UNITED STATES
DEPARTMENT OF THE TREASURY

U.S. Department of the Treasury
1750 Pennsylvania Avenue, NW
Washington, DC 20220

Appendix C: Departmental Offices Privacy, Transparency, and Records, National Institute of Standards and Technology Special Publication 800-53 Revision 4 and Revision 5, Appendix J Treasury Privacy Control Compliance Chart

Version: 2.0
Date: 30 April 2020

Appendix J

Draft, Treasury Compliance with National Institute of Standards and Technology Special Publication 800-53 Revision 4 and Revision 5 Privacy Control Compliance Chart

Acronyms and abbreviations

API	Application Programming Interfaces
ASM	Assistant Secretary for Management
ATO	Authority to Operate
CMA	Computer Matching Agreement
CPCLO	Chief Privacy and Civil Liberties Officer
CPO	Chief Privacy Officer
DASPTR	Deputy Assistant Secretary Privacy, Transparency, and Records
DHS	Department of Homeland Security
DIB	Data Integrity Board
DO	Departmental Offices

EO	Executive Order
FISMA	Federal Information Security Management Act of 2002
FOIA	Freedom of Information Act
FR	Federal Register
GAO	Government Accountability Office
GRS	General Records Schedule
ISE	Information Sharing Environment
IT	Information Technology
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
No.	Number
OCIO	Office of the Chief Information Office
OCRCL	Office for Civil Rights and Civil Liberties
OIG	Office of Inspector General
OLA	Office of Legislative Affairs
OMB	Office of Management and Budget
OPE	Office of the Procurement Executive
PA	Privacy Act
PAS	Privacy Act Statement
PCLTA	Privacy and Civil Liberties Threshold Analysis
PCLIA	Privacy and Civil Liberties Impact Assessment

PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PRA	Paperwork Reduction Act
PTR	Privacy, Transparency, and Records
Rev.	Revision
SA&A	Security Assessment & Authorization
SAOP	Senior Agency Official for Privacy
SOR	System of Records
SORN	System of Records Notice
SPP	Security Program Plan
SP	Special Publication
SRS	Specific Records Schedule
TFIMS	Treasury FISMA Information Management System
TRB	Technical Review Board

A copy of NIST SP 800-53 Rev. 4, dated April 2013 with updates as of January 2015 can be found here: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

A copy of NIST SP 800-53 Rev.5 draft, dated August 2017 can be found here: https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

This appendix provides a structured set of controls for protecting privacy and serves as a roadmap for Treasury to use in identifying and implementing privacy controls for the entire life cycle of PII, whether in paper or electronic form.

The following chart contains the privacy control number and title, the control's status, and a summary of how Treasury meets that control's requirements. The Office of Privacy, Transparency, & Records aligned these requirements with the Departmental Offices

Information Technology Security Program Plan (DO IT SPP), and annotated them with an asterisk (*) when the DO IT SPP meets the control's requirements. The term "maintenance" when used in the chart collectively refers to the collection, use, maintenance, and sharing of personally identifiable information (PII). Treasury is issuing this Privacy Program Plan while NIST 800-53 (revision 4) is still effective, but NIST 800-53 (revision 5) is in draft and under review. Therefore, a column is added for each privacy control to reflect the corresponding proposed revision 5 section for each control.

The Senior Agency Official for Privacy (SAOP) is responsible for implementing privacy compliance requirements at the Department of the Treasury. Treasury established a Departmental Privacy and Civil Liberties (PCL) team within its Office of Privacy, Transparency, and Records (PTR). PTR is led by the Deputy Assistant Secretary for PTR (DASPTR), who reports directly to the SAOP (who is also the Assistant Secretary for Management and the Treasury Chief Privacy and Civil Liberties Officer). PTR also maintains a team led by the Director for Privacy and Civil Liberties (PCL Director). The PCL Director acts as the Bureau Privacy and Civil Liberties Officer (BPCLO) for Treasury's Departmental Offices (DO) as well as Department-wide responsibilities.

In addition to the support that PTR provides for DO and Department-wide, the SAOP also enlists the support of staff that perform privacy functions at the Treasury bureau level. This includes bureau level privacy programs led by BPCLOs and others. In the chart below, all references to actions taken by the SAOP include actions performed by Treasury departmental and bureau privacy programs, bureau heads, the Office of General Counsel, Chief Information Officers, and system/program officials. These partners are collectively referred to as "Treasury privacy stakeholders" in the chart below. The specific role played by each of these stakeholders is described in more detail in the main text of this document.

Control No. and Title	Appendix J Control	Status	How Treasury Meets the Privacy Control	Rev. 5 Control No. and Title
AP-1, Authority to Collect	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.	Implemented	Before maintaining PII in a Treasury information system or paper file, Treasury privacy stakeholders determine whether the collection is legally authorized and consult with legal counsel, as necessary, regarding the authority of any program or activity that collects PII. The authority to collect PII is recorded in the following Treasury privacy documents: • SORNs • PCLIAs • PASs, and • CMAs	PA-2 Authority To Collect
AP-2, Purpose Specification	The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.	Implemented	Treasury privacy stakeholders review all laws and policies a program or system owner provides in support of maintaining a specific program or information system to ensure a reasonable nexus exists between any general authorization and the collection and use of specific PII. After the specific purposes are identified, they are clearly described in the related privacy compliance documentation, including published PCLIAs, CMAs, and SORNs, as well as PASs provided at the time of collection (for example, on forms organizations use to collect PII that will be maintained in a system of records). For certain information required to perform Treasury's mission, collection, use, maintenance, and sharing restrictions are described in law, regulation (for example, taxpayer information) or written agreement (for example, Terrorist Finance Tracking Program).	PA-3 Purpose Specification

AR-1, Governance and Privacy Program	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*].	Implemented *	As the Treasury-appointed SAOP, the ASM oversees all aspects of the privacy program, but enlists the support of Treasury privacy stakeholders who have the expertise necessary to navigate privacy issues that implicate unique bureau or program issues, authorities, and missions. The SAOP has Treasury-wide authority, resources, and responsibility to develop, implement, share, and maintain a complete governance and privacy program. Treasury privacy stakeholders work with legal counsel, cybersecurity officials, and others as needed to respond to particular issues by: • Ensuring the development, implementation, and enforcement of privacy policies and procedures • Defining roles and responsibilities for protecting PII • Determining the level of information sensitivity with regard to PII holdings • Identifying the laws, regulations, and internal policies that apply to the collection, use, maintenance, sharing, and disposal of PII • Monitoring privacy best practices, and • Monitoring compliance with identified privacy controls.	PM-19 Privacy Program Roles

AR-2, Privacy Impact and Risk Assessment	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 (and Civil Liberties) 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.	Implemented	Treasury privacy stakeholders use OMB Memorandum 03-22, *Privacy Impact Assessments*, to implement the privacy provisions of the E-Government Act of 2002. Treasury uses PCLIAs to: • Identify privacy risks and methods to minimize those risks • Ensure that programs or information systems meet legal, regulatory, and policy requirements, and • Tell the public how Treasury protects PII when it is collected, shared, stored, transmitted, and used. PCLIAs are performed before developing or procuring information systems, or initiating programs or projects, that collect, use, store, transmit, dispose, maintain, or share PII. PCLIAs are updated when system or process changes create new privacy risks. Treasury's PCLIA templates also address potential civil liberties issues that may result from the maintenance of PII (for example, due process, redress, and First Amendment issues).	RA-8 Privacy Impact Assessments RA-3 Risk Assessment
AR-3, Privacy Requirements for Contractors and Service Providers	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.	Implemented	Contractors and service providers who have access to Treasury systems and data are held to the same standards as Treasury employees. Treasury privacy stakeholders work with Treasury's Office of the Procurement Executive (OPE) to ensure that appropriate provisions are added to contracts where contractors will have access to Treasury PII. Contractors and service providers are contractually obligated to comply with all applicable privacy and related records management laws and policies. Treasury privacy stakeholders consult with legal counsel, the CIOs, and contracting officers regarding applicable laws, directives, policies, or regulations that may affect implementation of this control.	SA-9 EXTERNAL SYSTEM SERVICES

AR-4, Privacy Monitoring and Auditing	The organization monitors and audits privacy controls and internal privacy policy to ensure effective implementation.	Implemented	Treasury privacy stakeholders conduct regular assessments to promote accountability and address gaps in privacy compliance and controls by: • Conducting assessments of Treasury privacy policies and requirements to ensure they are current and effective • Monitoring legal, regulatory and policy developments to ensure that Treasury privacy policies continue to comply with applicable legal and OMB policy requirements • Using automated auditing tools to ensure appropriate use of PII by all system users, and • Ensuring that corrective actions, identified as part of the assessment process, are tracked and monitored until audit findings are corrected. Treasury privacy stakeholders coordinate monitoring and auditing efforts with information security officials to ensure that results are provided to senior managers and oversight officials.	CA-1 Assessment, Authorization, and Monitoring Policy and Procedures

AR-5, Privacy Awareness and Training	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*].	Implemented	Treasury promotes a culture of privacy through its Annual Privacy Awareness training. All Treasury employees and contractors must complete initial privacy training within 30 days of their appointment and are required to take refresher training annually. At least quarterly, all Treasury employees and contractors receive emails to remind them of the annual refresher requirement. All training is completed electronically and tracked on Treasury's Integrated Talent Management System (or other bureau systems). By completing privacy training, employees and contractors accept responsibility for complying with basic privacy requirements. Privacy training targets program or information system data collection and use requirements identified in public notices, such as PCLIAs, SORNs or CMAs. Training methods include: • Mandatory annual privacy awareness training • Targeted, role-based training to address issues unique to bureau or office missions and the PII they collect, and • Internal guides and handbooks that address particular privacy issues (e.g., the Treasury Privacy Act Handbook). Treasury regularly updates training materials based on changing statutory, regulatory, mission, program, business process, and information system requirements, or on the results of compliance monitoring and auditing.	AT-2 Awareness Training

AR-6, Privacy Reporting	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.	Implemented	Treasury privacy stakeholders consult with legal counsel and Treasury's Office of Legislative Affairs (OLA), where appropriate, to ensure that Treasury meets all applicable privacy reporting requirements. Treasury reporting requirements are found in the following legal and OMB requirements: • Annual SAOP Report under the FISMA • Semiannual report required under Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007 • Biennial report on Computer Matching and Privacy Protection Act Pursuant to the Privacy Act, as amended • Annual Privacy Report under Section 522 of the Consolidated Appropriations Act of 2005 • Data Mining report under the Federal Agency Data Mining Reporting Act of 2007 • Immediate reporting of "major incidents" to DHS US-CERT per OMB M-17-12 and FISMA 2015 • PCL Assessment Report under Section 5(b) of EO 13636, and • Other periodic reports as requested by the General Accountability Office (GAO).	PM-30 Privacy Reporting

AR-7, Privacy-Enhanced System Design and Development	The organization designs information systems to support privacy by automating privacy controls.	Implemented	Treasury builds privacy controls into new system design and development to minimize privacy risks, reduce the likelihood of breaches, and prevent other privacy-related incidents. Departmental Treasury privacy stakeholders are members of the OCIO Technical Review Board (TRB), which approves IT initiatives prior to their submission to the DO Information Technology Investment Review Board (DO IRB). The TRB provides technology leadership to ensure that IT initiative decisions align with the technical approach Treasury has approved for the development of DO information systems. Other privacy stakeholders participate in similar approval processes at the bureau level. TRB and other technical review board participation at the bureau level allows Treasury privacy stakeholders to ensure privacy concerns are addressed at the earliest stage of each system's life cycle. Additionally, Treasury PCLIAs include questions about pre and post-information system development technical solutions that might be available to ensure the accuracy, completeness, and timeliness of PII maintained in systems.	SA-3 System Development Life Cycle

AR-8, Accounting of Disclosures	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.	Implemented	Treasury privacy stakeholders use the PCLIA template to ensure that system of records managers are properly maintaining accountings of disclosures or can timely and accurately reconstruct a complete accounting of disclosures. Treasury is not required to keep an accounting of disclosures when the disclosures are made: • Within Treasury to personnel with a *need-to-know* • Under the FOIA, or • To a law enforcement agency under 5 U.S.C. § 552a(c)(3) In spite of the FOIA exclusion from the Privacy Act accounting requirement, FOIA disclosures and law enforcement disclosures are logged and available for review to the extent required by law at individual Treasury Offices that fulfill such requests. Treasury also reviews all systems of records to determine whether certain systems of records should be exempt from the requirement to provide the accounting of disclosures to individuals. Where appropriate, Treasury privacy stakeholders complete all OMB and regulatory processes necessary to establish required exemptions.	

DI-1, Data Quality	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.	Implemented	Treasury takes measures to protect data quality and validate the accuracy of PII that is used to make decisions about the rights, benefits, or privileges of individuals under federal programs. The Treasury PCLIA template includes a series of questions addressing the need to collect PII directly from the individual unless a particular system of records is exempted from this requirement. Treasury privacy stakeholders are involved in analyzing system requirements at the earliest stage of system development. This allows them to identify: • Untrustworthy PII sources, and • When additional management controls are required to allow individuals to verify their information before it is used to make decisions about their rights, benefits or privileges. Treasury PCLIAs also address this control by inquiring about technical solutions available to ensure the accuracy, completeness, and timeliness of PII maintained in systems of records. Treasury privacy stakeholders use the PCLIA responses to ensure the system provides mechanisms that allow editing and validation of PII collected and entered into information systems. These mechanisms may include, for example, Application Programming Interfaces (API) for automated address verification.	PM-23 Data Quality Management Or SI-19 Data Quality Operations

DI-2, Data Integrity and Data Integrity Board	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 Agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.	Implemented	Treasury's PCLIA process addresses data integrity by ensuring PII is: • Collected directly from individuals; • Not altered during storage, processing, or while in transit, and • Properly safeguarded as required during the Security Assessment & Authorization (SA&A) process before authority to operate (ATO) is granted to a federal information system. The PCLIA template also addresses Computer Matching Privacy Protection Act requirements when records maintained in systems of records are matched with certain data collections for the purpose of determining or affecting an individual's rights, benefits, and privileges. The DASPTR leads Treasury's DIB, which oversees and coordinates CMA approval. The DIB ensures that existing controls comply with Privacy Act computer matching requirements to maintain the integrity of data shared under each Computer Matching Agreement.	PM-25 Data Integrity Board

DM-1, Minimization of Personally Identifiable Information	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.	Implemented	Treasury privacy stakeholders work with system owners to identify the minimum PII elements information systems or programs require to accomplish a legally authorized purpose. Treasury's PCLIA process ensures that the amount and type of PII collected is minimized. The PCLIA requires system owners to identify what they deem to be relevant, necessary, and legal to collect. Treasury privacy stakeholders then work with system owners to eliminate any PII that falls outside of these requirements. Continuous monitoring requirements also allow Treasury privacy stakeholders to use the PCLIA process to ensure that data minimization analysis is conducted for any proposed modifications that include additional PII collection in a particular information system. Continuous monitoring requirements also allow privacy stakeholders to continuously reassess the continuing necessity and relevance of the PII originally maintained in the system. This includes analyzing existing PII holdings to determine if PII in aging systems is still relevant, necessary, and legal to remain compliant with the Privacy Act and Paperwork Reduction Act requirements. Treasury privacy stakeholders coordinate with Treasury federal records officers to ensure that any plan to reduce a system's PII holdings is achieved in compliance with applicable NARA retention schedules.	PM-26 Minimization of Personally Identifiable Information Used in Testing, Training, and Research

DM-2, Data Retention and Disposal	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).	Implemented	Treasury privacy stakeholders coordinate with Treasury's federal records officers to identify appropriate retention periods and disposal methods. Treasury addresses mission specific exceptions from NARA retention and disposal requirements in public notices (for example, an updated SORN) to maintain transparency. If NARA's General Records Schedules (GRS) or existing Treasury's Records Schedules (TRS) do not cover the particular records maintained in an information system, Treasury privacy stakeholders document in the PCLIA efforts to draft and secure NARA approval for a new Treasury Records Schedule.	SI-12 Information Management and Retention
DM-3, Minimization of PII Used in Testing, Training, and Research	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.	Implemented	Treasury privacy stakeholders analyze testing, training, and research efforts to ensure that live data is not used (if feasible) and to minimize the collection and use of PII to that which is necessary to conduct the particular testing, training, or research effort. For example, PII used in data entry training does not require actual PII; therefore, randomly generated information is a suitable alternative. Additional controls include scrutinizing contracts where the disclosure of PII to contractors is necessary to ensure the minimization of the data and its return or destruction upon completion of testing or research.	PM-26 Minimization of Personally Identifiable Information Used in Testing, Training, and Research

IP-1, Consent	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.	Implemented	Treasury privacy stakeholders tailor the public notice and methods for obtaining consent to ensure consistency with Privacy Act requirements. Public notices such as SORs, PCLIAs, CMAs, and Privacy Act Statements (PAS) tell the public what information is collected, why it is collected and to whom it is disclosed outside Treasury so they can determine if they want to provide the PII requested. These notice processes allow individuals to make informed decisions: • At the point of collection where Treasury provides a PAS (on paper forms, digitally, or through spoken word) identifying the authority for the collection, consequences for failing to provide PII, and whether the request for is mandatory or voluntary • If Treasury requests authorization to disclose PII for a certain purpose not expressly authorized in the Privacy Act, and/or • When Treasury makes requests for additional information to supplement a previous collection. All of these notices provide 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.	IP-2 Consent

IP-2, Individual Access	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.	Implemented	Treasury maintains Privacy Act compliant regulations at 31 CFR, Subpart C, which allow individuals to access their records maintained in Treasury system(s) of records. These regulations govern all requests individuals submit for access to their records that are maintained in a Treasury system of records. Treasury privacy stakeholders, in consultation with Treasury FOIA officers (processes and stakeholders vary by bureau), are responsible for processing Privacy Act requests in compliance with the regulations. Each Treasury SORN lists the official who is responsible for the SOR and provides procedures for requesting access. Privacy Act and FOIA points of contact are also posted on Treasury's public websites. The SORN describes how individuals are notified and can access their records if the SOR contains a record about them. Individuals who wish to determine if their records are maintained in a particular SOR are invited to make a written inquiry to the Disclosure Officer of the appropriate bureau as stated in Treasury SORNs under "Record Access Procedures." Whenever possible, Treasury allows individuals to review their PII held within a Treasury system of records. Treasury facilitates timely, simplified, and inexpensive access by placing FOIA offices across the organization. This allows requests to be directed to the organization's FOIA office nearest to the information. This practice reduces time and resources required to answer an individual's request. Access requests may be denied where SORs were properly exempted from the access requirements in accordance with Privacy Act requirements.	IP-6 Individual Access

IP-3, Redress	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.	Implemented	Treasury maintains Privacy Act compliant regulations at 31 CFR, Subpart C, which allow individuals to access their records maintained in Treasury system(s) of records and seek correction or amendment where appropriate. Treasury provides effective redress by: • Providing notice of the existence of a PII collection (for example, in SORNs or PCLIAs) • Providing plain language explanations of the processes and mechanisms for requesting access to records in SORNs • Establishing criteria for submitting requests for correction and publishing them in the Federal Register (FR) with a link to the FR on Treasury's public web site • Assigning resources to analyze and adjudicate requests in Treasury's FOIA and Privacy offices • Implementing means of correcting data collections if FOIA/Privacy offices validate the allegation of inaccuracy presented in a request for amendment of the individual's records • Reviewing all decisions that may have been the result of inaccurate information, and • Notifying individuals and organizations about a correction or amendment where appropriate.	IP-3 Redress
IP-4, Complaint Management	The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.	Implemented	The public can readily access information regarding Treasury complaint processes through the Treasury website and 31 CFR Subpart C, which provides the details needed to file complaints. It also includes contact information for the SAOP or other officials designated to receive complaints. Treasury's complaint management process includes tracking mechanisms implemented by the receiving organization (for example, Inspectors General) to ensure that complaints are reviewed and addressed in a timely manner.	PM-28 Complaint Management

SE-1 Inventory of Personally Identifiable Information	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.	Implemented *****	Information systems that maintain PII are identified during Privacy and Civil Liberties Threshold Assessments (PCLTA), PCLIAs, and information system authorization processes. All systems that maintain PII are documented in the Treasury inventory maintained in the Treasury FISMA Information Management System (TFIMS).	PM-29 Inventory of Personally Identifiable Information

SE-2, Privacy Incident Response	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.	Implemented *	The Treasury Departmental Privacy Incident Response Plan, developed by the CIO, in consultation with Treasury privacy stakeholders, includes: • Procedures for responding to Treasury cybersecurity incidents • Establishment of a cross-functional Privacy Incident Response Team that reviews, approves, and participates in the execution of the Privacy Incident Response Plan • A process for determining whether notice to oversight organizations or affected individuals is appropriate • A privacy risk assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and, where appropriate, to take steps to minimize any such risks • Internal procedures to ensure employees and contractors promptly report any privacy incident to Treasury cybersecurity officials an privacy stakeholders, consistent with organizational incident management structures, and • Internal procedures for reporting noncompliance with Treasury or bureau privacy policies to appropriate management or oversight officials. In addition, the SAOP must report to Congress when a “major” breach occurs as defined in the FISMA 2015 legislation.	IR-4 Incident Handling IR-7 Incident Response Assistance

TR-1, Privacy Notice	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.	Implemented	The SAOP, in consultation with legal counsel, system/program managers, and relevant Treasury privacy stakeholders, is responsible for the content of the Treasury's public notices. Treasury is in compliance with the public notice provisions of the Privacy Act, the E-Government Act's PIA requirement, OMB guidance related to federal agency privacy notices, and, where applicable, with policy pertaining to participation in the Information Sharing Environment (ISE). Note that Treasury refers to its PIAs as PCLIAs to account for the ASM/CPCLO's civil liberties responsibilities as required by law. Treasury provides general public notice through a variety of means, as required by law or policy, including SORNs, PCLIAs, CMAs, and PASs.	IP-4 Privacy Notice

TR-2, System of Records Notices and Privacy Act Statements	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.	Implemented	Treasury publishes SORNs to provide the public notice about records collected in a system of records, as defined by the PA. SORNs explain how the information is used, retained, and may be corrected, and whether certain portions of the system are subject to PA exemptions for law enforcement or national security reasons. Treasury PASs provide notice of: • Authority of organizations to collect PII • Whether providing PII is mandatory or optional • Principal purposes for which the PII is to be used • Intended disclosures (routine uses) of the information • Consequences for not providing all or some portion of the information requested Treasury employees or contractors provide a verbal PAS before collecting PII over the phone or through other oral communications.	PM-20 System of Records Notice IP-5 Privacy Act Statements

TR-3, Dissemination of Privacy Program Information	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.	Implemented	Treasury's PA page is on www.treasury.gov/privacy. It provides the public with access to PCLIAs, SORNs, and reports published by Treasury. The Privacy Act page also contains points of contact for privacy questions. Treasury uses PCLIAs, SORNs, privacy reports, and publicly available web pages to inform the public about its privacy practices. Treasury also provides access on its web pages to email addresses, phone lines, comment forms, Facebook, and Twitter feeds to allow the public to provide feedback or direct questions to privacy offices about privacy practices.	PM-21 Dissemination of Privacy Program Information
UL-1, Internal Use	The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.	Implemented	Treasury privacy stakeholders ensure that PII is only used for legally authorized purposes and only in a manner compatible with uses identified in the PA and in public notices. Treasury monitors and audits organization's use of PII and ensures that personnel are trained on the authorized uses of PII. Treasury privacy stakeholders also ensure that PII shared internally is required to achieve a Treasury mission function.	PA-3 (1) Purpose Specification | Usage Restrictions of Personally Identifiable Information

UL-2, Information Sharing with Third Parties	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.	Implemented	Treasury privacy stakeholders approve any proposed external sharing of PII, including with other public, international, or private sector entities, for consistency with uses described in Treasury public notices. Treasury also evaluates whether the proposed external sharing is compatible with the purposes specified in the applicable SORN or other notices. Treasury modifies and republishes affected PCLIAs, SORNs, CMAs, PASs and website notices as needed to address substantial modifications to systems and information collections.	PA-4 Information Sharing with External Parties