3.15 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY

Quick link to Personally Identifiable Information Processing and Transparency table

PT-1 POLICY AND PROCEDURES

Control:

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*] personally identifiable information processing and transparency 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 personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures; and

c. Review and update the current personally identifiable information processing and transparency:

   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*].

Discussion: Personally identifiable information processing and transparency policy and procedures address the controls in the PT family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of personally identifiable information processing and transparency policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to personally identifiable information processing and transparency policy and procedures include assessment or audit findings, breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: None.

Control Enhancements: None.

References: [OMB A-130].

PT-2 AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION

Control:

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.

Discussion: The processing of personally identifiable information is an operation or set of operations that the information system or organization performs with respect to personally identifiable information across the information life cycle. Processing includes but is not limited to creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal. Processing operations also include logging, generation, and transformation, as well as analysis techniques, such as data mining.

Organizations may be subject to laws, executive orders, directives, regulations, or policies that establish the organization's authority and thereby limit certain types of processing of personally identifiable information or establish other requirements related to the processing. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such authority, particularly if the organization is subject to multiple jurisdictions or sources of authority. For organizations whose processing is not determined according to legal authorities, the organization's policies and determinations govern how they process personally identifiable information. While processing of personally identifiable information may be legally permissible, privacy risks may still arise. Privacy risk assessments can identify the privacy risks associated with the authorized processing of personally identifiable information and support solutions to manage such risks.

Organizations consider applicable requirements and organizational policies to determine how to document this authority. For federal agencies, the authority to process personally identifiable information is documented in privacy policies and notices, system of records notices, privacy impact assessments, [PRIVACT] statements, computer matching agreements and notices, contracts, information sharing agreements, memoranda of understanding, and other documentation.

Organizations take steps to ensure that personally identifiable information is only processed for authorized purposes, including training organizational personnel on the authorized processing of personally identifiable information and monitoring and auditing organizational use of personally identifiable information.

Related Controls: AC-2, AC-3, CM-13, IR-9, PM-9, PM-24, PT-1, PT-3, PT-5, PT-6, RA-3, RA-8, SI-12, SI-18.

Control Enhancements:

(1) AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION | DATA TAGGING

Attach data tags containing [*Assignment: organization-defined authorized processing*] to [*Assignment: organization-defined elements of personally identifiable information*].

Discussion: Data tags support the tracking and enforcement of authorized processing by conveying the types of processing that are authorized along with the relevant elements of

personally identifiable information throughout the system. Data tags may also support the use of automated tools.

Related Controls: AC-16, CA-6, CM-12, PM-5, PM-22, PT-4, SC-16, SC-43, SI-10, SI-15, SI-19.

(2) AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION | AUTOMATION

Manage enforcement of the authorized processing of personally identifiable information using [*Assignment: organization-defined automated mechanisms*].

Discussion: Automated mechanisms augment verification that only authorized processing is occurring.

Related Controls: CA-6, CM-12, PM-5, PM-22, PT-4, SC-16, SC-43, SI-10, SI-15, SI-19.

References: [PRIVACT], [OMB A-130], [IR 8112].

PT-3 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES

Control:

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*].

Discussion: Identifying and documenting the purpose for processing provides organizations with a basis for understanding why personally identifiable information may be processed. The term "process" includes every step of the information life cycle, including creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal. Identifying and documenting the purpose of processing is a prerequisite to enabling owners and operators of the system and individuals whose information is processed by the system to understand how the information will be processed. This enables individuals to make informed decisions about their engagement with information systems and organizations and to manage their privacy interests. Once the specific processing purpose has been identified, the purpose is described in the organization's privacy notices, policies, and any related privacy compliance documentation, including privacy impact assessments, system of records notices, [PRIVACT] statements, computer matching notices, and other applicable Federal Register notices.

Organizations take steps to help ensure that personally identifiable information is processed only for identified purposes, including training organizational personnel and monitoring and auditing organizational processing of personally identifiable information.

Organizations monitor for changes in personally identifiable information processing. Organizational personnel consult with the senior agency official for privacy and legal counsel to ensure that any new purposes that arise from changes in processing are compatible with the purpose for which the information was collected, or if the new purpose is not compatible, implement mechanisms in accordance with defined requirements to allow for the new processing, if appropriate. Mechanisms may include obtaining consent from individuals, revising privacy policies, or other measures to manage privacy risks that arise from changes in personally identifiable information processing purposes.

Related Controls: AC-2, AC-3, AT-3, CM-13, IR-9, PM-9, PM-25, PT-2, PT-5, PT-6, PT-7, RA-8, SC-43, SI-12, SI-18.

Control Enhancements:

(1) PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES | DATA TAGGING

Attach data tags containing the following purposes to [*Assignment: organization-defined elements of personally identifiable information*]: [*Assignment: organization-defined processing purposes*].

Discussion: Data tags support the tracking of processing purposes by conveying the purposes along with the relevant elements of personally identifiable information throughout the system. By conveying the processing purposes in a data tag along with the personally identifiable information as the information transits a system, a system owner or operator can identify whether a change in processing would be compatible with the identified and documented purposes. Data tags may also support the use of automated tools.

Related Controls: CA-6, CM-12, PM-5, PM-22, SC-16, SC-43, SI-10, SI-15, SI-19.

(2) PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES | AUTOMATION

Track processing purposes of personally identifiable information using [*Assignment: organization-defined automated mechanisms*].

Discussion: Automated mechanisms augment tracking of the processing purposes.

Related Controls: CA-6, CM-12, PM-5, PM-22, SC-16, SC-43, SI-10, SI-15, SI-19.

References: [PRIVACT], [OMB A-130], [IR 8112].

PT-4 CONSENT

Control: 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.

Discussion: Consent allows individuals to participate in making decisions about the processing of their information and transfers some of the risk that arises from the processing of personally identifiable information from the organization to an individual. Consent may be required by applicable laws, executive orders, directives, regulations, policies, standards, or guidelines. Otherwise, when selecting consent as a control, organizations consider whether individuals can be reasonably expected to understand and accept the privacy risks that arise from their authorization. Organizations consider whether other controls may more effectively mitigate privacy risk either alone or in conjunction with consent. Organizations also consider any demographic or contextual factors that may influence the understanding or behavior of individuals with respect to the processing carried out by the system or organization. When soliciting consent from individuals, organizations consider the appropriate mechanism for obtaining consent, including the type of consent (e.g., opt-in, opt-out), how to properly authenticate and identity proof individuals and how to obtain consent through electronic means. In addition, organizations consider providing a mechanism for individuals to revoke consent once it has been provided, as appropriate. Finally, organizations consider usability factors to help individuals understand the risks being accepted when providing consent, including the use of plain language and avoiding technical jargon.

Related Controls: AC-16, PT-2, PT-5.

Control Enhancements:

(1) CONSENT | TAILORED CONSENT

Provide [*Assignment: organization-defined mechanisms*] to allow individuals to tailor processing permissions to selected elements of personally identifiable information.

Discussion: While some processing may be necessary for the basic functionality of the product or service, other processing may not. In these circumstances, organizations allow individuals to select how specific personally identifiable information elements may be processed. More tailored consent may help reduce privacy risk, increase individual satisfaction, and avoid adverse behaviors, such as abandonment of the product or service.

Related Controls: PT-2.

(2) CONSENT | JUST-IN-TIME CONSENT

Present [*Assignment: organization-defined consent mechanisms*] to individuals at [*Assignment: organization-defined frequency*] and in conjunction with [*Assignment: organization-defined personally identifiable information processing*].

Discussion: Just-in-time consent enables individuals to participate in how their personally identifiable information is being processed at the time or in conjunction with specific types of data processing when such participation may be most useful to the individual. Individual assumptions about how personally identifiable information is being processed might not be accurate or reliable if time has passed since the individual last gave consent or the type of processing creates significant privacy risk. Organizations use discretion to determine when to use just-in-time consent and may use supporting information on demographics, focus groups, or surveys to learn more about individuals' privacy interests and concerns.

Related Controls: PT-2.

(3) CONSENT | REVOCATION

Implement [*Assignment: organization-defined tools or mechanisms*] for individuals to revoke consent to the processing of their personally identifiable information.

Discussion: Revocation of consent enables individuals to exercise control over their initial consent decision when circumstances change. Organizations consider usability factors in enabling easy-to-use revocation capabilities.

Related Controls: PT-2.

References: [PRIVACT], [OMB A-130], [SP 800-63-3].

PT-5 PRIVACY NOTICE

Control: 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*].

Discussion: Privacy notices help inform individuals about how their personally identifiable information is being processed by the system or organization. Organizations use privacy notices to inform individuals about how, under what authority, and for what purpose their personally identifiable information is processed, as well as other information such as choices individuals might have with respect to that processing and other parties with whom information is shared. Laws, executive orders, directives, regulations, or policies may require that privacy notices include specific elements or be provided in specific formats. Federal agency personnel consult with the senior agency official for privacy and legal counsel regarding when and where to provide

privacy notices, as well as elements to include in privacy notices and required formats. In circumstances where laws or government-wide policies do not require privacy notices, organizational policies and determinations may require privacy notices and may serve as a source of the elements to include in privacy notices.

Privacy risk assessments identify the privacy risks associated with the processing of personally identifiable information and may help organizations determine appropriate elements to include in a privacy notice to manage such risks. To help individuals understand how their information is being processed, organizations write materials in plain language and avoid technical jargon.

Related Controls: PM-20, PM-22, PT-2, PT-3, PT-4, PT-7, RA-3, SC-42, SI-18.

Control Enhancements:

(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*].

Discussion: Just-in-time notices inform individuals of how organizations process their personally identifiable information at a time when such notices may be most useful to the individuals. Individual assumptions about how personally identifiable information will be processed might not be accurate or reliable if time has passed since the organization last presented notice or the circumstances under which the individual was last provided notice have changed. A just-in-time notice can explain data actions that organizations have identified as potentially giving rise to greater privacy risk for individuals. Organizations can use a just-in-time notice to update or remind individuals about specific data actions as they occur or highlight specific changes that occurred since last presenting notice. A just-in-time notice can be used in conjunction with just-in-time consent to explain what will occur if consent is declined. Organizations use discretion to determine when to use a just-in-time notice and may use supporting information on user demographics, focus groups, or surveys to learn about users' privacy interests and concerns.

Related Controls: PM-21.

(2) PRIVACY NOTICE | PRIVACY ACT STATEMENTS

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.

Discussion: If a federal agency asks individuals to supply information that will become part of a system of records, the agency is required to provide a [PRIVACT] statement on the form used to collect the information or on a separate form that can be retained by the individual. The agency provides a [PRIVACT] statement in such circumstances regardless of whether the information will be collected on a paper or electronic form, on a website, on a mobile application, over the telephone, or through some other medium. This requirement ensures that the individual is provided with sufficient information about the request for information to make an informed decision on whether or not to respond.

[PRIVACT] statements provide formal notice to individuals of the authority that authorizes the solicitation of the information; whether providing the information is mandatory or voluntary; the principal purpose(s) for which the information is to be used; the published routine uses to which the information is subject; the effects on the individual, if any, of not providing all or any part of the information requested; and an appropriate citation and link to the relevant system of records notice. Federal agency personnel consult with the senior agency official for privacy and legal counsel regarding the notice provisions of the [PRIVACT].

Related Controls: PT-6.

Control Enhancements: None.

References: [PRIVACT], [OMB A-130], [OMB A-108].

PT-6 SYSTEM OF RECORDS NOTICE

Control: 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.

Discussion: The [PRIVACT] requires that federal agencies publish a system of records notice in the Federal Register upon the establishment and/or modification of a [PRIVACT] system of records. As a general matter, a system of records notice is required when an agency maintains a group of any records under the control of the agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier. The notice describes the existence and character of the system and identifies the system of records, the purpose(s) of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom records are maintained, the routine uses to which the records are subject, and additional details about the system as described in [OMB A-108].

Related Controls: AC-3, PM-20, PT-2, PT-3, PT-5.

Control Enhancements:

(1) SYSTEM OF RECORDS NOTICE | ROUTINE USES

Review all routine uses published in the system of records notice at [*Assignment: organization-defined frequency*] to ensure continued accuracy, and to ensure that routine uses continue to be compatible with the purpose for which the information was collected.

Discussion: A [PRIVACT] routine use is a particular kind of disclosure of a record outside of the federal agency maintaining the system of records. A routine use is an exception to the [PRIVACT] prohibition on the disclosure of a record in a system of records without the prior written consent of the individual to whom the record pertains. To qualify as a routine use, the disclosure must be for a purpose that is compatible with the purpose for which the information was originally collected. The [PRIVACT] requires agencies to describe each routine use of the records maintained in the system of records, including the categories of users of the records and the purpose of the use. Agencies may only establish routine uses by explicitly publishing them in the relevant system of records notice.

Related Controls: None.

(2) SYSTEM OF RECORDS NOTICE | EXEMPTION RULES

Review all Privacy Act exemptions claimed for the system of records at [*Assignment: organization-defined frequency*] to ensure they remain appropriate and necessary in accordance with law, that they have been promulgated as regulations, and that they are accurately described in the system of records notice.

Discussion: The [PRIVACT] includes two sets of provisions that allow federal agencies to claim exemptions from certain requirements in the statute. In certain circumstances, these provisions allow agencies to promulgate regulations to exempt a system of records from select provisions of the [PRIVACT]. At a minimum, organizations' [PRIVACT] exemption

regulations include the specific name(s) of any system(s) of records that will be exempt, the specific provisions of the [PRIVACT] from which the system(s) of records is to be exempted, the reasons for the exemption, and an explanation for why the exemption is both necessary and appropriate.

Related Controls: None.

References: [PRIVACT], [OMB A-108].

PT-7 SPECIFIC CATEGORIES OF PERSONALLY IDENTIFIABLE INFORMATION

Control: Apply [*Assignment: organization-defined processing conditions*] for specific categories of personally identifiable information.

Discussion: Organizations apply any conditions or protections that may be necessary for specific categories of personally identifiable information. These conditions may be required by laws, executive orders, directives, regulations, policies, standards, or guidelines. The requirements may also come from the results of privacy risk assessments that factor in contextual changes that may result in an organizational determination that a particular category of personally identifiable information is particularly sensitive or raises particular privacy risks. Organizations consult with the senior agency official for privacy and legal counsel regarding any protections that may be necessary.

Related Controls: IR-9, PT-2, PT-3, RA-3.

Control Enhancements:

(1) SPECIFIC CATEGORIES OF PERSONALLY IDENTIFIABLE INFORMATION | SOCIAL SECURITY NUMBERS

When a system processes Social Security numbers:

(a) Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier;

(b) Do not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her Social Security number; and

(c) Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

Discussion: Federal law and policy establish specific requirements for organizations' processing of Social Security numbers. Organizations take steps to eliminate unnecessary uses of Social Security numbers and other sensitive information and observe any particular requirements that apply.

Related Controls: IA-4.

(2) SPECIFIC CATEGORIES OF PERSONALLY IDENTIFIABLE INFORMATION | FIRST AMENDMENT INFORMATION

Prohibit the processing of information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity.

Discussion: The [PRIVACT] limits agencies' ability to process information that describes how individuals exercise rights guaranteed by the First Amendment. Organizations consult with the senior agency official for privacy and legal counsel regarding these requirements.

Related Controls: None.

References: [PRIVACT], [OMB A-130], [OMB A-108], [NARA CUI].

PT-8 COMPUTER MATCHING REQUIREMENTS

Control: When a system or organization processes information for the purpose of conducting a matching program:

a. Obtain approval from the Data Integrity Board to conduct the matching program;

b. Develop and enter into a computer matching agreement;

c. Publish a matching notice in the Federal Register;

d. Independently verify the information produced by the matching program before taking adverse action against an individual, if required; and

e. Provide individuals with notice and an opportunity to contest the findings before taking adverse action against an individual.

Discussion: The [PRIVACT] establishes requirements for federal and non-federal agencies if they engage in a matching program. In general, a matching program is a computerized comparison of records from two or more automated [PRIVACT] systems of records or an automated system of records and automated records maintained by a non-federal agency (or agent thereof). A matching program either pertains to federal benefit programs or federal personnel or payroll records. A federal benefit match is performed to determine or verify eligibility for payments under federal benefit programs or to recoup payments or delinquent debts under federal benefit programs. A matching program involves not just the matching activity itself but also the investigative follow-up and ultimate action, if any.

Related Controls: PM-24.

Control Enhancements: None.

References: [PRIVACT], [CMPPA], [OMB A-130], [OMB A-108].