MITRE

Generic System Privacy Requirements and Tests

MITRE Privacy Engineering

August 2019

Approved for Public Release; Distribution Unlimited. Case Number 19-00598-4.

Table of Contents

1 Background and Purpose

Privacy is a system property that, like other non-functional system properties such as security and performance, can be specified in the form of implementable requirements and tested based on those requirements. This document provides a set of generic privacy requirements and tests that can be used to verify that a system works as expected from a privacy perspective. The privacy requirements and tests described here are situated within a general framework based on the Fair Information Practice Principles oriented toward enterprise systems in U.S. federal agencies that handle personally identifiable information (PII).[1] Both that framework and those implementable requirements and their associated tests should be directly usable or adaptable by organizations within the both the public and private sectors.

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 Approach

The privacy requirements specified in this document are hierarchically structured, starting with privacy principles based on the Fair Information Practice Principles specified in Office of Management and Budget (OMB) Circular A-130.[2] The list of Fair Information Practice Principles is provided in the table below.

Table 1. Fair Information Practice Principles from OMB Circular A-130.

Area	Principle
Access and Amendment	Agencies should provide individuals with appropriate access to PII and appropriate opportunity to correct or amend PII.
Accountability	Agencies should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.
Authority	Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.
Minimization	Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.
Quality and Integrity	Agencies should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.

[1] PII is defined as ". . . information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." Source: Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016.

[2] Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016.

Area	Principle
Individual Participation	Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Agencies should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.
Purpose Specification and Use Limitation	Agencies should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.
Security	Agencies should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.
Transparency	Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

In this document, a general enterprise privacy requirement is derived from each principle and further refined into a system privacy requirement.[3] Each system privacy requirement is translated into progressively more granular level 1 and level 2 privacy requirements. Each level 2 privacy requirement has one or more tests associated with it.

3 General Notes and Assumptions

General notes and assumptions regarding the requirements and tests in this document are:

- These tests focus on system characteristics, capabilities, and configuration. Where other aspects of the enterprise relate, such as business decisions, we are assuming those decisions were made prior to system design and development. These tests do not address those areas, though they do refer to those decisions and related documentation where necessary.
- Tests are written in a general format so as to apply broadly to most systems. Given the diversity of system types and platforms, the steps to execute each test may be different across systems. For example, when examining user permissions in relation to Strict Confidentiality, the steps will be different for a UNIX system and a Windows system.
- The tests are assumed to apply to systems preparing to run in a production environment. If related environments in which the data, system, or process may function (e.g., backup, disaster recovery, business continuity) are sufficiently different from the production environment to result in alternative implementations of privacy controls, then the relevant tests should be carried out in the other environments as well.

[3] The complete framework breaks down each general enterprise privacy requirement into four context-specific privacy requirements: business process, system development, system, and operations. This document focuses on the system privacy requirements and associated tests.

- Some requirements are written as conditional statements (i.e., "For systems that ___"). These requirements and associated tests will only apply to certain systems as they are dependent on particular characteristics.
- The nature of a system may render other requirements and associated tests nonapplicable.
- Section 6 discusses potential next steps for streamlining the testing process, including options for consolidating the tests. For example, some tests require the same activity but expect different results depending on the requirement. Tests with the same activity could be grouped together, enabling the tester to run the test only once and interpret the results in the various ways required. Section 6 contains additional discussion and examples.
- Each test represents an action that a tester must perform.
- There is only one enterprise privacy requirement, Authority, that does not have a corresponding system requirement specified, as it is included under Transparency.
- As written, the requirements and tests can be used as the basis for tailored privacy-related system requirements and tests.

4 How to Use This Document

This section provides useful background for understanding and using the privacy requirements and tests in Section 5. Below are definitions for common terms used throughout this document, as well as additional notes about the structure of the content provided in the tables.

4.1 Definitions

Individual: Refers to the person to whom the PII in the system pertains.
Review: To verify the presence or alignment of a characteristic, capability, or configuration or to assess a characteristic, capability, or configuration against an established standard.
Source System: System providing data to the system being tested.
System: System being tested.
Target System: System receiving data from the system being tested.
Third Party: A person, organization, or system external to the organization using the requirements and tests.
User: An authorized user of the system.

4.2 Document Structure

The following information will aid the reader in understanding the structure of the privacy test tables in Section 5:

- The level 1 and level 2 requirements break down the enterprise system privacy requirements into system characteristics or properties that are testable.
- Faults represent issues that could cause the system to behave in a way that prevents it from meeting the defined requirements. The tests are constructed to detect these faults when they occur in systems.
- The comments column is used for further explaining privacy tests and terminology, as well as for describing differences among individual systems that may affect the way in which tests are conducted.

- The red bar shown on the tables distinguishes between necessary and optional information for testers. The columns on the left show the derivation of the tests, while the columns on the right directly support testing activity.

5 Test Cases

5.1 Access and Amendment

General Enterprise Privacy Requirement

Agencies should provide individuals with appropriate access to PII and appropriate opportunity to correct or amend PII.

System Requirement
Systems shall be capable of appropriately supporting access and correction.

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
1.1 Individuals shall have the ability to access their PII.	**1.1.1** For systems where individuals directly enter their PII, the system shall provide immediate notification of the right to and the circumstances under which the individual may access their PII.	The system does not notify individuals of the right to and circumstances under which they may access their PII prior to saving, processing, or propagating such PII.	**1.1.1.1** Submit test PII to the system and observe any notice provided.	This requirement applies to all systems that collect PII directly from the individual.	The system will notify the individual that PII submitted may be accessed as authorized, prior to saving, processing, or propagating the PII.	The system will not notify the individual that PII submitted may be accessed as authorized, prior to saving, processing, or propagating the PII.
	1.1.2 For systems where individuals directly enter their PII, the system shall enable the individual to review their PII before submitting it for processing.	The system does not permit individuals to review PII they have entered prior to saving, processing, or propagating such PII.	**1.1.2.1** Submit test PII to the system.		The system will provide the individual with the opportunity to review PII prior to saving, processing, or propagating the PII.	The system will not provide the individual with the opportunity to review PII prior to saving, processing, or propagating the PII.

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
1.2 The system shall support authorized updates/corrections to PII.	**1.2.1** For systems that receive PII from third parties, the system shall notify the third parties of the mechanisms and circumstances governing the update/ correction of the submitted PII.	The system does not notify third parties of the process to correct any PII submitted.	**1.2.1.1** Submit test PII as a third party to the system and observe any notice provided.	This requirement applies to all systems that collect, process, or transmit PII.	The system will provide an advisory regarding how PII submitted may be corrected, as authorized.	The system will not provide an advisory regarding how PII submitted may be corrected, as authorized.
	1.2.2 For systems that receive PII from third parties, the system shall enable them to update/correct submitted PII.	The system does not permit third parties to update/correct PII that they have submitted to the system.	**1.2.2.2** Submit test PII to the system as a third party, then attempt to update the test PII originally submitted.		The originally submitted PII will be updated.	The originally submitted PII will not be updated.
	1.2.3 For systems that receive PII from source systems, the system shall enable them to update/correct the submitted PII.	The system does not permit source systems to update/correct PII that they have submitted to the system.	**1.2.3.1** Submit test PII to the system from a source system, then attempt to update the test PII originally submitted.		The originally submitted PII will be updated.	The originally submitted PII will not be updated.
	1.2.4 For systems into which individuals directly enter their PII, the system shall provide immediate notification of the right to and the circumstances under	The individual who enters PII directly into the system does not receive immediate notification of the right to and circumstances	**1.2.4.1** Enter test PII into the system and observe any notice provided.		The system will provide immediate notification of the right to and circumstances under which individuals may	The system will not provide immediate notification of the right to and circumstances under which individuals may

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
	which the individual may update/correct their PII.	under which they may update/correct their PII.			update/correct their PII.	update/correct their PII.
1.3 The system shall support propagation of updates/corrections to PII.	**1.3.1** The system shall propagate all authorized updates/corrections of PII to target systems.	Corrections to PII are not propagated to target systems.	**1.3.1.1** Submit updated test PII to the system and verify that the update is transmitted to target systems.		The system will propagate updated PII to target systems.	The system will not propagate updated PII to target systems.

5.2 Accountability

General Enterprise Privacy Requirement

Agencies should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.

System Requirement

Information necessary to support reporting—including metrics—related to the effectiveness of privacy controls shall be captured by agency systems. Systems shall be designed such that access to PII is granted only to authorized users with a business need for the PII.

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
2.1 Auditing and reporting capabilities shall support monitoring of PII manipulation.	**2.1.1** The system shall capture all requests to update PII in the system and when the update has been completed.	An audit log is not kept on PII updated in the system.	**2.1.1.1** Review audit log that provides evidence of PII being updated in the system to verify its existence.		An audit log pertaining to PII being updated in the system will exist.	An audit log pertaining to PII being updated in the system will not exist.
		The system is not configured to perform all required oversight activity.	**2.1.1.2** Submit updated test PII to the system.		Audit log will show all evidence of PII updated in the system.	Audit log will not show all evidence of PII updated in the system.

	2.1.2 For systems that generate their own analysis of PII, the system shall be equipped with mechanisms to produce trend and comparative analysis on the manipulation of PII.	There is no function to generate trend and comparative analysis on updated PII.	**2.1.2.1** Attempt to generate report on the total number of times updated PII was submitted to the system and the data fields updated within a specified time period.	Comparative analysis may include frequency of requests to and action of updating PII, common data fields updated, and peak periods for these occurrences.	System report will be generated providing the specific trend and comparative analysis information requested.	System report will not be generated or will be incomplete.
		There is no function to generate trend and comparative analysis on new PII.	**2.1.2.2** Review function that generates trend and comparative analysis on newly produced or input PII.	If the system interface is highly constrained, where users and their degrees of freedom are predetermined, then technically this requirement should be a non-issue. Conversely, if users' freedoms are not predetermined and less controlled, then this requirement becomes more relevant.	System report will be generated providing the specific trend and comparative analysis information requested.	System report will not be generated or will be incomplete.
	2.1.3 The system shall report on	The system is not configured to report on system	**2.1.3.1** Review the system's design documentation for		Reporting function will exist.	Reporting function will not exist.

	inappropriate manipulation of PII.	anomalies, including supplemental event details and trend analysis information.	reporting function for system anomalies.			
			2.1.3.2 Review the system's design documentation for analysis function.		Analysis function will exist.	Analysis function will not exist.
	2.1.4 The system shall recognize established thresholds that when met signify suspicious user activity.	The system does not flag and report on system anomalies.	**2.1.4.1** Attempt to engage in a behavior (e.g., user excessively accessing records) that might indicate inappropriate use of PII.		The system will flag and report anomalous behavior.	The system will not flag and report anomalous behavior.
	2.1.5 The system shall notify the user, administrator, or other relevant party of any failure during transfer of PII.	Notification is not sent upon transfer failure.	**2.1.5.1** Initiate a data transfer to an authorized system and introduce an interruption that will cause the transfer to fail. Observe any alerts produced by the system.	Transfer failures can result in incomplete records for individuals. Examples of failures to introduce would be to disconnect one of the test systems from the network, attempt to connect to a destination system that will not allow a connection from the system being tested, or writing to a full drive. Notifications may include on-screen alerts, log entries,	The system will generate a notification to the appropriate party.	The system will not generate a notification.

				or some other method. This test should be repeated for various system types and transfer methods, as the variables in each scenario may produce different results.		
2.2 The system shall monitor new PII produced to ensure it is relevant for the purposes of the system.	**2.2.1** The system shall maintain an audit log of attempts to produce new PII.	The system is not configured to log information on new PII produced.	**2.2.1.1** Review audit log that shows evidence of new PII produced.	If the system interface is highly constrained, where users and their degrees of freedom are predetermined, then technically this requirement should be a non-issue. Conversely, if users' freedoms are not predetermined and less controlled, then this requirement becomes more relevant.	Audit logs will capture information related to new PII produced.	Audit logs will not capture information related to new PII produced.

2.3 Exchanges of PII to and from the system shall be within the permitted data use and sharing scope identified in the system's privacy and other documentation.	**2.3.1** PII exchanges between the system and third parties shall be accounted for by formal documentation e.g., Privacy Impact Assessment (PIA), Memorandum of Understanding (MOU), Interconnection Security Agreement (ISA).	The system is not configured to recognize permissible system connections/ interfaces for collecting and providing PII.	**2.3.1.1** Review alignment between authorized system connections and system interface configurations to ensure that the system is interfacing only with authorized third party systems.		The system will interface with only authorized third party systems.	The system will interface with unauthorized third party systems.
		The system conducts PII exchanges with third parties with which it does not have an agreement.	**2.3.1.2** Compare applicable authorization agreement(s) against PII exchanges between the system and third parties to verify that data exchanges are authorized.		PII exchanges between the system and third parties will be covered by proper documentation.	PII exchanges between the system and third parties will not be covered by proper documentation.
	2.3.2 For systems that maintain an accounting of disclosures under sub-section (c) of the Privacy Act,[4] the system shall log the date, purpose, and	The system is not configured to capture information for accounting of disclosures.	**2.3.2.1** Review the system's design documentation to verify there is a function responsible for capturing information pertaining to disclosure activity.	Subsection (c) of the Privacy Act requires the agency to keep accurate account of when and to whom it has disclosed PII. This includes the date,	System function will exist for capturing information pertaining to disclosure activity.	System function will not exist for capturing PII pertaining to disclosure activity.

[4] Privacy Act of 1974, 5 U.S.C. § 552a.

	to whom the record was disclosed.	The system does not log disclosure activity.	**2.3.2.2** Disclose PII from the system to a target entity to verify that the disclosure is logged.	nature, and purpose of each disclosure of a record.	PII disclosure activity will be logged.	PII disclosure activity will not be logged.
2.4 The system shall support identified technical functionalities applied to protect PII.	**2.4.1** The system's technical monitoring and reporting functionalities shall be consistent with those described in the system's privacy compliance documents.	Certain technical functionalities identified in the PIA, System of Records Notice (SORN), or other privacy compliance documents do not exist in the system.	**2.4.1.1** Review the application of technical monitoring and reporting functionalities in the system to ensure that they match technical functionalities described in the system's PIA, SORN, and any other privacy compliance documents that describe this information.		Technical monitoring and reporting functionalities will be identical to those described.	Technical monitoring and reporting functionalities will not be identical to those described.
2.5 Authorizations shall be based on a business need for the PII.	**2.5.1** The authorization schema[5] for the system shall align with the business logic within the system.	The logic of the authorization schema does not align with business need for the access.	**2.5.1.1** Review the functions of the system and the authorization schema of the system, and compare them for alignment.	If the authorization schema is not in alignment with business functions it could result in entities having greater access to PII than needed.	The authorization schema will allow access only to the PII required for the user/system to complete the authorized function.	The authorization schema will allow access to PII beyond what is required for the user/system to complete the authorized function.

[5] The phrase "authorization schema" refers to the logic of how authorization permissions are designed to function within the system (e.g., by group, by role, by transaction type, etc.). An example of an authorization schema where permissions appropriately match functions would be a schema where a group of "reviewers" is separate from a group of "approvers". Individuals assigned to the "reviewer" group could read PII and make recommendations, but not approve actions. Individuals in the "approver" group could read recommendations and approve actions. An authorization schema where all individuals are automatically authorized to approve all actions is an example of a schema where the alignment between permissions and functions may be inappropriate.

		The authorization schema is not granular enough to specifically tie actions to business need.	**2.5.1.2** Review the authorization schema and compare it to the SORN and any applicable Computer Matching Agreements and data sharing MOUs/Memoranda of Agreement (MOAs).	If the authorization schema allows for access or roles that are not included as part of relevant privacy documents, the system will be in violation of the Privacy Act of 1974.	The authorization schema will match the documented notice of routine uses and authorized groups and will match the Computer Matching Agreements and data sharing MOUs/MOAs.	The authorization schema will allow access beyond the documented notice of routine uses and authorized groups and/or will not match the Computer Matching Agreements or data sharing MOUs/MOAs.
			2.5.1.3 Review a sample of the existing or proposed users/systems and compare their business responsibilities to their permissions within the system.	If the authorization schema is too broad, it will result in entities having greater access to PII than needed; if the schema is too narrow, it will result in overly burdensome administration of the system authorizations.	The sampled users/systems will have access only to the PII required for their business responsibilities.	The sampled users/systems will have access to PII beyond what is required for their business responsibilities.
2.6 For systems that handle authorizations, permissions shall be updated within an appropriate timeframe and appropriately	**2.6.1** The system shall respond to authorization changes within a defined timeframe.	Authorizations do not reflect removal or reduction of authorization within the applicable timeframe.	**2.6.1.1** Remove a user/system's authorization to access the system.		Authorizations will reflect removal or reduction of authorization within the applicable timeframe.	Authorizations will not reflect removal or reduction of authorization within the applicable timeframe.

connected with other organizational events (e.g., separations, job changes).			**2.6.1.2** Remove a user/system's authorization permission.		Authorizations will reflect removal or reduction of authorization within the applicable timeframe.	Authorizations will not reflect removal or reduction of authorization within the applicable timeframe.
			2.6.1.3 Reduce the authorization status of a user/system.		Authorizations will reflect removal or reduction of authorization within the applicable timeframe.	Authorizations will not reflect removal or reduction of authorization within the applicable timeframe.
	2.6.2 The system shall connect to source systems so as to process changes in authorizations based on relevant organizational events (e.g. separations, job changes, etc.).	The system will not connect to all the appropriate source systems.	**2.6.2.1** Review the system design to verify that the system connects to all of the appropriate source systems for changes in user/system status.		The system will connect to all of the appropriate source systems for changes in user/system status.	The system will not connect to all of the appropriate source systems for changes in user/system status.
		The system connects to the appropriate source systems, but connections are not functional.	**2.6.2.2** Make a change to a user/system's status in the source system such that access to the system being tested would be removed or reduced (e.g., a separation).	The number of test cases may vary based on: a) the number of other agency source systems that are connected to, b) the number of permissions in	The system will update the authorizations to reflect the changes in authorization.	The system will not update the authorizations to reflect the changes in authorization.

				the test system, and c) the number of external events that automatically change the authorization levels of a user/system within the test system.		
			2.6.2.3 Make a change to a user/system's status in the source system such that a specific permission authority would be removed (e.g., a department change).		The system will update the authorizations to reflect that the user/system no longer has the specific permission.	The system will not update the authorizations to reflect that the user/system no longer has the specific permission.
2.7 Only authorized entities may gain initial access to the system.	**2.7.1** The system shall request appropriate credentials at the time of request for initial access so as to sufficiently identify the user/system making the request.	The system does not request appropriate credentials.	**2.7.1.1** Attempt to gain access to the system without entering appropriate credentials.	The definition of appropriate credentials will vary based on: 1) the PII and processing capabilities of the system, 2) the technology platform of the system, and 3) connections to any centralized	The system will not attempt to verify authorization of a user/system without entry of appropriate credentials.	The system will attempt to authorize a user/system without entry of appropriate credentials.

				authorization facilities.		
		The system requests appropriate credentials, but can't identify the user/system.	**2.7.1.2** Attempt to gain access to the system with valid credentials.		The system will correctly identify the user/system.	The system will not correctly identify the user/system.
		The system requests credentials, but incorrectly identifies the user/system.	**2.7.1.3** Attempt to gain access to the system as multiple users/systems.		The system will correctly identify each unique user/system.	The system will not correctly identify each unique user/system.

5.3 Authority

General Enterprise Privacy Requirement

Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.

System Requirement

Included under Transparency.

5.4 Minimization

General Enterprise Privacy Requirement

Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.

System Requirement

Controls shall be implemented to automatically and appropriately limit PII that is input, produced, transferred, stored, or viewable and to properly destroy it when no longer required.

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
Collection/Input						
4.1 Interfaces shall ensure that only predetermined PII required to meet the purposes of the system is accepted as input.	**4.1.1** PII input from users shall be limited to predetermined data elements.	The system does not capture PII data elements using structured mechanisms.	**4.1.1.1** Review user interfaces in which PII is entered. Establish rationale for any unstructured capture mechanisms (e.g., free text boxes).	Structured mechanisms for capturing PII input (e.g., discrete and appropriately formatted input fields for specific PII data elements) help constrain the PII that can be captured.	User interfaces will capture PII data elements using structured mechanisms, except in those cases for which a documented rationale exits.	User interfaces will capture PII data elements using unstructured mechanisms for which no documented rationale exists.
		Unstructured data inputs (e.g. text boxes) do not display the necessary warnings at the point of data entry to discourage users from providing unnecessary	**4.1.1.2** Review display screens for evidence of appropriate warning.	Unstructured data inputs pose a risk, as they are difficult to govern and users can enter any information they choose.	Display screens will include the requisite warnings in the same vicinity as the unstructured entry field.	Requisite warnings will be absent or inadequate.

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
		and/or prohibited PII.				
	4.1.2 PII entering the system from other systems shall be limited to predetermined data elements.	The system pulls more PII data elements than necessary from source systems.	**4.1.2.1** Review interfaces to verify PII data elements being requested.	Individual queries may also be executed. Volume of queries may drive the approach used.	The system will request only PII data elements pre-determined to be necessary.	The system will request PII data elements that have not been pre-determined to be necessary.
		The system is not configured to limit PII data elements received from source systems.	**4.1.2.2** Review interfaces to verify PII data elements being received.	May also send full record to system, including unnecessary PII data elements. Unnecessary PII data elements may also be sent individually; however, it is likely more efficient/feasible to send a record that contains multiple types of elements that should not be accepted.	The system will only capture PII data elements it is specifically expecting.	The system will capture PII data elements that it is not specifically expecting.
Use/Production						
4.2 PII produced by the system shall be limited to only that which is required to meet the purposes of the system.	**4.2.1** Generation of new PII shall be restricted to pre-determined data elements.	The system generates PII data elements other than those intended.	**4.2.1.1** Review output of each system function for PII data elements.		All system functions will output intended PII data elements.	Functions will exist for which unintended PII data elements are output.

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
4.3 The purposes and limitations of PII use shall be communicated along with system outputs where the user interface permits.	**4.3.1** User interfaces shall provide a notification when saving PII outside the system or printing PII, reminding the user of the permissible uses and restrictions on usage of the PII.	Notification of purposes and restrictions for using the PII is not presented to users prior to file generation.	**4.3.1.1** Attempt to save a file or data extract from the system that contains PII.	Notification may be handled in multiple ways, depending on the capabilities of the system, including screen views or pop-up notices.	The system will provide a notification reminding the user of the purposes and restrictions associated with the use of the PII removed from the system.	The system will not provide a notification reminding the user of the purposes and restrictions associated with the use of the PII removed from the system.
		Notification of purposes and restrictions for using the PII is not presented to users prior to printing.	**4.3.1.2** Attempt to print a file containing PII from the system.		The system will provide a notification reminding the user of the purposes and restrictions associated with the use of the PII being printed.	The system will not provide a notification reminding the user of the purposes and restrictions associated with the use of the PII being printed.
	4.3.2 For systems with supporting technology, PII output shall be properly labeled regarding permissible uses and restrictions on usage of the PII.	Saved output files containing PII are not properly labeled.	**4.3.2.1** Create and save a file containing system output with PII and review the label associated with it.	This requirement depends on system capabilities. When available, automated means of applying labels should be used. Labels may include a file header or footer, a	Output file will contain one or more labels to denote authorized use of the PII	Output file will not contain any labels denoting authorized use or label is incorrect.
		System printouts containing PII are not properly labeled.	**4.3.2.2** Print a file containing PII and review the label printed on it.		Printed file will contain one or more labels to denote	Printed file will not contain any labels denoting authorized use or label is incorrect.

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
				watermark, a designation in the file name, or some other means of communicating the authorized purpose. When practical for the purpose, consider making electronic file outputs read-only.	authorized use of the PII.	
		Outputs containing PII allow removal of labeling before saving or printing.	**4.3.2.3** Create and save a file containing system output with PII. Attempt to alter the label that communicates the authorized use. Attempt to remove the label that communicates the authorized use.		The label will not be altered or removed.	The label will be altered or removed.
			4.3.2.4 Submit a request to print a report containing PII. Attempt to alter the label that communicates the authorized use. Attempt to remove the label that communicates the authorized use.		The label will not be altered or removed.	The label will be altered or removed.
Use/Transfer						
4.4 Transfers of PII beyond the system boundary for use by other users and/or systems shall meet the purposes of this	**4.4.1** PII shall only be transferred to authorized entities for predetermined, documented	System interfaces allow transfers of PII to unauthorized systems.	**4.4.1.1** Review interfaces to verify that PII is being transferred to the intended systems.		The system will transfer PII only to intended systems.	The system will transfer PII to systems not intended to receive it.

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
system and those of the target users and/or systems.	purposes and business needs.		**4.4.1.2** Compare connection permissions for systems against the list of systems allowed to transfer PII out of the system.		The system will allow transfers only to authorized systems.	The system will allow transfers to unauthorized systems.
			4.4.1.3 Attempt to connect from an unauthorized system and transfer PII out of the system.		The system will allow transfers only to authorized systems.	The system will allow transfers to unauthorized systems.
			4.4.1.4 Attempt to initiate from system transfer of PII to an unauthorized system.		The system will allow transfers only to authorized systems.	The system will allow transfers to unauthorized systems.
		PII that does not meet criteria in sharing agreements is transferred to a third party system.	**4.4.1.5** Compare applicable interfaces (e.g., as specified in Interface Control Documents) with sharing agreements.	Sharing agreements with third parties may include information documented in SORNs, ISAs, MOUs, MOAs, and other formal agreements.	The system will only allow the transfer of PII consistent with agreements.	The system will allow the transfer of PII not consistent with agreements.
	4.4.2 When transferring PII to other agency systems or to third	Notification of purposes and restrictions for using the PII is not	**4.4.2.1** Attempt to transfer PII from the system and observe any	Notification may be handled in multiple ways, depending on the	The system will provide notification reminding the	The system will not provide notification reminding the user of the purposes

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
	parties via the user interface, the system shall notify the user of the permissible uses and restrictions on usage of the PII.	presented prior to transferring the PII.	notification provided.	capabilities of the system, including screen views or pop-up notices. Depending on business requirements, the system may also be required to support an acknowledgement of notice received by the user.	user of the purposes and restrictions associated with the use of the PII transferred from the system.	and restrictions associated with the use of the PII transferred from the system.
	4.4.3 For systems with supporting technology, PII data fields shall be properly tagged as PII.	Data fields not properly tagged.	**4.4.3.1** Review database schema to confirm that PII data elements are tagged as such and that other data elements are not tagged as PII.		PII data elements will be tagged as PII. Other data elements will not be tagged as PII.	PII data elements will be tagged incorrectly or untagged and/or other data elements will be tagged as PII.
			4.4.3.2 Review data fields within the database to confirm that PII data elements are tagged as such and that other data elements are not tagged as PII.		PII data elements will be tagged as PII. Other data elements will not be tagged as PII.	PII data elements will be tagged incorrectly or untagged and/or other data elements will be tagged as PII.
	4.4.4 For systems with supporting technology, PII transferred to	Target system not capable of interpreting data field tags.	**4.4.4.1** Attempt to transfer data to an authorized system. Review the	This test is outside the boundary of the system tested; however, it is a	The target system will correctly interpret tags	The target system will not correctly interpret tags for PII data fields.

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
	other systems shall be transferred with proper tagging of data fields.		manner in which the target system handles the data field tags for PII.	critical step in the use of data tagging and must be considered. Metadata should be included in this review and may be the primary means for meeting this requirement. Metadata may provide information such as time/date stamps, purposes of the PII, and other valuable information about the data.	for PII data fields.	
Retention/Storage						
4.5 Any persistent storage of PII initiated by the system shall meet the purposes of the system.	**4.5.1** The system shall only retain PII pre-determined to be necessary in the authorized data store(s).	The system writes PII data elements not pre-determined to be necessary to the data store(s).	**4.5.1.1** Review the system architecture and identify the PII stored by the system.		The system will only retain PII data elements that have been pre-determined to be necessary.	The system will retain PII data elements that have not been pre-determined to be necessary.
			4.5.1.2 Review test records processed by the system.		The system will only retain PII data elements that have been pre-determined to be necessary.	The system will retain PII data elements that have not been pre-determined to be necessary.

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
		PII is written to the incorrect data store(s).	**4.5.1.3** Review interfaces to the data stores to verify that PII is being saved in the intended data stores.	Consider the impact of cloud computing, shared disk arrays, and other technologies in identifying the risk of saving information to an incorrect location.	The system will only allow PII to be saved to the intended data stores.	The system will allow PII to be saved to data stores other than the ones intended.
			4.5.1.4 Attempt to use the system to save PII to an unauthorized data store.		The system will allow PII to be saved only to the authorized data stores.	The system will allow PII to be saved to unauthorized data stores.
4.6 Any persistent storage of PII initiated by the system shall meet defined retention schedules.	**4.6.1** The system shall have a mechanism for tracking the retention periods associated with the PII it contains.	Retention tracking mechanism does not exist.	**4.6.1.1** Review the data model and data store architecture for retention tracking.	Data tags, date stamps, metadata, and other mechanisms may be used to support this requirement. .	The system will have a mechanism for tracking the retention period of each record.	The system will not have a mechanism for tracking the retention period of each record.
		Retention period not associated with PII.	**4.6.1.2** Review test data in the system for association with relevant retention periods.		PII will be associated with the applicable retention period.	PII will not be associated with a retention period and/or will be associated with the wrong retention period.
	4.6.2 The system shall only retain PII for the length of time specified	The system is not configured to enforce retention periods.	**4.6.2.1** Instantiate test data with a designated retention period	Unless there is a business need to retain PII for historical	The system will delete or appropriately archive PII after	PII will remain in the system after its retention period has expired.

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
	in the applicable Records Control Schedules.		and observe what happens when the retention period expires.	purposes, it should be deleted when no longer needed.	its retention period has expired.	
	4.6.3 For systems that handle the backup process, backup schedules shall be designed in accordance with the applicable Records Control Schedules.	PII is maintained in backups that exceeds the retention periods defined in the Records Control Schedules.	**4.6.3.1** Review the backup scripts and procedures to ensure PII is backed up in a manner that is consistent with the retention periods defined in the Records Control Schedules.	Records Control Schedules may vary from system to system. The test assumes that the cognizant authority has approved the Records Control Schedules and that these are consistent with the retention periods documented in the SORN(s) that cover this system. The schedule for rotation and overwriting backup media should be considered to further ensure retention periods are not exceeded.	Backup file(s) will not contain PII that exceeds its defined retention period.	Backup file(s) will contain PII that exceeds its defined retention period.
Disclosure/Storage						
4.7 The system shall limit disclosures of PII to what is necessary for the	**4.7.1** The system shall limit disclosure of PII to those data elements that are	The system does not limit PII data elements pushed to target systems to those pre-	**4.7.1.1** Review target system updates to verify PII data elements being sent.	Additional thought may be required when full records are being disclosed,	The system will only send PII data elements pre-determined to be necessary	The system will send PII data elements other than those pre-determined to be

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
purposes of the system.	necessary for the purposes of the system.	determined to be necessary.		including whether disclosure of the full record (instead of specific data elements) is compatible with the purposes of the system.	to target systems.	necessary to target systems.
		The system does not limit target system access to those PII data elements pre-determined to be necessary.	**4.7.1.2** Attempt queries from target systems for PII data elements not pre-determined to be necessary.		The system will only allow target systems to retrieve PII data elements pre-determined to be necessary.	The system will allow target systems to retrieve PII data elements other than those pre-determined to be necessary.
Disclosure/Viewing						
4.8 User ability to access PII contained in the system shall be limited to performing functions required to meet the purposes of the system.	**4.8.1** Views of PII shall be defined for each distinct user and/or target system role.	View templates are not implemented.	**4.8.1.1** Review system design documentation to examine view template design.		Design documentation will include information regarding the appropriate view content for each system role.	Design documentation will not adequately address the views for each role or discussion of views is absent.
		View templates are properly implemented but specific data fields are not appropriately limited (e.g. partial masking of SSN).	**4.8.1.2** Log into the system as test users with differing roles to verify that viewable PII is consistent with roles.		All PII data elements will be correctly displayed.	One or more PII data elements will not be correctly displayed.
		View templates are improperly applied.	**4.8.1.3** Log into the system as test users with differing roles to verify that views are consistent with roles.		The system will display the appropriate view to the user.	The system will not display the appropriate view to the user, which may include display of more PII data elements than allowed.

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
		Templates not used to create reports that contain PII.	**4.8.1.4** Review system functions used to generate reports.		Reports will be generated using templates that specify PII consistent with the functions of the system.	Reports will be generated without the use of templates and potentially will contain inappropriate PII.
		The system does not adequately limit authorization for authenticated users or systems according to system purpose.	**4.8.1.5** Review access controls for user accounts and target system connections.		The system will only allow user accounts and target systems access to PII that is appropriate to their associated roles in fulfilling the purposes of the system.	The system will allow user accounts or target systems access to PII beyond what is appropriate to their roles.
Retention/Destruction						

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
4.9 When PII is deleted, all instances of that PII shall be deleted.	**4.9.1** All instances and formats of each PII data element shall be locatable and shall be deleted when any one instance of that PII is deleted.	Other PII instances are not searched for.	**4.9.1.1** Review deletion routine for search and delete functionality.		Deletion routine will be constructed to search for and delete other instances of the PII to be deleted.	Deletion routine will not be properly constructed to search for and delete all other instances of the PII.
		Links between PII instances are not created or are broken.	**4.9.1.2** Load test input data so as to produce multiple instances of processed PII. Initiate processing and deletion, then manually query the database for the presence of each instance of PII.		No instances of PII will be returned.	One or more instances of PII will be returned. If all instances other than the explicitly deleted instance are returned, foreign keys in applicable tables and rows may have null values. If only some instances are returned, foreign keys in applicable tables and rows may be incorrect.

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
	4.9.2 The system shall support clean-up of temporary storage it generates in a manner consistent with the retention needs of the system.	Temporary files containing PII exist beyond the life of transactions or designated timeframe of use.	**4.9.2.1** Observe the designated locations for temp files created by the system's normal processes. Review the contents of any persistent temp files following a transaction or process involving PII.	Heavily system dependent, impacted by operating system, development platform, and specific application code.	Temp files containing PII will not exist beyond their required useful life.	Temp files containing PII will exist beyond their required useful life.
		PII exists in memory beyond its necessary use.	**4.9.2.2** Dump the memory contents created by the system's normal processes and review for presence of PII following a transaction or process involving PII.		No PII will be found in memory beyond its required presence.	PII will exist in memory beyond its required presence.

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
	4.9.3 For systems that share PII with other systems, the system shall propagate all authorized deletions of PII to target systems in accordance with requirements.	Authorized PII deletions from an authorized source are not propagated to target systems.	**4.9.3.1** Load input test PII into the system. Delete the test PII and confirm that a deletion message was transmitted to applicable target systems.	Deleting downstream PII is not always an appropriate business decision. This test will depend on the documented purposes and requirements of the target systems.	The system will transmit a message to target systems to delete the PII.	The system will not transmit a message to target systems to delete the PII.

5.5 Quality and Integrity

General Enterprise Privacy Requirement

Agencies should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.

System Requirement

Systems shall implement controls to maintain the necessary levels of accuracy, timeliness, and completeness of PII and/or to provide notifications when these thresholds are not being met. To the greatest extent possible, systems shall use PII collected directly from the individual and shall support, when appropriate, verification of PII with all relevant parties and notification of individuals prior to adverse action.

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
5.1 The system shall check PII for accuracy.	**5.1.1** The system shall ensure that multiple instances of the same PII data elements do not deviate unacceptably in their values.	Multiple instances of the same specific PII data element exist in the system or are submitted to the system, and the values are not all the same, where deviations are not authorized.	**5.1.1.1** Compare all instances where the test PII data elements appear in the system.		All instances of the same PII data element will have the same value.	All instances of the same PII data element will not have the same value.
	5.1.2 The system shall check time sequenced PII to ensure correct sequencing.	Time sequenced PII exists in the system and it is not sequenced properly (e.g., a child's DoB predates a parent's DoB).	**5.1.2.1** Enter incorrectly sequenced PII into the system and observe any warnings provided.	The exact nature of what is tested is highly system dependent.	The system will warn the user that the time sequence of the PII is incorrect.	The system will not warn the user that the time sequence of the PII is incorrect.

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
	5.1.3 The system shall check received PII for type and format consistency.	The system accepts an alphabetic value where a numeric value is expected or vice versa.	**5.1.3.1** Submit a numeric value for an alphabetic field and an alphabetic value for a numeric field.		The system will not accept the incorrect data type.	The system will accept the incorrect data type.
		The system accepts an alpha-numeric value of a length or format incompatible with the length or format expected.	**5.1.3.2** Submit an alpha-numeric PII element to the system that is incompatible with the length or format expected.		The system will not accept the incompatible data.	The system will accept the incompatible data.
		The system accepts PII that is not logically consistent (e.g., DoB and age do not match).	**5.1.3.3** Submit test PII that is not logically consistent (e.g., DoB and age do not match) to the system and observe any warnings.	The exact nature of what is tested is highly system dependent.	The system will warn the user that logical errors or inconsistencies exist.	The system will not warn the user that logical errors or inconsistencies exist.
5.2 The system shall recognize and alert the user when PII is outdated for the intended purposes of the system.	**5.2.1** The system shall check PII date thresholds to detect outdated PII and alert the user.	The system processes or propagates PII that is outside of defined date thresholds.	**5.2.1.1** Submit test PII to the system that is out of date for the intended purposes and observe any warnings.		The system will warn the user that the PII submitted is outdated for the purposes of the system.	The system will not warn the user that the PII submitted is outdated for the purposes of the system.
5.3 The system shall ensure that PII is sufficiently complete for the	**5.3.1** The system shall recognize and alert the user when	The system collects, processes, or	**5.3.1.1** Submit test PII that does not meet the established level of	The exact nature of what is tested is	The system will warn the user that the PII	The system will not warn the user that the PII

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
intended purposes of the system.	PII is not sufficiently complete to adequately accomplish the intended purposes of the system.	propagates PII that is incomplete for the intended purposes of the system.	completeness to the system and observe any warnings.	highly system dependent.	submitted is incomplete and will abort processing or flag any output based on the incomplete PII.	submitted is incomplete and/or will not abort processing and/or will not flag any output based on the incomplete PII.
5.4 The individual shall have the ability to verify their PII, as authorized.	**5.4.1** For systems that collect PII from a third party, the individual shall have the ability to verify their PII, where authorized, prior to any adverse action being taken on the basis of that PII.	The system propagates PII from third parties without flagging the PII as requiring verification prior to any action based on the PII.	**5.4.1.1** Submit test PII to the system as a third party.	Applies to all systems that collect PII from third parties.	The system will flag the third party PII as requiring verification prior to action based on that PII.	The system will not flag the PII as requiring verification prior to action being taken based on that PII.
		The system produces actionable output based on PII from a third party without verification of the PII by the individual.	**5.4.1.2** Submit test PII to the system as a third party which produces actionable output.	Applies only to systems that produce actionable output.	The system will not produce actionable output or will flag such output as requiring verification of PII prior to execution of the action.	The system will produce actionable output and will not flag such output as requiring verification of PII prior to execution of the action.
5.5 To the greatest extent possible, systems shall use PII collected	**5.5.1** PII collected directly from the individual shall take precedence over PII	The system uses PII collected from a third party source to	**5.5.1.1** Submit test PII collected as a third party source and the same test PII collected from the individual to	Applies to systems where similar PII element(s) gathered from both the individual	The system will produce output based on the PII collected from the individual.	The system will produce output based on the PII collected from the third party.

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
directly from the individual.	collected from third parties.	accomplish its purposes where the same PII collected from the individual is available.	the system with variations in the two PII submissions.	and one or more third party sources are collected, processed, or propagated, and where the PII from either source may be used to accomplish the purposes of the system.		
5.6 The individual shall be notified of adverse output from the system that is based on their PII prior to any action being taken.	**5.6.1** The system shall notify the individual either directly or indirectly of adverse output based on PII submitted to the system and notify the individual of the mechanisms for redress.	The system does not notify individuals of adverse output based on the PII submitted or the right of and mechanisms for rebuttal.	**5.6.1.1** Submit test PII that results in adverse output.	This requirement applies to systems that may produce adverse actionable output based on PII.	The system will notify the individual of adverse output and mechanisms for rebutting such output.	The system will not notify the individual of adverse output and/or mechanisms for rebutting such output.

5.6 Individual Participation

General Enterprise Privacy Requirement

Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Agencies should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.

System Requirement

Systems that directly interact with data subjects shall implement an appropriate consent process to the greatest extent possible. Systems shall be capable of appropriately supporting redress.

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
6.1 Systems that directly interface with individuals shall distinguish between mandatory and voluntary PII collection.	**6.1.1** For systems that collect PII directly from individuals, the system shall provide notice of the privacy practices associated with the system, the PII collected, and a description of how the PII is used and managed.	Notice is not provided at the point of collection.	**6.1.1.1** Attempt to enter test PII as an individual using the system. Observe any notice provided by the system.	Notice at the point of collecting PII directly from the individual allows for the assumption that the individual is providing consent for the PII collected and the purposes for which it will be used. There are various methods of providing notices through systems, depending on the purposes of the system. For example, notice may be provided through the website privacy	The system will provide notice to the user.	The system will not provide notice to the user.

				policy, as a pop-up box, end-user agreement, or as text located above the input fields for PII.		
	6.1.2 For systems that collect PII directly from individuals, the system input interfaces shall denote specific PII elements that users are required to provide and clearly note that providing all other PII is optional.	Instructions or other notes are absent from input screen.	**6.1.2.1** Review input screens to verify that user view contains instructions noting the distinction between required and optional PII.		Clear instructions regarding required and optional fields will be present on user input screens.	Clear instructions will be absent.
		Individual PII data elements not clearly marked.	**6.1.2.2** Review input screens to verify that user view clearly marks required data elements.		Required and optional data fields will be clearly indicated on user input screens.	Clear indicators will be absent.
	6.1.3 For systems that collect PII from sources other than the individual, the system shall support a method of tracking consent when appropriate.	Records do not contain a flag or some other designation denoting consent.	**6.1.3.1** Review test record for the pre-determined method of tracking/flagging consent.	There are multiple scenarios where this requirement may apply, such as when new PII is created or PII is disclosed in new ways, when legal decisions are made, or when decisions regarding benefits are made. This test will require close coordination with the Business Owner to determine specifics. "Consent" refers to providing	System records will contain a mechanism for denoting consent where relevant.	System records will not have a means of tracking consent where relevant.

				individuals the opportunity to give permission regarding how the agency collects, uses, and discloses their PII, including the decision whether to provide PII when practicable. Where consent is relevant, flags or metadata can be used in the record to denote the types of consent allowed and the level of consent provided by the individual.		
		The system does not interpret consent flag.	**6.1.3.2** Create test record with the consent flag enabled and one with the consent flag disabled. Attempt to execute an action that requires use of the consent flag.		The system will process the allowed transaction for the record with the consent flag enabled and will not process the transaction for the record that does not have the flag enabled.	The system will process the transaction for the record that does not have the consent flag enabled.
6.2 The system shall support the tracking of disputed PII.	**6.2.1** When the individual disputes the accuracy of PII or any output based on the disputed PII, the system shall maintain a flag	The system stores or propagates disputed PII or output resulting from disputed PII without	**6.2.1.1** Submit test PII to the system. Subsequently submit a dispute of the same PII.	This requirement applies to systems that may produce adverse actionable output based on PII.	The PII will be flagged as being in dispute.	The PII will not be flagged as being in dispute.

	indicating that the PII is in dispute.	flagging such PII as being in dispute.				

5.7 Purpose Specification and Use Limitation

General Enterprise Privacy Requirement

Agencies should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.

System Requirement

All PII collected or otherwise used must be relevant to the authorized purpose of the system.

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
7.1 PII in the system shall meet the authorized, documented purposes of the system.	**7.1.1** The system shall only collect and use PII relevant to its purposes as described in relevant notices.	The system captures or processes PII data elements that are not directly relevant.	**7.1.1.1** Review system data model and database architecture and associate each PII data element or logical aggregate of elements (e.g., mailing address) with a rationale for its inclusion.	Purpose Limitation is fundamentally system-specific. The implementation of this principle is heavily dependent on legal authorization and policy and could vary greatly for individual systems. Of the Enterprise Privacy Requirements, this is likely the most difficult for generating generic tests.	Each documented rationale for PII inclusion is consistent with the purposes of the system as described in relevant notices.	There is PII for which the documented rationale is not consistent with the purposes of the system as described in relevant notices.

5.8 Security

General Enterprise Privacy Requirement

Agencies should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.

System Requirement

Systems shall be capable of enforcing confidentiality, integrity, non-repudiation, and availability relating to PII.

NOTE: *Given that processes should already exist to handle testing of security controls, the privacy-centered Security test case focuses on correct reflection of the PII confidentiality impact level. The PII confidentiality impact level should not be any higher than the overall confidentiality rating assigned to the data. (See National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60[6] and SP 800-122[7] for more information.)*

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
8.1 The system's security controls shall be consistent with the PII confidentiality impact level.	**8.1.1** The system's security controls shall be based on a confidentiality impact level equal to or greater than the PII confidentiality impact level.	The system confidentiality impact level is not consistent with the PII confidentiality impact level. (This includes those cases where the PII confidentiality impact level is undetermined.)	**8.1.1.1** Verify the PII and system confidentiality impact levels and compare the two.		The system confidentiality impact level will be greater than or equal to the PII confidentiality impact level.	The system confidentiality impact level will be less than the PII confidentiality impact level or the PII confidentiality impact level will be undetermined.

[6] NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.
[7] NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* April 2010.

5.9 Transparency

General Enterprise Privacy Requirement
Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

System Requirement
Notices of privacy practices with respect to systems shall accurately reflect the current characteristics of those systems.

Level 1 Requirement	Level 2 Requirement	Faults	Tests	Comments	Expected Results: Pass	Expected Results: Fail
9.1 Unless otherwise allowed by law or other authority, the system shall handle PII in a manner that is consistent with privacy notices provided to data subjects.	**9.1.1** The system's intake of PII shall be consistent with the privacy notices related to the system, including System of Records Notice, Privacy Impact Assessment, and notices provided at points of collection.	The system takes in PII that is different or whose source is different than what is described in the relevant privacy notices.	**9.1.1.1** Compare documented system inputs with relevant privacy notices.	Types and breadth of notice provided may vary widely by system. Testers must consult with relevant offices to ensure an accurate understanding of notice statements.	System inputs will be consistent with what is described in relevant privacy notices.	There will be discrepancies between system inputs and what is described in relevant privacy notices.
	9.1.2 The system's use of PII shall be consistent with the privacy notices related to the system, including System of Records Notice, Privacy	The system is designed to use PII in a manner that is inconsistent with the relevant privacy notices.	**9.1.2.1** Compare documented system functions with relevant privacy notices.		System functions will be consistent with what is described in relevant privacy notices.	There will be discrepancies between system functions and what is described in relevant privacy notices.

	Impact Assessment, and notices provided at points of collection.					
	9.1.3 The system's disclosures of PII shall be consistent with the privacy notices related to the system, including System of Records Notice, Privacy Impact Assessment, and notices provided at points of collection.	The system propagates PII in a manner that is inconsistent with the relevant privacy notices.	**9.1.3.1** Compare documented system outputs with relevant privacy notices.		The system will only propagate PII consistent with what is described in relevant privacy notices.	There will be discrepancies between system outputs and what is described in relevant privacy notices.

6 Potential Next Steps

As this catalog of generic requirements and tests evolves, we will seek to identify further efficiencies. This may include:

- Grouping the privacy test cases based on similar business processes
- Combining test cases that call for similar activities

Grouping privacy test cases by business process identifies situations where one action produces results for multiple tests. The business process of PII disclosure demonstrates this scenario. Under the Minimization principle, test cases verify the disclosure of only required PII. Under the Accountability principle, test cases ensure an accounting of all disclosures. By viewing the disclosure process as a single business process, these tests can be combined to create output that satisfies each.

Another source of potential efficiencies is combining privacy test cases that require similar actions. As an example, test cases under Accountability and under Transparency require a comparison of privacy documentation against certain types of system functionality or architecture. Under the test plan for a system, the documentation comparison could occur once with all of the relevant results captured at the same time.

Appendix A Acronyms

ISA	Interconnection Security Agreement
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
SORN	System of Records Notice