

Version <X.Y>

<Date>

Prepared for:

<Organization>

Prepared by:

<Author(s)>

Contract: <Contract ID>

<Other Front Matter>

<Organization-specific legal boilerplate, if applicable>

For Internal <Organization> Use. This document was prepared for authorized distribution only. It has not been approved for public release.



This document is derived from  
*MITRE Adaptive Capabilities Testing (ACT)™*.  
act.mitre.org | act@mitre.org

<Organization>

MITRE Adaptive Capabilities Testing (ACT)™

<System Name> (<System Acronym>)

Privacy  
Questionnaire

Record of Changes

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Responsible Author | Description of Change |
| 1.0 | May 30, 2025 | Nate Lee Andrew Bennett Ernie Riviere | Initial release of MITRE ACT templates and work aids. |

Purpose

This questionnaire provides a suggested *guide* for the Privacy Assessor to use when interviewing system personnel as part of an ACT Security Assessment. It contains a large set of interview questions that the M&O assessor *might* ask. Not all questions are required to be asked and/or answered, and each question might be presented to multiple system personnel in different roles. The M&O Assessor is free to deviate from this questionnaire in whatever manner they deem appropriate based on the specific context of the assessment and the interview.

Note that since many organizations are still transitioning from NIST SP 800-53 revision 4 to revision 5, this template maps questions to both the revision 5 controls and the revision 4 Appendix J privacy controls. The revision 4 Appendix J controls were deprecated, merged with or mapped to existing controls, and removed from 800-53 rev.5; if the organization has already transitioned to revision 5, the revision 4 control mappings can be removed from this document.

**Note to the Author Using this Template:**

This is a *template* for producing a MITRE ACT template tailored to your specific organization. Everything in this template can and should be customized by you to meet your organization’s specific needs and objectives.

Various objects and sections of text throughout the template are highlighted – these are **items that are very likely to require customization**, but you are free and encouraged to **edit the entire document and process** to suit your organization’s needs. By documenting your actual ACT process (including how it deviates from the baseline herein) in this template you are ensuring that your ACT assessments are consistent, repeatable, and can be accurately compared to assessments from other organizations’ implementations of ACT.

Interview Details

Table . Interview Logistics

|  |  |
| --- | --- |
| Date of Interview |  |
| Location of Interview |  |

Table . Interviewer(s)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Role | Name | Organization | Phone Number | Email Address |
| Interviewer |  | Assessment Team |  |  |

Table . Interview Participants

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Role | Name | Organization | Phone Number | Email Address |
| Assessment POC |  |  |  |  |
| Application Developer |  |  |  |  |
| Business Owner |  |  |  |  |
| Cloud Services Administrator |  |  |  |  |
| Configuration Manager |  |  |  |  |
| Contingency Planning Manager |  |  |  |  |
| Contracting Officer (COR) |  |  |  |  |
| Cyber Risk Advisor (CRA) |  |  |  |  |
| Database Administrator |  |  |  |  |
| Datacenter/Facilities Manager |  |  |  |  |
| Development Lead |  |  |  |  |
| Firewall Administrator |  |  |  |  |
| Human Resources Manager |  |  |  |  |
| Incident Handling Manager |  |  |  |  |
| Information System Security Officer (ISSO) / Manager (ISSM) |  |  |  |  |
| ISSO/ISSM - Contractor |  |  |  |  |
| Mainframe Administrator |  |  |  |  |
| Media Custodian |  |  |  |  |
| Middleware Utilities Administrator |  |  |  |  |
| Network Administrator |  |  |  |  |
| Privacy Subject Matter Expert (PSME) |  |  |  |  |
| Program Manager |  |  |  |  |
| Security Utilities Administrator |  |  |  |  |
| System Administrator |  |  |  |  |
| System Owner |  |  |  |  |
| Training Manager |  |  |  |  |
| Virtualization Administrator |  |  |  |  |

Topics Quick Reference

[1. Policy and Procedures 1](#_Toc198837942)

[2. Authority and Purpose 2](#_Toc198837943)

[3. Accountability, Audit, and Risk Management 4](#_Toc198837944)

[4. Data Quality and Integrity 8](#_Toc198837945)

[5. Data Minimization and Retention 9](#_Toc198837946)

[6. Individual Participation and Redress 11](#_Toc198837947)

[7. Security 14](#_Toc198837948)

[8. Transparency 15](#_Toc198837949)

[9. Use Limitation 17](#_Toc198837950)

# 

# Policy and Procedures

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rev 5 Control | Rev 4 Control | Question(s) | Guidance | Evidence Examples | Response |
| N/A | **N/A** | * Provide an overview of your roles and responsibilities related to application or system privacy, as well as the controls in place to secure it. Include all components for which you have a specific responsibility to ensure privacy in relation to the application or system. | * N/A | * N/A |  |
| All “-1” Controls | **All “-1” Controls** | * Describe the policies and procedures in place that support the organization’s Risk Management Framework (RMF) privacy requirements. * How are the policies and procedures disseminated to the staff? * How often do you receive information on updates? * If you had a question on how the privacy control should be implemented, what sources would you use to clarify the organization’s implementation? | *The Privacy Plan policies and procedures should address the overall privacy program within the organization. All staff should be familiar with the policies and be able to reference the location of the policy and procedures. This question should be asked of all interviewees (Privacy Program Official/Staff, ISSO).* | * N/A |  |
| N/A | **N/A** | * Has the system been designed to automate any privacy controls? * Have privacy requirements been integrated into the lifecycle? * Are periodic reviews of the system performed to ensure that compliance is maintained with the Privacy Act, organization privacy policy, and any other requirements? | *Automating privacy controls provides a concrete way of ensuring information systems are behaving in a way that is intended to achieve privacy objectives. Implementation of this control enables organizations to automate application of privacy controls.* | * system design documentation * database schema * access controls * SORN * PIA |  |

# Authority and Purpose

Ensures that the organization identifies the legal authority that determines a particular personally identifiable information (PII) collection or activity that impacts privacy and specifies in the privacy notices the purpose(s) for which PII is collected.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rev 5 Control | Rev 4 Control | Question(s) | Guidance | Evidence Examples | Response |
| PT-2 | **AP-1** | * Does the application or system collect, use, maintain, and/or share PII (to include PHI)? * Describe the legal authority that permits the collection, use, maintenance, and/or sharing of PII. * Is the authority to collect PII documented in the System of Records Notice (SORN), Privacy Impact Assessment (PIA), and/or other applicable documentation such as Privacy Act Statements, Notices of Privacy Practices, Website Privacy Policies, or Computer Matching Agreements? * Is the PII collected, used, maintained, or disseminated by the information system related to, and compatible with, the purpose and scope of the authority described in the information system documentation, such as a SORN or PIA. | *Before collecting PII, the organization determines whether the collection of PII is legally authorized. Program officials consult with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel regarding the authority of any program or activity to collect PII. The authority to collect PII is documented in the SORN and/or PIA or other applicable documentation such as Privacy Act Statements or Computer Matching Agreements (CMA).* | * SORN * PIA |  |
| PT-3 | **AP-2** | * Describe the purpose(s) for which PII is collected, used, maintained, and shared in the information system or application. * Are the purposes described in privacy compliance documentation, privacy notices, and privacy policies? | *Often, statutory language expressly authorizes specific collections and uses of PII. When statutory language is written broadly and thus subject to interpretation, organizations ensure, in consultation with the SAOP/CPO and legal counsel, that there is a close nexus between the general authorization and any specific collection of PII. Once the specific purposes have been identified, the purposes are clearly described in the related privacy compliance documentation, including but not limited to PIAs, SORNs, and Privacy Act Statements provided at the time of collection.* | * privacy notices |  |

# Accountability, Audit, and Risk Management

Ensures that effective controls for governance, monitoring, risk management, and assessment are implemented to demonstrate that the organization complies with applicable privacy protection requirements and minimizes overall privacy risk.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rev 5 Control | Rev 4 Control | Question(s) | Guidance | Evidence Examples | Response |
| PM-3 PM-18 PM-19 | **AR-1** | * Has a Senior Official for Privacy (SOP) been appointed? * Has an enterprise governance and privacy program been established? * Has part of the budget been allocated to implement the enterprise privacy program? * Has an enterprise privacy plan been developed? Please provide. * Have privacy policy and procedures been developed and promulgated to applicable organizational staff? Please provide. * How often are the privacy plan, policies, and procedures updated? | *The development and implementation of a comprehensive governance and privacy program demonstrates organizational accountability for and commitment to the protection of individual privacy. Accountability begins with the appointment of an SAOP/CPO with the authority, mission, resources, and responsibility to develop and implement a multifaceted privacy program.* | * organization governance * privacy plan / policy |  |
| RA-3 RA-8 | **AR-2** | * Has a privacy risk management process been documented and implemented? Describe. * Has a Privacy Impact Assessment (PIA) been performed? Please provide. * How often is the PIA reviewed? | *Effective implementation of privacy risk management processes requires both organizational and information system processes across the life cycle of the organization’s mission, business processes, and information systems. PIAs are structured reviews (qualitative and quantitative) of both the risk and effect of how information is handled and maintained as well as the potential impacts or harms to individuals and organizations for loss of control or mishandling of the PII.* | * organization privacy policy / procedures * PIA |  |
| SA-1 SA-4 SA-9 | **AR-3** | * Have privacy roles, responsibilities, and access requirements been established for contractors and service providers? * Have privacy requirements been included in contracts and other acquisition-related documents? * Is a random sample of agency contracts reviewed to ensure that the contracts include clauses that make all requirements of the Privacy Act apply to the system? How often? | *Contracts and other acquisition-related documents provide an enforceable means to ensure privacy and security controls are provided for PII shared with or disclosed to recipients outside of the organization, such that contractors and service providers protect PII in the same way the organization does.* | * organization privacy policy * acquisition documents |  |
| CA-2 | **AR-4** | * Are privacy controls monitored and audited to ensure effective implementation? How often? * Describe how changes to applicable privacy laws, regulations, and policy affecting internal privacy policy are monitored? How often are these monitored? * Describe how corrective actions identified through privacy monitoring or auditing are documented, tracked, and mitigated. | *To promote accountability, organizations identify and address gaps in privacy compliance, management, operational, and technical controls by conducting regular assessments (e.g., internal risk assessments). These assessments can be self-assessments or third-party audits that result in reports on compliance gaps identified in programs, projects, and information systems.* | * organization privacy policy * audit logs with PII * system design documentation |  |
| AT-1 AT-2 AT-3  PL-4 | **AR-5** | * Has a privacy training and awareness strategy been developed and implemented? * How often do general staff receive basic privacy training? How often do staff who have responsibility for PII receive more specific role-based training? * Are staff required to sign, either manually or electronically, privacy acceptable rules of behavior? Provide a sample. | *Privacy Training is an effective means to reduce privacy risk for an organization and is mandated by the Privacy Act of 1974, as amended, and OMB M-17-12. Through implementation of a privacy training and awareness strategy, the organization promotes a culture of privacy. Privacy training and awareness programs typically focus on broad topics, such as responsibilities under the Privacy Act of 1974 and E-Government Act of 2002 and the consequences of failing to carry out those responsibilities, how to identify new privacy risks, how to mitigate privacy risks, and how and when to report privacy incidents.* | * privacy and awareness training material * training records * privacy role-based training and compliance tracking mechanisms |  |
| PM-27 | **AR-6** | * Describe who provides privacy updates to oversight bodies, such as OMB and Congress. | *Privacy reporting helps organizations to determine progress in meeting privacy compliance requirements and to ensure organizational accountability. Through internal and external privacy reporting, organizations promote accountability and transparency in organizational privacy operations. Reporting also helps organizations determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the Federal Government, identify vulnerabilities and gaps in policy and implementation, and identify success models.* | * reports to OMB, Congress, and other oversight bodies, as appropriate * reports to senior management and personnel |  |
| N/A | **AR-7** | * Has the system been designed to automate any privacy controls? * Have privacy requirements been integrated into the lifecycle? * Are periodic reviews of the system performed to ensure that compliance is maintained with the Privacy Act, organization privacy policy, and any other requirements? | *Automating privacy controls provides a concrete way of ensuring information systems are behaving in a way that is intended to achieve privacy objectives. Implementation of this control enables organizations to automate application of privacy controls.* | * system design documentation * database schema * access controls * SORN * PIA |  |
| PM-21 | **AR-8** | * Describe how an accurate accounting of disclosures is maintained for the system of record. * How long is the accounting of disclosures retained? | *Both the Privacy Act and HIPAA require accountings of disclosures in certain circumstances. There are differences in the requirements to account for disclosures under the Privacy Act and under HIPAA. The Senior Official for Privacy (SOP), periodically consults with managers of their organization’s systems of records to ensure that the required accountings of disclosures of records are being properly maintained and provided to persons named in those records consistent with the dictates of the Privacy Act. Organizations are not required to keep an accounting of disclosures when the disclosures are made to individuals with a need to know, are made pursuant to the Freedom of Information Act, or are made to a law enforcement agency.* | * records documenting the disclosures of information held in the system of records under its control * retention policy for the disclosure records |  |

# Data Quality and Integrity

Ensures that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rev 5 Control | Rev 4 Control | Question(s) | Guidance | Evidence Examples | Response |
| PM-22 | **DI-1** | * Describe how the accuracy, relevance, timeliness, and completeness of PII information is confirmed upon collection or creation of the PII. * Is PII collected directly from the individual to the greatest extent practicable? Describe. * Describe how inaccurate or outdated PII used by the application or system is identified and corrected. How often does this occur? | *When a record is used to make determinations related to a right, benefit, or privilege for an individual, the Privacy Act of 1974, as amended, requires the information used to be accurate, relevant, timely, and complete to assure fairness to the individual in the determination. Agencies should ensure the quality of all PII, even if it is not protected by the Privacy Act. Organization’s data quality assurance processes should be commensurate with the impact to an individual’s rights, benefits, or privileges as determined by the system owner in consultation with the organization’s privacy office.* | * organization privacy policy / procedures |  |
| PM-24 SI-1 | **DI-2** | * Have processes been documented to ensure the integrity of PII through existing security controls? * Has a Data Integrity Board (DIB) been established, when appropriate, to oversee organizational computer matching agreements? | *Organizations conducting or participating in CMAs with other organizations, regarding applicants for and recipients of financial assistance or payments under federal benefit programs, or regarding certain computerized comparisons involving federal personnel or payroll records, establish a Data Integrity Board to oversee and coordinate their implementation of such matching agreements.* | * organization privacy policy / procedures * SSP |  |

# Data Minimization and Retention

Ensures that the data minimization and retention requirements implemented to collect, use, and retain PII are relevant and necessary for the purpose for which it was originally collected.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rev 5 Control | Rev 4 Control | Question(s) | Guidance | Evidence Examples | Response |
| SA-8(33) PM-5(1) | **DM-1** | * Have the minimum PII elements that are relevant and necessary to accomplish the purpose of collection been identified? * Is the collection and retention of PII limited to the minimum elements identified in privacy notices? * How often are system PII holdings reviewed to ensure that only PII identified in the privacy notices is collected and retained? | *Coordinating review of the organization’s holdings of PII with existing system review processes maximizes the efficient use of organization resources and will ensure all PII retained, even if the PII is not maintained in a Privacy Act system of records, is relevant and accurate. Reducing PII to the minimum required to accomplish the legally authorized purpose of collection and retaining PII for the minimum necessary period of time reduces the risk of PII breaches and will reduce the risk of the organization making decisions based on inaccurate PII.* | * organization privacy policy / procedures * PII holdings or inventory |  |
| MP-6 SI-12 SI-12(3) | **DM-2** | * Is each collection of PII retained for the time period specified by the NARA-approved records schedule? * Describe how the organization disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA approved record retention schedule. * Are FIPS-validated techniques or methods used to ensure secure deletion or destruction of PII? | *Both the Privacy Act and the Federal Records Act require records to be maintained and disposed of in accordance with a published Records Schedule. Disposal and destruction of PII must be done securely so that it may not be reconstructed. NARA provides retention schedules that govern the disposition of federal records. Program officials and business owners coordinate with records officers, Cyber Risk Advisors, and with NARA to identify appropriate retention periods and disposal methods. NARA may require organizations to retain PII longer than is operationally needed. In those situations, organizations describe such requirements in the notice.* | * data retention policy/procedures * data disposal policy / procedures * backup policy / procedures * system design documentation |  |
| PM-25 SI-12(2) | **DM-3** | * Have policies and procedures been established that minimize the use of PII for testing, training, and research? * Have controls been implemented to protect PII used for testing, training, and research? Describe. | *When developing and testing information systems, PII is at a heightened risk for accidental loss, theft, or compromise. Therefore, the organization needs to take measures to reduce that risk. If PII must be used, organizations take measures to minimize any associated risks and to authorize the use of and limit the amount of PII for these purposes. Organizations consult with the Senior Official for Privacy (SOP) and legal counsel to ensure that the use of PII in testing, training, and research is compatible with the original purpose for which it was collected. When PII is of a sufficiently sensitive nature, to the greatest extent possible, PII should not be used when testing or developing an information system.* | * organization privacy policy |  |

# Individual Participation and Redress

Ensures that individuals can be active participants in the decision-making process regarding the collection and use of their PII, by providing individuals with access to PII and the ability to have their PII corrected or amended.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rev 5 Control | Rev 4 Control | Question(s) | Guidance | Evidence Examples | Response |
| PT-4 | **IP-1** | * Are individuals able to authorize the collection, use, maintenance, and sharing of PII prior to its collection? * Does the organization provide a means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII? * Is consent obtained from individuals prior to any new uses or disclosure of previously collected PII? * Are individuals aware of and consent to all uses of PII not initially described in the public notice? | *Individual participation and agreement to provide information is fundamental to an individual making an informed decision regarding the collection, use, and safeguarding of their PII.*  *Consent is fundamental to the participation of individuals in the decision-making process regarding the collection and use of their PII and the use of technologies that may increase risk to personal privacy. To obtain consent, organizations provide individuals appropriate notice of the purposes of the PII collection or technology use and a means for individuals to consent to the activity. Organizations tailor the public notice and consent mechanisms to meet operational needs. Organizations achieve awareness and consent, for example, through updated public notices.* | * organization privacy policy / procedures * application / system PII input screen |  |
| AC-1 AC-3(14) PM-20 PT-5 PT-6 | **IP-2** | * Can individuals access their PII maintained in the application/system? * Does the organization publish rules and regulations governing how individuals may request access to records that are maintained in the application/system? * Are access procedures published in a system of records notice (SORN)? * Describe how the organization adheres to Privacy Act requirements and OMB policies and guidance regarding Privacy Act requests. | *The Individual Participation Fair Information Practice Principles (FIPP) requires organizations to provide mechanisms for individuals to gain access to their PII when appropriate. The Privacy Act of 1974, as amended, requires organizations to provide mechanisms for individuals to gain access to their PII when that PII meets the definition of a “record.” Access is also an important aspect of supporting correction of PII and redress against alleged violations and misuse of their PII.* | * organization privacy policy / procedures * SORN |  |
| PM-22 SI-18 SI-18(4) SI-18(5) | **IP-3** | * Describe the process that enables individuals to have inaccurate, incomplete, or obsolete PII maintained by the organization corrected or amended. * Has this process been disseminated to external information sharing partners, if applicable? * Is there an established process that notifies affected individuals that their information has been corrected or amended? | *Redress supports data integrity requirements for PII by providing a process for individuals to request correction of, or amendment to, their PII maintained by the organization. Redress supports the ability of individuals to ensure the accuracy of PII held by the organization. Effective redress processes demonstrate organizational commitment to data quality especially in those business functions where inaccurate data may result in inappropriate decisions or denial of benefits and services to individuals. Organizations use discretion in determining if records are to be corrected or amended, based on the scope of redress requests, the changes sought, and the impact of the changes.* | * organization privacy policy / procedures |  |
| PM-26 | **IP-4** | * Has a process been established for receiving and responding to complaints, concerns, or questions from individuals about organizational privacy practices? | *Establishing a complaint management process ensures complaints are addressed in a timely manner and provides an avenue for individuals to participate in government activities that may impact privacy. Information received from complaints provides external input regarding organizational privacy and security practices which may improve processes and systems involved in collection, use, and maintenance of PII.* | * organization privacy procedures * sample inquiries and complaints |  |

# Security

The SE privacy controls supplement the security controls to ensure that technical, physical, and administrative safeguards are in place to protect PII collected or maintained by the organization against loss, unauthorized access, or disclosure, and to ensure that planning and responses to privacy incidents comply with OMB policies and guidance.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rev 5 Control | Rev 4 Control | Question(s) | Guidance | Evidence Examples | Response |
| PM-5(1) | **SE-1** | * Is there an inventory that identifies organizational information systems that collect, use, maintain, or share PII? How often is the inventory updated? * Is the inventory shared with the Senior Officer/Official for Privacy? How often? | *The PII inventory identifies the organization’s information assets and identifies those assets collecting, using, maintaining, or sharing PII. The PII inventory identifies those assets most likely to impact privacy; provides a starting point for organizations to implement effective administrative, technical, and physical security policies and procedures to protect PII; and to mitigate risks of PII exposure. The PII inventory enables organizations to identify systems and programs that contain PII so that they can then identify and address privacy risks.* | * inventory of systems that collect/maintain PII |  |
| IR-8 IR-8(1) | **SE-2** | * Has a privacy incident and breach response plan been developed and implemented for the application/system? Please provide. * Are privacy incidents and breaches responded to in accordance the organization’s Privacy Incident and Breach Response Plans? | *In contrast to the Incident Response (IR) family, which concerns a broader range of incidents affecting information security, this control uses the term Privacy Incident to describe only those incidents that relate to PII.* | * privacy incident response procedures * privacy incident response procedures |  |

# Transparency

Ensures that the organization provides public notice of the information practices and the privacy impact of programs and activities.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rev 5 Control | Rev 4 Control | Question(s) | Guidance | Evidence Examples | Response |
| PT-5 PT-5(1) | **TR-1** | * How does the organization provide effective notice to the public/individuals regarding activities that impact privacy, the authority for collecting PII, choices individuals have regarding how PII is used, and the ability to access and have PII amended or corrected? * Describe the following: the PII the organization collects and the purpose(s) of the collection; how the organization uses PII internally; any sharing of PII with external entities and the purposes for such sharing; whether individuals can consent to specific uses or sharing of PII and how to exercise such consent; how individuals obtain access to PII; how PII is protected. * Describe how the organization revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy. | *Providing the appropriate notification of privacy practices to the individual enables the individual to make an informed decision when they provide their consent. Effective notice, by virtue of its clarity, readability, and comprehensiveness, enables individuals to understand how an organization uses PII generally and, where appropriate, to make an informed decision prior to providing PII to an organization. Effective notice also demonstrates the privacy considerations that the organization has addressed in implementing its information practices. The organization may provide public notice through a variety of means. Some of these may be required by law or regulations, such as SORNs for Privacy Act systems, PIAs for agency information systems and electronic collections of information, and website privacy policies for agency websites.* | * public notice regarding individual privacy |  |
| PT-5(2) PT-6 | **TR-2** | * Have any SORNs been published for the application/system? * How often are SORNs updated? * Are Privacy Act statements included on organizational forms that collect PII? | *Organizations issue SORNs to provide the public notice regarding PII collected in a system of records. SORNs explain how the information is used, retained, and may be corrected, and whether certain portions of the system are subject to Privacy Act exemptions for law enforcement or national security reasons.* | * SORN |  |
| PM-20 | **TR-3** | * Does the public have access to information about organizational privacy activities? * How can the public communicate with the Senior Official for Privacy/Privacy Office? * Have privacy practices been published through the system/application? Are they publicly available? | *Making information about an organization’s privacy program readily available to the public reduces the burden on individuals wanting to better understand an organization’s privacy practices. It also reduces the burden on privacy offices and program officials by providing answers to common privacy questions through an easily accessible forum.* | * publicly available privacy policies |  |

# Use Limitation

Ensures that the organization uses PII either as specified in the public notice, in a manner compatible with those specified purposes, or as otherwise permitted by law

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rev 5 Control | Rev 4 Control | Question(s) | Guidance | Evidence Examples | Response |
| PT-3 | **UL-1** | * Describe how the organization uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in the public notice. | *Organizations take steps to ensure that they use PII only for legally authorized purposes and in a manner compatible with uses identified in the Privacy Act and/or in public notices. These steps include monitoring and auditing organizational use of PII and training organizational personnel on the authorized uses of PII. With guidance from the Senior Official for Privacy (SOP) and where appropriate, legal counsel, the organization documents processes and procedures for evaluating any proposed new uses of PII to assess whether they fall within the scope of the organizational authorities.* | * privacy policy * privacy notices * SORN |  |
| AC-21 AT-3(5) AU-2 PT-2 PT-3 |  | * Are there any third-party MOUs, MOAs, Letters of Intent, CMAs, or similar agreements? Please provide. * If PII is shared externally, is it only for the authorized purposes identified in the Privacy Act and/or described in privacy notices? * Describe how the organization monitors, audits, and trains staff on the authorized sharing of PII with third parties, if applicable. | *Sharing PII with third parties introduces new risks to the individual which, as applicable, requires the organization to establish formal agreements with the third party and to ensure the sharing is compatible with the purposes described in any notice to, and consent from, the individual. Consideration of privacy risks for sharing PII apply regardless of the method used or whether the information remains stored in the system of records.* | * privacy policy * privacy practices * any MOUs, MOAs, Letters of Intent, CMAs, or similar agreements with third parties |  |