2.17	Privacy Risk & Issue Tracking				
2.17.1	Implements a process to manage privacy risks and issues, prioritize resolution, and track through to closure	CIO Council White Paper on Best Practices, Element 2	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	

5.1.3 Element 3.0: Engineering & Information Security

Table A-3. Engineering & Information Security Program Requirements.

Sub-Element No.	Privacy Program Requirements	References	Current Maturity Level 1: Ad Hoc 2: Defined 3: Consistently Implemented 4: Managed & Measurable 5: Optimized	Target Maturity Level 1: Ad Hoc 2: Defined 3: Consistently Implemented 4: Managed & Measurable 5: Optimized	Comments • Organization or Role Responsible • Steps taken towards next maturity level • Implementation decisions
3.1	Integration into Systems Engineering Process				
3.1.1	Ensures that all resources planning and management activities consider privacy throughout the system development life cycle and risks are managed	OMB A-130: Main Body § 5(a)(1)(c) NIST 800-53 v4, Appendix J, AR-7	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
3.1.2	Designs information systems to support privacy by automating privacy controls	NIST 800-53 v4, Appendix J, AR-7	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
3.1.3	Limits the capabilities of system to only those functions that support authorized collection, use, retention, and disclosure or PII	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	

3.1.4	Includes privacy sections in relevant system development documents (e.g. requirements documents, interface control documents)	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
3.1.5	Ensures the process for retiring systems adequately addresses privacy requirements	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
3.2	Cybersecurity Coordination				
3.2.1	Aligns information privacy principles and activities with cybersecurity processes and activities	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
3.3	Authority to Connect (ATO) Analysis				
3.3.1	Reviews authorization packages for information systems for privacy concerns.	OMB A-130: Appendix I § 4(e)(9)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
3.3.2	Develops, approves, and maintains privacy plans for information systems prior to authorization, reauthorization and continuous monitoring	OMB A-130: Appendix I § 4(c)(9) and 4(e)(8)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
3.4	Privacy Control Selection				

3.4.1	Designates program management, common, information system-specific, and hybrid privacy controls	OMB A-130: Appendix I § 4(c)(12) and 4(e)(5)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
3.4.2	Implements a privacy control selection process	OMB A-130: Appendix I § 4(c)(6)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
3.4.3	Integrates privacy considerations into the organization's risk management process	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
3.4.4	Protects all forms of personal information--including but not limited to paper, electronic, audio, video--from unauthorized access	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
3.5	Privacy in Emerging Technologies				
3.5.1	Evaluates privacy considerations for new and emerging technologies as part of the organization's technology assessment and infrastructure planning activities	A-130; Main Body § 5(a)(1)(b)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	

5.1.4 Element 4.0: Incident Response

Table A-4. Incident Response Program Requirements.

Sub-Element No.	Privacy Program Requirements	References	Current Maturity Level 1: Ad Hoc 2: Defined 3: Consistently Implemented 4: Managed & Measurable 5: Optimized	Target Maturity Level 1: Ad Hoc 2: Defined 3: Consistently Implemented 4: Managed & Measurable 5: Optimized	Comments <ul style="list-style-type: none">Organization or Role ResponsibleSteps taken towards next maturity levelImplementation decisions
4.1	Incident Management Procedures				
4.1.1	Develops and implements a Privacy Incident Response Plan that enables the organization to respond promptly to privacy incidents, including breaches	NIST 800-53 v4, Appendix J, SE-2(a) OMB A-130: Appendix I § 4(f)(1), 4(f)(7)-4(f)(8) CIO Council White Paper on Best Practices, Element 4	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
4.2	Incident Notification & Reporting				
4.2.1	Provides periodic training and communications regarding privacy incident reporting procedures to all members of the workforce	CIO Council White Paper on Best Practices, Elements 4 and 6	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
4.2.2	Provides multiple channels for reporting privacy incidents	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2	

			<input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
4.3	Response Capabilities				
4.3.1	Establishes roles and responsibilities to ensure oversight and coordination of incident response	OMB A-130: Appendix I § 4(f)(3)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
4.3.2	Periodically tests incident response procedures	OMB A-130: Appendix I § 4(f)(4)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
4.3.3	Documents incident response lessons learned and update procedures	OMB A-130: Appendix I § 4(f)(5)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
4.3.4	Ensures that processes are in place to verify corrective actions for privacy incidents	OMB A-130: Appendix I § 4(f)(6)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
4.3.5	Reports incidents in accordance with applicable authoritative guidance	OMB A-130: Appendix I § 4(f)(9)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
4.3.6	Provides reports on incidents as required	OMB A-130:	<input type="checkbox"/> Level 1	<input type="checkbox"/> Level 1	

		Appendix I § 4(f)(10)	<input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
4.3.7	Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan	NIST 800-53 v4, Appendix J, SE-2 (b)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
4.3.8	Integrates privacy incident management processes with business processes that deal with PII as well as with other forms of incident response (e.g., cybersecurity incident response)	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
4.4	High-Impact Privacy Incident Response Team				
4.4.1	Defines additional incident response procedures and roles for responding to high-impact privacy incidents, including notification and engagement of senior leadership with decision-making authority from relevant offices within the organization	CIO Council White Paper on Best Practices, Element 4	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	

5.1.5 Element 5.0: Individual Participation, Transparency, & Redress

Table A-5. Individual Participation, Transparency, & Redress Program Requirements.

Sub-Element No.	Privacy Program Requirements	References	Current Maturity Level 1: Ad Hoc 2: Defined 3: Consistently Implemented 4: Managed & Measurable 5: Optimized	Target Maturity Level 1: Ad Hoc 2: Defined 3: Consistently Implemented 4: Managed & Measurable 5: Optimized	Comments <ul style="list-style-type: none">Organization or Role ResponsibleSteps taken towards next maturity levelImplementation decisions
5.1	Dissemination of Privacy Program Information				
5.1.1	Ensures that the public has access to information about its privacy activities and is able to communicate with its senior privacy official	NIST 800-53 v4, Appendix J, TR-3(a)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
5.2	Privacy Notices				
5.2.1	Makes public privacy documentation as required and appropriate	NIST 800-53 v4, Appendix J, TR-1	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
5.2.2	Conducts periodic reviews of privacy documentation to ensure it remains current and revises documentation as needed	NIST 800-53 v4, Appendix J, AR-2, TR-2	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4	

			<input type="checkbox"/> Level 5	<input type="checkbox"/> Level 5	
5.2.3	Provides effective notice to the public and to individuals in plain language prior to or at the time of collection regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of 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	NIST 800-53 v4, Appendix J, TR-1(a)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
5.2.4	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	NIST 800-53 v4, Appendix J, TR-1(b)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
5.2.5	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 800-53 v4, Appendix J, TR-1(c)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	

5.2.6	Includes notices (including Privacy Act Statements when required for U.S. federal government organizations) 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	NIST 800-53 v4, Appendix J, TR-2(c)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
5.3	Consent				
5.3.1	Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection	NIST 800-53 v4, Appendix J, IP-1(a)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
5.3.2	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	NIST 800-53 v4, Appendix J, IP-1(b)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
5.3.3	Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII	NIST 800-53 v4, Appendix J, IP-1(c)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
5.3.4	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	NIST 800-53 v4, Appendix J, IP-1(d)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	

5.4	Manage Complaints & Inquiries				
5.4.1	Implements a process for receiving, managing, and responding to complaints, concerns, or questions from individuals about the organizational privacy practices, tracking through to resolution and closure	NIST 800-53 v4, Appendix J, IP-4 CIO Council	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
5.5	Individual Access				
5.5.1	Provides individuals the ability to have access to their PII maintained in its system(s)	NIST 800-53 v4, Appendix J, IP-2(a)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
5.5.2	For U.S. federal government organizations: Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records	NIST 800-53 v4, Appendix J, IP-2(b)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
5.2.3	For U.S. federal government organizations: Publishes access procedures in System of Records Notices (SORNs)	NIST 800-53 v4, Appendix J, IP-2(c)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
5.2.4	For U.S. federal government organizations: Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests	NIST 800-53 v4, Appendix J, IP-2(d)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	

5.2.5	Provides access procedures in relevant spoken languages where applicable	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
5.2.6	Documents and communicates reasons for denying access	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
5.6	Amendment, Correction, & Redress				
5.6.1	Provides a process for individuals to have inaccurate PII maintained by the organization corrected or amended, as appropriate	NIST 800-53 v4, Appendix J, IP-3(a)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
5.6.2	Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII within a reasonable timeframe, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended	NIST 800-53 v4, Appendix J, IP-3(b)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
5.6.3	Documents and communicates reasons for denying amendment, correction, or redress	NIST 800-53 v4, Appendix J, IP-3 Supplemental Guidance Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	

5.6.4	Implements and makes public in relevant spoken languages where applicable procedures for requesting redress	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
5.6.5	Implements measure granted for redress within a reasonable timeframe	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
5.7	Public Facing Online Presence				
5.7.1	Ensures that its privacy practices are publicly available through organizational websites or otherwise	NIST 800-53 v4, Appendix J, TR-3(b)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
5.7.2	Maintains and posts privacy policies on websites, mobile applications, and other digital services	OMB A-130: Main Body § 5(f)(1)(j)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
5.7.3	For U.S. federal government organizations: Provides links on the organization's website to privacy information published in the Federal Register and other sources	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	

5.1.6 Element 6.0: Privacy Training & Awareness

Table A-6. Privacy Training & Awareness Program Requirements.

Sub-Element No.	Privacy Program Requirements	References	Current Maturity Level 1: Ad Hoc 2: Defined 3: Consistently Implemented 4: Managed & Measurable 5: Optimized	Target Maturity Level 1: Ad Hoc 2: Defined 3: Consistently Implemented 4: Managed & Measurable 5: Optimized	Comments <ul style="list-style-type: none">Organization or Role ResponsibleSteps taken towards next maturity levelImplementation decisions
6.1	Workforce Training				
6.1.1	Maintains organization-wide privacy training for all employees and contractors	OMB A-130: Appendix I § 4(h)(1)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
6.1.2	Ensures that privacy training is consistent with applicable policies, standards, and guidelines	OMB A-130: Appendix I § 4(h)(2)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
6.1.3	Apprises organization employees about privacy assistance, resources, and techniques	OMB A-130: Appendix I § 4(h)(3)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	

6.1.4	Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures	NIST 800-53 v4, Appendix J, AR-5(a)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
6.1.5	Administers basic privacy training and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) at least annually	OMB A-130: Appendix I § 4(h)(4), 4(h)(5) NIST 800-53 v4, Appendix J, AR-5(b)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
6.1.6	Tracks and reports completion of mandatory annual privacy training commensurate with professional responsibilities	CIO Council white Paper on Best Practices, Element 6	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
6.1.7	Requires completion of mandated privacy training prior to authorizing access to PII	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
6.1.8	Regularly evaluates training and awareness materials to determine effectiveness and whether it is current, revises materials to reflect feedback	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
6.2	Privacy Awareness Communications				
6.2.1	Supplements training with activities that reinforce the workforce's understanding of privacy expectations	NIST 800-53 v4, Appendix J, AR-5 (implicit in Supplemental Guidance)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	

6.3	Internal Online Presence				
6.3.1	Provides workforce with access to current privacy resources at a centralized location	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	

5.1.7 Element 7.0: Accountability

Table A-7. Accountability Program Requirements.

Sub-Element No.	Privacy Program Requirements	References	Current Maturity Level 1: Ad Hoc 2: Defined 3: Consistently Implemented 4: Managed & Measurable 5: Optimized	Target Maturity Level 1: Ad Hoc 2: Defined 3: Consistently Implemented 4: Managed & Measurable 5: Optimized	Comments <ul style="list-style-type: none">Organization or Role ResponsibleSteps taken towards next maturity levelImplementation decisions
7.1	Rules of Behavior Acknowledgement				
7.1.1	Ensures that personnel read and certify (manually or electronically) acceptance of responsibilities for privacy requirements in rules of behavior at least annually	OMB A-130: Appendix I § 4(h)(7) NIST 800-53 v4, Appendix J, AR-5(c)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
7.1.2	Holds personnel accountable for complying with privacy requirements and policies	OMB A-130: Appendix I § 3(b)(9)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
7.2	Internal & External Reporting				
7.2.1	Develops, disseminates, and updates timely and accurate reports to appropriate oversight bodies to demonstrate accountability with specific statutory and regulatory privacy program	OMB A-130: Appendix I § 4(1) NIST 800-53 v4, Appendix J, AR-6	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	

	mandates and to senior management and other personnel with responsibility for monitoring privacy program performance and compliance				
7.3	Privacy Monitoring and Auditing				
7.3.1	Identifies privacy control assessment methodologies and metrics	OMB A-130: Appendix I § 4(e)(4)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
7.3.2	Monitors and audits privacy controls and internal privacy policy to ensure effective implementation	NIST 800-53 v4, Appendix J, AR-4 OMB A-130: Appendix I § 3(b)(6), 4(c)(13)-4(c)(14), and 4(e)(3)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
7.3.3	Develops and maintains a privacy continuous monitoring strategy and a privacy continuous monitoring program	OMB A-130: Appendix I § 4(d)(9), 4(d)(10)-4(d)(11), and 4(e)(2)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
7.3.5	Corrects deficiencies that are identified in information systems	OMB A-130: Appendix I § 4(c)(15) and 4(k)	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	
7.3.6	Assesses the senior privacy official's performance with regard to the effectiveness of the privacy program	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	

7.4	Incorporate Lessons Learned				
7.4.1	Evaluates privacy risks, complaints, and incidents to identify knowledge gaps in the workforce or other privacy issues and uses this data to update policies, procedures, business processes, standards, and training	Effective practice	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3 <input type="checkbox"/> Level 4 <input type="checkbox"/> Level 5	

Appendix B: Summary of Privacy Program Analysis Results

Use the current and target privacy maturity levels recorded in Appendix A for each sub-element as input for completing the table below to summarize the results of the privacy program analysis and identify each item as low, medium, or high priority to be addressed. Items that are already optimized should be designated as “Complete.” Each item should be integrated into the organization’s privacy plan and tracked as part of monitoring the privacy program’s performance.

General guidelines for addressing priorities are:

- High Priority items should be closed within six months.
- Medium Priority items should be addressed within two years.
- Low Priority Items should be addressed within a longer timeframe based on the organization’s functions, risk tolerance, and resources.

Table B-1. Summary of Findings of Privacy Program Analysis and Assessment

Sub-Element No.	Privacy Program Requirements	PRIORITY TO ADDRESS				Comments
		High	Medium	Low	Complete (Already Optimized)	
1.0	Leadership & Organization					
1.1	Program Organizational Structure					
1.2	Program Design and Strategy					
1.3	Program Privacy Principles					
1.4	Privacy Program Governance					
1.5	Privacy Program Management					
1.6	Resource Management					
1.7	Stakeholder Coordination					
1.8	Outreach & Collaboration					
2.0	Privacy Risk Management					
2.1	Regulations Development					
2.2	Privacy Policy, Procedures, and Standards					
2.3	PII Inventory, Categorization, & Minimization					
2.4	Project/Initiative Start-Up Consults					

Sub-Element No.	Privacy Program Requirements	PRIORITY TO ADDRESS				Comments
		High	Medium	Low	Complete (Already Optimized)	
2.5	Privacy Risk & Impact Assessments					
2.6	System of Records Notice					
2.7	Legal Agreements					
2.8	Accounting of Disclosures					
2.9	Data Quality & Integrity					
2.10	PII Retention, Disposition, & Destruction					
2.11	PII Used in Non-Operational Environments & Research					
2.12	Internal Use					
2.13	Information Sharing					
2.14	Oversight and Monitoring Planning					
2.15	Government Privacy Changes Monitoring					
2.16	IT Investment, Acquisition, & Contractor Management					
2.17	Privacy Risk & Issue Tracking					
3.0	Engineering & Information Security					
3.1	Integration into Systems Engineering Process					
3.2	Cybersecurity Coordination					
3.3	Authority to Connect (ATO) Analysis					
3.4	Privacy Control Selection					
3.5	Privacy in Emerging Technologies					
4.0	Incident Response					
4.1	Incident Management Procedures					
4.2	Incident Notification & Reporting					
4.3	Response Capabilities					
4.4	High-Impact Privacy Incident Response Team					
5.0	Individual Participation, Transparency & Redress					
5.1	Dissemination of Privacy Program Information					
5.2	Privacy Notices					
5.3	Consent					
5.4	Manage Complaints & Inquiries					
5.5	Individual Access					
5.7	Public Facing Online Presence					

Sub-Element No.	Privacy Program Requirements	PRIORITY TO ADDRESS				Comments
		High	Medium	Low	Complete (Already Optimized)	
6.0	Privacy Training & Awareness					
6.1	Workforce Training					
6.2	Privacy Awareness Communications					
6.3	Internal Online Presence					
7.0	Accountability					
7.1	Rules of Behavior Acknowledgement					
7.2	Internal & External Reporting					
7.3	Privacy Monitoring and Auditing					
7.4	Incorporate Lessons Learned					