COALFIRE

WHITE PAPER

NIST SP 800-53 Privacy controls migration

From Revision 4 to Revision 5

IAN WALTERS, PRINCIPAL

877-224-8077 | info@coalfire.com | Coalfire.com

Table of contents

Purpose **2**
Background **2**
NIST 800-53 Revisions 2
Privacy Controls **3**
AP - Authority and Purpose 3
AR - Accountability, Audit, And Risk Management 4
DI - Data Quality and Integrity 11
DM - Data Minimization and Retention 13
IP - Individual Partnership and Redress 15
SE - Security 18
TR - Transparency 20
UL - Use Limitation 22
Legal disclaimer **24**

Purpose

This whitepaper maps the Privacy controls previously found in Appendix J of NIST SP 800-53 Revision 4 to their new locations in Revision 5.

Background

NIST 800-53 Revisions

Special Publication 800-53, titled "*Security and Privacy Controls for Information Systems and Organizations*", is a comprehensive framework developed by the National Institute of Standards and Technology (NIST). It provides a framework of security and privacy controls designed to protect the confidentiality, integrity, and availability of information systems and the data they process.

In Revision 4 of the publication, privacy controls were in an appendix which was separate from the main framework of security control requirements.

In Revision 5, those privacy controls were incorporated in the main framework.

Revision 4 was officially withdrawn on September 23, 2021.

Privacy Controls

References to NIST 800-53 Revision 5 are based on version 5.1.1 which was issued on November 7th, 2023.

AP - Authority and Purpose

AP-1 Authority to Collect	
Revision 4	The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need.
Revision 5	**PT-2 Authority to Process Personally Identifiable Information** a. Determine and document the [Assignment: organization-defined authority] that permits the [Assignment: organization-defined processing] of personally identifiable information; and b. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is authorized.

AP-2 Purpose Specification	
Revision 4	The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.
Revision 5	**PT-3 Personally Identifiable Information Processing Purposes** a. Identify and document the [Assignment: organization-defined purpose(s)] for processing personally identifiable information; b. Describe the purpose(s) in the public privacy notices and policies of the organization; c. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is compatible with the identified purpose(s); and d. Monitor changes in processing personally identifiable information and implement [Assignment: organization-defined mechanisms] to ensure that any changes are made in accordance with [Assignment: organization-defined requirements].

AR - Accountability, Audit, And Risk Management

AR-1 Governance and Privacy Program	
Revision 4	The organization: a. Appoints a Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems; b. Monitors federal privacy laws and policy for changes that affect the privacy program; c. Allocates [Assignment: organization-defined allocation of budget and staffing] sufficient resources to implement and operate the organization-wide privacy program; d. Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures; e. Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and f. Updates privacy plan, policies, and procedures [Assignment: organization-defined frequency, at least biennially].
Revision 5	**PM-3 Information Security and Privacy Resources** a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement; b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and c. Make available for expenditure, the planned information security and privacy resources **PM-18 Privacy Program Plan** a. Develop and disseminate an organization-wide privacy program plan that provides an overview of the agency's privacy program, and: 1. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program; 2. Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements; 3. Includes the role of the senior agency official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities; 4. Describes management commitment, compliance, and the strategic goals and objectives of the privacy program; 5. Reflects coordination among organizational entities responsible for the different aspects of privacy; and 6. Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; and b. Update the plan [Assignment: organization-defined frequency] and address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments. **PM-19 Privacy Program Leadership Role** Appoint a senior agency official for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.

AR-2 Privacy Impact Risk Assessment	
Revision 4	The organization: a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and b. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.
Revision 5	**RA-3 Risk Assessment** a. Conduct a risk assessment, including: 1. Identifying threats to and vulnerabilities in the system; 2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and 3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information; b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments; c. Document risk assessment results in [Selection (one): security and privacy plans; risk assessment report; [Assignment: organization-defined document]]; d. Review risk assessment results [Assignment: organization-defined frequency]; e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]; and f. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system. **RA-8 Privacy Impact Assessments** Conduct privacy impact assessments for systems, programs, or other activities before: a. Developing or procuring information technology that processes personally identifiable information; and b. Initiating a new collection of personally identifiable information that: 1. Will be processed using information technology; and 2. Includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities, or employees of the federal government.

AR-3 Privacy Requirement for Contractor and Service Provider	
Revision 4	The organization: a. Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and b. Includes privacy requirements in contracts and other acquisition-related documents
Revision 5	**SA-1 System and Services Acquisition Policy and Procedures** a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that:

AR-3 Privacy Requirement for Contractor and Service Provider	
	a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and c. Review and update the current system and services acquisition: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. **SA-4 Acquisition Process** Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service: a. Security and privacy functional requirements; b. Strength of mechanism requirements; c. Security and privacy assurance requirements; d. Controls needed to satisfy the security and privacy requirements. e. Security and privacy documentation requirements; f. Requirements for protecting security and privacy documentation; g. Description of the system development environment and environment in which the system is intended to operate; h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and i. Acceptance criteria. **SA-9 External System Services** a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [Assignment: organization-defined controls]; b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [Assignment: organization-defined processes, methods, and techniques].

AR-4 Privacy Monitoring and Auditing	
Revision 4	The organization monitors and audits privacy controls and internal privacy policy [Assignment: organization-defined frequency] to ensure effective implementation.
Revision 5	**CA-2 Control Assessments** a. Select the appropriate assessor or assessment team for the type of assessment to be conducted; b. Develop a control assessment plan that describes the scope of the assessment including:

AR-4 Privacy Monitoring and Auditing	
	1. Controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment; d. Assess the controls in the system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements; e. Produce a control assessment report that document the results of the assessment; and f. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].

AR-5 Privacy Awareness and Training	
Revision 4	The organization: a. Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures; b. Administers basic privacy training [Assignment: organization-defined frequency, at least annually] and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII [Assignment: organization-defined frequency, at least annually]; and c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements [Assignment: organization-defined frequency, at least annually].
Revision 5	**AT-1 Awareness and Training Policy and Procedures** a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that: a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and c. Review and update the current awareness and training: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. **AT-2 Literacy Training and Awareness** a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors): 1. As part of initial training for new users and [Assignment: organization-defined frequency] thereafter; and 2. When required by system changes or following [Assignment: organization-defined events]; b. Employ the following techniques to increase the security and privacy awareness of system users [Assignment: organization-defined awareness techniques];

AR-5 Privacy Awareness and Training	
	c. Update literacy training and awareness content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques. **AT-3 Role-Based Training** a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [Assignment: organization-defined roles and responsibilities]: 1. Before authorizing access to the system, information, or performing assigned duties, and [Assignment: organization-defined frequency] thereafter; and 2. When required by system changes; b. Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training. **PL-4 Rules of Behavior** a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy; b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system; c. Review and update the rules of behavior [Assignment: organization-defined frequency]; and d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [Selection (one or more): [Assignment: organization-defined frequency]; when the rules are revised or updated].

AR-6 Privacy Reporting	
Revision 4	The organization develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.
Revision 5	**PM-27 Privacy Reporting** a. Develop [Assignment: organization-defined privacy reports] and disseminate to: 1. [Assignment: organization-defined oversight bodies] to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and 2. [Assignment: organization-defined officials] and other personnel with responsibility for monitoring privacy program compliance; and b. Review and update privacy reports [Assignment: organization-defined frequency].

AR-7 Privacy Enhanced System Design and Development	
Revision 4	The organization designs information systems to support privacy by automating privacy controls.
Revision 5	**SA-8 Security and Privacy Engineering Principles**

AR-7 Privacy Enhanced System Design and Development	
	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles]. **SA-15 Development Process, Standards, and Tools** a. Require the developer of the system, system component, or system service to follow a documented development process that: 1. Explicitly addresses security and privacy requirements; 2. Identifies the standards and tools used in the development process; 3. Documents the specific tool options and tool configurations used in the development process; and 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and b. Review the development process, standards, tools, tool options, and tool configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: [Assignment: organization-defined security and privacy requirements]. **SA-17 Developer Security and Privacy Architecture and Design** Require the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that: a. Is consistent with the organization's security and privacy architecture that is an integral part the organization's enterprise architecture; b. Accurately and completely describes the required security and privacy functionality, and the allocation of controls among physical and logical components; and c. Expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection.

AR-8 Accounting of Disclosure	
Revision 4	The organization: a. Keeps an accurate accounting of disclosures of information held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made; b. Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and c. Makes the accounting of disclosures available to the person named in the record upon request
Revision 5	**PM-21 Accounting of Disclosures** a. Develop and maintain an accurate accounting of disclosures of personally identifiable information, including: 1. Date, nature, and purpose of each disclosure; and 2. Name and address, or other contact information of the individual or organization to which the disclosure was made; b. Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer; and

AR-8 Accounting of Disclosure	
	c. Make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request.

DI - Data Quality and Integrity

DI-1 Data Quality, DI-1(1) Validate PII, DI-1(2) Re-Validate PII	
Revision 4	The organization: a. Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information; b. Collects PII directly from the individual to the greatest extent practicable; c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems [Assignment: organization-defined frequency]; and d. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information. The organization requests that the individual or individual's authorized representative validate PII during the collection process. The organization requests that the individual or individual's authorized representative revalidate that PII collected is still accurate [Assignment: organization-defined frequency].
Revision 5	**PM-22 Personally Identifiable Information Quality Management** Develop and document organization-wide policies and procedures for: a. Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle; b. Correcting or deleting inaccurate or outdated personally identifiable information; c. Disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities; and d. Appeals of adverse decisions on correction or deletion requests. **SI-18 Personally Identifiable Information Quality Operations** a. Check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle [Assignment: organization-defined frequency]; and b. Correct or delete inaccurate or outdated personally identifiable information.

DI-2 Data Integrity and Data Integrity Board, DI-2(1) Publish Agreements on Website	
Revision 4	The organization: a. Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and b. Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements123 and to ensure that those agreements comply with the computer matching provisions of the Privacy Act. The organization publishes Computer Matching Agreements on its public website.
Revision 5	**PM-24 Data Integrity Board** Establish a Data Integrity Board to:

DI-2 Data Integrity and Data Integrity Board, DI-2(1) Publish Agreements on Website

a. Review proposals to conduct or participate in a matching program; and

b. Conduct an annual review of all matching programs in which the agency has participated.

SI-1 System and Information Integrity Policy and Procedures

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and information integrity policy that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and

c. Review and update the current system and information integrity:

1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

DM - Data Minimization and Retention

DM-1 Minimization of PII, DM-1(1) Locate/Remove/Redact/Anonymize PII	
Revision 4	The organization: a. Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection; b. 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; and c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings [Assignment: organization-defined frequency, at least annually] to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose. The organization, where feasible and within the limits of technology, locates and removes/redacts specified PII and/or uses anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.
Revision 5	**PM-5(1) System Inventory | Inventory of Personally Identifiable Information** Establish, maintain, and update [Assignment: organization-defined frequency] an inventory of all systems, applications, and projects that process personally identifiable information. **SA-8(33) Security and Privacy Engineering Principles | Minimization** Implement the privacy principle of minimization using [Assignment: organization-defined processes] **SI-12(2) Information Management and Retention | Minimize Personally Identifiable Information in Testing, Training, and Research** Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: [Assignment: organization-defined techniques].

DM-2 Data Retention and Disposal, DM-2(1) System Configuration	
Revision 4	The organization: a. Retains each collection of personally identifiable information (PII) for [Assignment: organization-defined time period] to fulfill the purpose(s) identified in the notice or as required by law; b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and c. Uses [Assignment: organization-defined techniques or methods] to ensure secure deletion or destruction of PII (including originals, copies, and archived records). The organization, where feasible, configures its information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under an approved record retention schedule.
Revision 5	**MP-6 Media Sanitization** a. Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; and

DM-2 Data Retention and Disposal, DM-2(1) System Configuration	
	b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. **SI-12 Information Management and Retention** Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. **SI-12(3) Information Management and Retention | Information Disposal** Use the following techniques to dispose of, destroy, or erase information following the retention period: [Assignment: organization-defined techniques].

DM-3 Minimization of PII Used in Testing, Training & Research, DM-3(1) Risk Minimization Techniques	
Revision 4	The organization: a. Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and b. Implements controls to protect PII used for testing, training, and research. The organization, where feasible, uses techniques to minimize the risk to privacy of using PII for research, testing, or training.
Revision 5	**PM-25 Minimization of Personally Identifiable Information Used in Testing, Training, and Research** a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research; b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes; c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and d. Review and update policies and procedures [Assignment: organization-defined frequency]. **SI-12(2) Information Management and Retention | Minimize Personally Identifiable Information in Testing, Training, and Research** Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: [Assignment: organization-defined techniques].

IP - Individual Partnership and Redress

IP-1 Consent, IP-1(1) Mechanism Supporting Itemized or Tiered Consent	
Revision 4	The organization: a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection; b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII; c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and d. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII. The organization implements mechanisms to support itemized or tiered consent for specific uses of data.
Revision 5	**PT-4 Consent** Implement [Assignment: organization-defined tools or mechanisms] for individuals to consent to the processing of their personally identifiable information prior to its collection that facilitate individuals' informed decision-making.

IP-2 Individual Access	
Revision 4	The organization: a. Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records; b. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records; c. Publishes access procedures in System of Records Notices (SORNs); and d. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.
Revision 5	**AC-1 Access Control Policy and Procedures** a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that: a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the access control policy and the associated access controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and c. Review and update the current access control: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. **AC-3(14) Access Enforcement | Individual Access**

IP-2 Individual Access	
	Provide [Assignment: organization-defined mechanisms] to enable individuals to have access to the following elements of their personally identifiable information: [Assignment: organization-defined elements]. **PM-20 Dissemination of Privacy Program Information** Maintain a central resource webpage on the organization's principal public website that serves as a central source of information about the organization's privacy program and that: a. Ensures that the public has access to information about organizational privacy activities and can communicate with its senior agency official for privacy; b. Ensures that organizational privacy practices and reports are publicly available; and c. Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices. **PT-5 Privacy Notice** Provide notice to individuals about the processing of personally identifiable information that: a. Is available to individuals upon first interacting with an organization, and subsequently at [Assignment: organization-defined frequency]; b. Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language; c. Identifies the authority that authorizes the processing of personally identifiable information; d. Identifies the purposes for which personally identifiable information is to be processed; and e. Includes [Assignment: organization-defined information]. **PT-6 System of Records Notice** For systems that process information that will be maintained in a Privacy Act system of records: a. Draft system of records notices in accordance with OMB guidance and submit new and significantly modified system of records notices to the OMB and appropriate congressional committees for advance review; b. Publish system of records notices in the Federal Register; and c. Keep system of records notices accurate, up-to-date, and scoped in accordance with policy.

IP-3 Redress	
Revision 4	The organization: a. Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and b. Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.
Revision 5	**PM-22 Personally Identifiable Information Quality Management** Develop and document organization-wide policies and procedures for:

	IP-3 Redress
	a. Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle; b. Correcting or deleting inaccurate or outdated personally identifiable information; c. Disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities; and d. Appeals of adverse decisions on correction or deletion requests. **SI-18 Personally Identifiable Information Quality Operations** a. Check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle [Assignment: organization-defined frequency]; and b. Correct or delete inaccurate or outdated personally identifiable information. **SI-18(4) Personally Identifiable Information Quality Operations | Individual Requests** a. Check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle [Assignment: organization-defined frequency]; and b. Correct or delete inaccurate or outdated personally identifiable information. **SI-19 De-Identification** a. Remove the following elements of personally identifiable information from datasets: [Assignment: organization-defined elements of personally identifiable information]; and b. Evaluate [Assignment: organization-defined frequency] for effectiveness of de-identification.

	IP-4 Complaint Management, IP-4(1) Response Times
Revision 4	The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices. The organization responds to complaints, concerns, or questions from individuals within [Assignment: organization-defined time period].
Revision 5	**PM-26 Complaint Management** Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes: a. Mechanisms that are easy to use and readily accessible by the public; b. All information necessary for successfully filing complaints; c. Tracking mechanisms to ensure all complaints received are reviewed and addressed within [Assignment: organization-defined time period]; d. Acknowledgement of receipt of complaints, concerns, or questions from individuals within [Assignment: organization-defined time period]; and e. Response to complaints, concerns, or questions from individuals within [Assignment: organization-defined time period].

SE - Security

SE-1 Inventory of PII	
Revision 4	The organization: a. Establishes, maintains, and updates [Assignment: organization-defined frequency] an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and b. Provides each update of the PII inventory to the CIO or information security official [Assignment: organization-defined frequency] to support the establishment of information security requirements for all new or modified information systems containing PII.
Revision 5	**PM-5(1) System Inventory | Inventory of Personally Identifiable Information** Establish, maintain, and update [Assignment: organization-defined frequency] an inventory of all systems, applications, and projects that process personally identifiable information.

SE-2 Privacy Incident Response	
Revision 4	The organization: a. Develops and implements a Privacy Incident Response Plan; and b. Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.
Revision 5	**IR-8 Incident Response Plan** a. Develop an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; 8. Addresses the sharing of incident information; 9. Is reviewed and approved by [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]; and 10. Explicitly designates responsibility for incident response to [Assignment: organization-defined entities, personnel, or roles]. b. Distribute copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing; d. Communicate incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and e. Protect the incident response plan from unauthorized disclosure and modification. **IR-8(1) Incident Response Plan | Breaches**

SE-2 Privacy Incident Response	
	Include the following in the Incident Response Plan for breaches involving personally identifiable information: a. A process to determine if notice to individuals or other organizations, including oversight organizations, is needed; b. An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and c. Identification of applicable privacy requirements.

TR - Transparency

TR-1 Privacy Notices, TR-1(1) Real-Time or Layered Notice	
Revision 4	The organization: a. Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary; b. Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and c. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change. The organization provides real-time and/or layered notice when it collects PII.
Revision 5	**PT-5 Privacy Notice** Provide notice to individuals about the processing of personally identifiable information that: a. Is available to individuals upon first interacting with an organization, and subsequently at [Assignment: organization-defined frequency]; b. Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language; c. Identifies the authority that authorizes the processing of personally identifiable information; d. Identifies the purposes for which personally identifiable information is to be processed; and e. Includes [Assignment: organization-defined information]. **PT-5(1) Privacy Notice | Just-In-Time Notice** Present notice of personally identifiable information processing to individuals at a time and location where the individual provides personally identifiable information or in conjunction with a data action, or [Assignment: organization-defined frequency].

TR-2 System of Records Notices and Privacy Act Statements, TR-2(1) Public Website Publication	
Revision 4	The organization: a. Publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII); b. Keeps SORNs current; and c. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected. The organization publishes SORNs on its public website.
Revision 5	**PT-5(2) Privacy Notice | Privacy Act Statements**

TR-2 System of Records Notices and Privacy Act Statements, TR-2(1) Public Website Publication	
	Include Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals **PT-6 System of Records Notice** For systems that process information that will be maintained in a Privacy Act system of records: a. Draft system of records notices in accordance with OMB guidance and submit new and significantly modified system of records notices to the OMB and appropriate congressional committees for advance review; b. Publish system of records notices in the Federal Register; and c. Keep system of records notices accurate, up-to-date, and scoped in accordance with policy.

TR-3 Dissemination of Privacy Program Information	
Revision 4	The organization: a. Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO); and b. Ensures that its privacy practices are publicly available through organizational websites or otherwise.
Revision 5	**PM-20 Dissemination of Privacy Program Information** Maintain a central resource webpage on the organization's principal public website that serves as a central source of information about the organization's privacy program and that: a. Ensures that the public has access to information about organizational privacy activities and can communicate with its senior agency official for privacy; b. Ensures that organizational privacy practices and reports are publicly available; and c. Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

UL - Use Limitation

UL-1 Internal Use	
Revision 4	The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.
Revision 5	**PT-3 Personally Identifiable Information Processing Purposes** a. Identify and document the [Assignment: organization-defined purpose(s)] for processing personally identifiable information; b. Describe the purpose(s) in the public privacy notices and policies of the organization; c. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is compatible with the identified purpose(s); and d. Monitor changes in processing personally identifiable information and implement [Assignment: organization-defined mechanisms] to ensure that any changes are made in accordance with [Assignment: organization-defined requirements].

UL-2 Information Sharing with Third Parties	
Revision 4	The organization: a. Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes; b. Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used; c. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and d. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.
Revision 5	**AC-21 Information Sharing** a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and b. Employ [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing and collaboration decisions. **AT-3(5) Role-Based Training | Processing Personally Identifiable Information** Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of personally identifiable information processing and transparency controls. **AU-2 Event Logging** a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;

UL-2 Information Sharing with Third Parties	
	c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-02a.) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency]. **PT-2 Authority to Process Personally Identifiable Information** a. Determine and document the [Assignment: organization-defined authority] that permits the [Assignment: organization-defined processing] of personally identifiable information; and b. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is authorized. **PT-3 Personally Identifiable Information Processing Purposes** a. Identify and document the [Assignment: organization-defined purpose(s)] for processing personally identifiable information; b. Describe the purpose(s) in the public privacy notices and policies of the organization; c. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is compatible with the identified purpose(s); and d. Monitor changes in processing personally identifiable information and implement [Assignment: organization-defined mechanisms] to ensure that any changes are made in accordance with [Assignment: organization-defined requirements].

Legal disclaimer

This white paper is provided by Coalfire Systems, Inc. or its subsidiaries (“Coalfire”) for informational purposes only. This white paper is the property of Coalfire and is protected by U.S. and international copyright laws. Unauthorized use, reproduction, or distribution of this white paper, in whole or in part, is strictly prohibited. Factual information included in this white paper has been taken from sources that Coalfire believes to be reliable, but its accuracy, completeness, or interpretation cannot be guaranteed. Information is current as of the date of this white paper only and is subject to change without notice. This white paper is provided “as-is” with no warranties, including any warranty of merchantability, fitness for a particular purpose, and non-infringement. Coalfire expressly disclaims all liability arising from or relating to the use of any information or material included in this white paper for any purpose, including any actions taken or not taken based on the contents of this white paper. You are solely responsible for making your own independent assessment of the information in this white paper and for the development, implementation, and execution of your information security program. For questions regarding any legal or compliance matters referenced in this white paper, you should consult your legal counsel, security advisor, or the relevant standard authority.

About the author

Ian Walters, Principal

Ian is a seasoned cybersecurity professional with a wealth of experience across a spectrum of frameworks and standards, including NIST 800-53, HIPAA, ISO 27001, ISO 20000, and ISO 9001.

With a meticulous eye for detail and a strategic mindset, Ian excels in developing tailored solutions to ensure compliance and mitigate risks within complex organizational environments. His expertise extends to leading audits and risk assessments, as well as providing advisory for driving continuous improvement initiatives to enhance cybersecurity posture and operational resilience.

About Coalfire

The world's leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS businesses – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success. For more information, visit **Coalfire.com**.

Copyright © 2025 Coalfire. All rights reserved. The information in this document is subject to change at any time based on revisions to applicable regulations and standards. Any forward-looking statements are not predictions and are subject to change without notice. Coalfire is not responsible for any errors or omissions.

WP_NIST 800-53 Privacy Controls Migration_07162025