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

Department of the Treasury Privacy Program Plan

Version: 1.0
Date: 27 May 2020

Table of Contents

1.0 Introduction

This Privacy Program Plan (PPP) describes how the Department of the Treasury ("Treasury" or "Department")[1], implements Office of Management and Budget (OMB) Circular A-130 guidance[2], for effectively managing Personally Identifiable Information (PII) as a strategic resource. This PPP also provides references to resources needed for compliance in daily privacy operations, and discusses distribution of authority/responsibility to implement these requirements by:

- Describing the structure of the Treasury-wide privacy program,
- Identifying resources dedicated to the privacy program,
- Discussing the infrastructure within Treasury for implementing the statutory and policy privacy designations/roles delegated to Treasury's Assistant Secretary for Management (ASM),
- Describing the role of other Treasury officials and privacy stakeholders in assisting the ASM in performing delegated privacy functions, and
- Explaining how Treasury implements or plans to implement program management controls and common controls for meeting applicable privacy requirements and managing privacy risks.

This PPP serves as a high-level outline of the Treasury-wide privacy program. The PPP is a living management document designed to accommodate changes in laws, technologies, and standards. Treasury bureaus and offices are encouraged to use it as the foundation for their own PPP when addressing bureau specific privacy matters.

2.0 Treasury Privacy Program Infrastructure and Organization

2.1 The Secretary of the Treasury

The Secretary of the Treasury's ("Secretary" or "Treasury Secretary") general authority is derived from 31 United States Code (U.S.C), Sections 301 and 321. Treasury's mission is to maintain a strong economy and create economic growth and stability at home and abroad, strengthen national security by combating threats and protecting the integrity of the financial system, and manage the U.S. Governments finances and resources effectively. Strong privacy protections are a key element in achieving these objectives.

[1] The "Department" or "Treasury" includes all of the Treasury Department's bureaus and offices.

[2] OMB Circular A-130 requires that all federal agencies: (a) consider and protect an individual's privacy throughout the information lifecycle; (b) develop and implement an agency-wide privacy program that includes people, processes, and technology; (c) ensure compliance with applicable privacy requirements regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of personally identifiable information (PII); (d) comply with all applicable privacy laws, including Privacy Act requirements; and (e) evaluate policies that impact privacy; and (f) manage privacy risks.

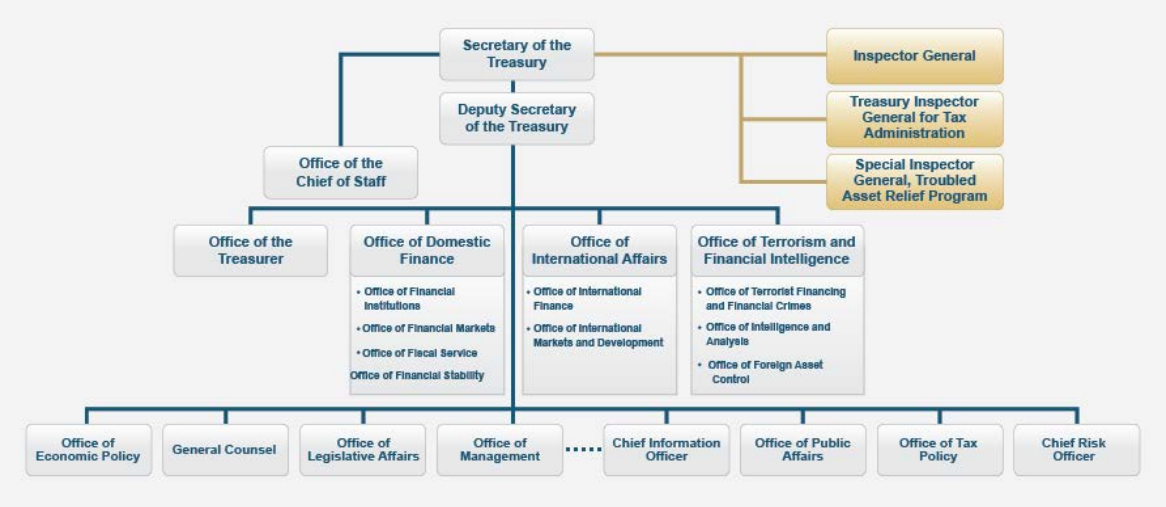

Figure 2.0 Treasury Organization (as of May 2020)

When Congress passes privacy legislation, it typically includes responsibilities directed to the Secretary as the "head of the agency." The Secretary typically delegates privacy duties and responsibilities to the Assistant Secretary for Management (ASM), whose placement in the organization is best suited to conduct the necessary oversight.

2.2 The ASM's Privacy Roles

The ASM (within the "Office of Management" in the figure above) is responsible for the overall implementation of privacy and civil liberties requirements. In Treasury Order 102-25, "Delegation of Authority Concerning Privacy and Civil Liberties" ("TO 102-25"), the Treasury Secretary designated the ASM as the Department's Chief Privacy and Civil Liberties Officer[3] (CPCLO), Senior Agency Official for Privacy[4] (SAOP), and Information Sharing Environment Privacy Official.[5] Specifically, TO 102-25 documents the Secretary of the Treasury's delegation of authority to the ASM to act on "all matters concerning privacy and civil liberties including,

[3] *The Consolidated Appropriations Act of 2005* requires Treasury to appoint a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy. Pub. L. No. 108-447, § 522(a)(1). Similarly, Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* requires the Department to appoint a senior officer to serve as its Privacy and Civil Liberties Officer. *See* Pub. L. No. 110-53, § 803(a)(1). Consistent with these requirements, Treasury Directive 25-09, *Privacy and Civil Liberties Activities Pursuant to Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007,* assigns all of these responsibilities to the Treasury Chief Privacy and Civil Liberties Officer.

[4] Office of Management and Budget Memorandum 05-08, *Designation of Senior Agency Officials for Privacy*, (Feb. 11, 2005), directs agency heads to designate a Senior Agency Official for Privacy with agency-wide responsibility for ensuring implementation of information privacy protections and full compliance with information privacy laws, regulations, and policies.

[5] *The Intelligence Reform and Terrorism Prevention Act of 2004*, as amended by the *Implementing Recommendations of the 9/11 Commission Act of 2007,* and implemented by Executive Order 13388, provides for the creation of the Information Sharing Environment (ISE), a framework to facilitate the maximum sharing of terrorism information. 6 U.S.C § 485(d)(2) and Executive Order 13388 established the need to protect privacy, civil liberties, and other legal rights of certain individuals with respect to information shared in the ISE. Treasury Directive 25-10, *Information Sharing Environment Privacy and Civil Liberties Policy*, establishes a privacy and civil liberties policy to guide the Department of the Treasury and assigns responsibility for overseeing all privacy and civil liberties activities related to protected information shared in the ISE to the ISE Privacy Official.

but not limited to, those associated with the Privacy Act of 1974, the Consolidated Appropriations Act of 2005, and the Implementing Recommendations of the 9/11 Commission Act of 2007."

2.2.1 The ASM's Role as Treasury's Senior Agency Official for Privacy (SAOP)

On September 16, 2016, OMB issued Memorandum 16-24, *Role and Designation of Senior Agency Official for Privacy*, in which it describes the SAOP's role and responsibilities as follows:

> The SAOP has the overall responsibility and accountability for ensuring the agency's implementation of information privacy protections, including the agency's full compliance with federal laws, regulations, and policies relating to information privacy, such as the Privacy Act. As required by the Privacy Act of 1974, the Federal Information Security Modernization Act (FISMA), and other laws and policies, each agency must take appropriate steps necessary to protect personal information from unauthorized use, access, disclosure or sharing, and to protect associated information systems from unauthorized access, modification, disruption or destruction.

The Secretary of the Treasury delegated the SAOP duties to the ASM because the ASM has broad insight into all Treasury bureaus and offices as the principal policy advisor to the Secretary and Deputy Secretary on the development and execution of the budget for Treasury and the internal management of the Department.

The SAOP is Treasury's key policy advisor on implementing the Privacy Act, and the privacy provisions of the E-Government Act of 2002, including FISMA, as amended in 2014. The ASM's primary responsibilities as the SAOP include:

- Acting as Treasury's senior policy authority on matters relating to the public disclosure of information, disclosure risks, and data sharing
- Developing and overseeing implementation of Department-wide policies and procedures relating to the Privacy Act, and assuring that PII contained in Privacy Act system of records (SOR) is handled in compliance with its provisions
- Communicating Treasury's privacy vision, principles and policies internally and externally
- Ensuring that Treasury addresses the privacy implications of all regulations and policies
- Promoting strategies for information collection and dissemination to ensure Treasury's privacy policies and principles are reflected in all operations
- Ensuring that Treasury complies with applicable privacy laws and regulations by enforcing policies and procedures and verifying bureaus and offices adherence to them
- Managing the process for reviewing and approving privacy programs as part of the OMB budget process

- Working with the Office of the Chief Information Officer (OCIO) to ensure the FISMA Security Assessment and Authorization (SA&A) process includes identification and remediation of privacy-related issues
- Managing privacy risks associated with Treasury activities that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by Treasury programs and information systems
- Ensuring employees and contractors receive appropriate training on privacy laws, regulations, policies, and procedures for handling personal information
- Facilitating and negotiating agreements with senior management, and establishing relationships with partners in private industry and other federal agencies to foster the development and sharing of privacy-related best practices, and
- Partnering with the OCIO to ensure all aspects of the Treasury privacy program are incorporated into Treasury's enterprise infrastructure, information technology (IT) and information lifecycle processes, and IT and non-IT security programs.

2.2.2 The ASM's Role as Treasury's Chief Privacy Officer (CPO)

Section 522 of the Consolidated Appropriations Act of 2005 requires Treasury to appoint a CPO to assume primary responsibility for privacy and data protection policy. These duties require the CPO to:

- Ensure that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection and disclosure of information in an identifiable form
- Ensure that technologies used to collect, use, store and disclose information in identifiable form allow for continuous auditing of compliance with stated privacy policies and practices
- Ensure that PII contained in Privacy Act SORs is handled in full compliance with the fair information practice principles that form the foundation of the Privacy Act of 1974
- Evaluate legislative and regulatory proposals involving collection, use and disclosure of personal information by the federal government
- Conduct privacy impact assessments for proposed rules of the department
- Prepare a report to Congress on an annual basis on activities of the department that affect privacy
- Ensure that the department protects information PII and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction
- Train and educate employees on privacy and data protection policies to promote awareness of and compliance with established privacy and data protection policies, and

- Ensure compliance with the department's established privacy and data protection policies.

2.2.3 The ASM's Role as Treasury's Chief Privacy and Civil Liberties Officer (CPCLO)

Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007 required Treasury to appoint a senior officer to serve as its Privacy and Civil Liberties Officer (PCLO). See Pub. L. No. 110-53, § 803(a)(1). Under Section 803, the PCLO is required to:

- Assist the head of such department, agency, or element and other officials of such department, agency, or element in appropriately considering privacy and civil liberties concerns when such officials are proposing, developing, or implementing laws, regulations, policies, procedures, or guidelines related to efforts to protect the Nation against terrorism
- Periodically investigate and review department, agency, or element actions, policies, procedures, guidelines, and related laws and their implementation to ensure that such department, agency, or element is adequately considering privacy and civil liberties in its actions
- Ensure that such department, agency, or element has adequate procedures to receive, investigate, respond to, and redress complaints from individuals who allege such department, agency, or element has violated their privacy or civil liberties
- Provide advice on proposals to retain or enhance a particular governmental power, considering whether such department, agency, or element has established that:
    - The need for the power is balanced with the need to protect privacy and civil liberties
    - There is adequate supervision of the use by such department, agency, or element of the power to ensure protection of privacy and civil liberties, and
    - There are adequate guidelines and oversight to properly confine its use.

Consistent with these requirements, Treasury Directive (TD) 25-09, "Privacy and Civil Liberties Activities Pursuant to Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007," assigns all of these responsibilities to the Treasury CPCLO, (the Treasury ASM).

2.2.4 The ASM's Role as Treasury's Information Sharing Environment Privacy Official (ISE PO

The *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA) (P.L. 108- 458), as amended by the *Implementing Recommendations of the 9/11 Commission Act of 2007* ("the 9/11 Commission Act") (P.L. 110-53), and implemented by Executive Order 13388, provides for the creation of the ISE, a framework to facilitate the maximum sharing of terrorism information, as defined in 6 U.S.C 485(a)(5). Section 485(d)(2) and Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information To Protect Americans*, also established the

need to protect privacy, civil liberties, and other legal rights of certain individuals with respect to information shared in the ISE.

As an ISE participant, Treasury is required to comply with the *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment* (the "ISE Privacy Guidelines"). The ISE Privacy Guidelines require that each participating agency "develop and implement a written ISE privacy [and civil liberties] protection policy that sets forth the mechanisms, policies, and procedures its personnel will follow in implementing [the ISE Privacy] Guidelines." The ISE Privacy Guidelines also require Treasury to appoint an ISE Privacy Official to oversee implementation of the guidelines.

TO 102-25 designates the ASM as Treasury's ISE PO. The Treasury ISE policy is maintained in Treasury Directive (TD) 25-10 and Treasury Directive Publications (TDP) 25-10, *Information Sharing Environment Privacy and Civil Liberties Policy: Implementation Plan,* July 2013. The TD and TDP address Treasury's sharing of terrorism information with other agencies in the ISE to the maximum extent allowed under applicable law.

Throughout this PPP, the combined privacy roles of the ASM referenced above are referred to collectively as "CPCLO" or "ASM/CPCLO" duties.

2.3 Primary External and Internal Privacy Controls and Oversight

The ASM/CPCLO is responsible for ensuring compliance with privacy requirements that originate from statutes passed by Congress, as well as Executive Orders (EO) and Presidential directives issued by the President of the United States. The President issues directives and EOs to his departments to manage operations of the Federal Government. EOs are legally binding orders given by the President as the head of the executive branch. They direct federal agencies in their execution of congressionally established laws and policies. Treasury's privacy organization is structured to implement EOs and respond to external requirements from the President and Congress.

2.3.1 Congress

The U.S. Congress' approach to privacy protection is often referred to as a "sectoral" approach. Rather than having a single, overarching data protection approach favored in the European Union and other countries, the U.S. Congress addresses privacy protection on a piecemeal basis. This approach focuses on issues relevant to particular sectors in the U.S. economy, and Congress drafts statutes to address the privacy risks unique to those sectors. In addition, to be responsive to concerns in particular sectors of the U.S. economy, Congress also focuses on particular types of PII that are typically collected in the private sector. As a result, the U.S. has separate privacy laws that focus on protecting financial information, health information, education information, electronic communications, video rentals, cable communications, credit reporting, and debt collection. Each of these laws is different in scope of coverage and penalties imposed. Many of these laws affect information federal agencies collect, but they do so in varying degrees and in different ways. Some of these laws have limited or no application to federal agencies.

In 1974, Congress created the Privacy Act to serve as a single, overarching federal law (see Appendix D, Key Federal Privacy Statutes) that provides a baseline for how federal agencies collect, use, maintain, and disclose PII. The Privacy Act is referred to as "baseline" because U.S.

law and Office of Management and Budget circulars and memoranda impose additional protections on particular types of information that federal agencies collect and maintain (for example, tax return information).

2.3.2 The President

OMB serves the President in overseeing the implementation of his/her vision across the executive branch. Specifically, OMB's mission is to assist the President in meeting his policy, budget, management, and regulatory objectives and to fulfill the agency's statutory responsibilities.

When it passed the Paperwork Reduction Act (PRA) in 1980, Congress created the Office of Information and Regulatory Affairs (OIRA) as a component of OMB. OIRA is charged with reviewing new collections of information initiated by federal agencies. OIRA is also charged with reviewing draft regulations, and developing and overseeing the implementation of government-wide policies in the areas of IT, information policy, and privacy. It also provides assistance to federal agencies by issuing privacy guidance in the form of circulars and memoranda. A list of applicable OMB memoranda and circulars, as well as Government Accountability Office (GAO) reports, and National Institute of Standards and Technology (NIST) standards can be found in Appendix B.

The ASM/CPCLO develops and maintains Treasury policies to implement EOs and OMB guidance related to privacy.

2.3.3 The Judiciary

The Judiciary interprets privacy law and resolves conflicts between the law and the Constitution. Court decisions affect privacy in federal agencies primarily (though not exclusively) as a result of judicial interpretations of the Privacy Act and the Freedom of Information Act (FOIA).

2.3.4 Treasury's Inspectors General

The Treasury Inspector General (OIG) is required to keep both the Secretary and the Congress fully and currently informed about the problems and deficiencies relating to the administration of department programs and operations and the necessity for corrective action. In this capacity, the OIG audits and issues reports regarding deficiencies in non-Internal Revenue Service Treasury programs, including privacy programs.

The Treasury Inspector General for Tax Administration (TIGTA) provides independent oversight of Internal Revenue Service (IRS) programs and operations. TIGTA promotes the economy, efficiency, and effectiveness in the administration of the internal revenue laws through its audit, inspections and evaluations, and investigations programs. It is also committed to the prevention and detection of fraud, waste, and abuse within the IRS and related entities. As part of its oversight activities, TIGTA has audited and issued reports regarding the IRS privacy program.

The Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP) is a federal law enforcement agency and an independent audit watchdog that targets financial institution crime and other fraud, waste and abuse related to the Troubled Asset Relief Program (TARP). In this capacity, SIGTARP audits and issues reports which could include privacy issues.

2.3.5 Treasury Orders, Directives, and Publications

The Secretary of the Treasury typically implements legal, regulatory, and policy requirements through publication of Treasury Orders (TOs), Treasury Directives (TDs), and Treasury Directive Publications (TDPs).

TOs are documents signed by the Secretary or Deputy Secretary that delegate authority residing in the Secretary or Deputy Secretary to other senior Treasury officials, define the organization of the Department and the reporting relationships among the most senior officials, and establish Treasury policy. For example, in TO 102-25, *Delegation of Authority Concerning Privacy and Civil Liberties*, the Treasury Secretary delegated authority to the ASM to handle privacy and civil liberties duties originating in statutes and policy directives.

TDs are documents signed by the appropriate senior Treasury official(s) that may further delegate authority from the most senior officials to other Treasury officials and provide processes for implementing legal obligations and departmental policy objectives.

The following TDs are relevant to privacy:

- TD 25-03, Filing Documents for Publication With the Office of the Federal Register
- TD 25-04, The Privacy Act of 1974, As Amended
- TD 25-06, The Treasury Data Integrity Board
- TD 25-07, Privacy and Civil Liberties Impact Assessment (PCLIA)
- TD 25-08, Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- TD 25-09, Privacy and Civil Liberties Activities Pursuant to Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53
- TD 25-10, Information Sharing Environment Privacy and Civil Liberties Policy
- TD 85-01, Department of the Treasury Information Technology (IT) Security Program

TDPs are detailed reference or process documents published in support of a specific TD. The responsible office (the office with the subject matter expertise) issues a TDP if it is expressly authorized by the companion TD. The TDP contains the procedures to implement policy established in a TD.

The links to TOs and TDs are on Treasury's website at (https://home.treasury.gov/about/general-information/orders-and-directives).

2.4 Assisting the CPCLO: Role of the Office of Privacy, Transparency, & Records, and other Treasury Privacy Stakeholders

An effective privacy program requires the ASM/CPCLO to evaluate and identify potential privacy risks associated with organizational activities. In addition, the ASM/CPCLO must oversee compliance efforts to mitigate risks while maintaining transparency, mission support, and effective business operations. At Treasury, the ASM/CPCLO leads all facets of privacy

policy development and implementation in coordination with the Office of Privacy, Transparency, & Records (PTR) and other Treasury privacy stakeholders.

To maintain an effective privacy program, the ASM/CPCLO must have the necessary authority, resources, and support to implement policies and programs to protect privacy and the PII that the Department collects, uses, maintains, and discloses. The ASM's primary privacy support staff is managed by the Deputy Assistant Secretary for Privacy, Transparency, & Records, who oversees four teams led by: the Director for Privacy & Civil Liberties, the Director for FOIA and Transparency, the Director for PTR Operations, and the Director for Records and Information Management (RIM) (See Figure 2.1).

2.4.1 Deputy Assistant Secretary for Privacy, Transparency, and Records (DASPTR)

PTR is led by the DASPTR, who reports directly to the ASM/CPCLO. The DASPTR is the ASM's principal advisor on privacy and civil liberties matters and is responsible for assisting the ASM in fulfilling the privacy and civil liberties duties delegated from the Secretary to the ASM in TO 102-25. In addition, the DASPTR is responsible for ensuring Treasury-wide compliance with information management laws, regulations, and policies, including the Privacy Act, the Federal Records Act, the Freedom of Information Act, and the Paperwork Reduction Act.

In most federal agencies, these information management functions are dispersed among different components within the agency or are treated as independent disciplines housed within the same component. Some federal agencies include two or more of these disciplines in a single office, but they are typically viewed as having independent missions and not as interrelated pieces of the same puzzle. Treasury is unique because it brings all of these information management disciplines together in one office. PTR has torn down the pre-existing silos/boundaries between these programs and, along with the OCIO and Treasury's other privacy stakeholders, promotes a holistic view of information management as a single puzzle with interlocking pieces.

2.4.2 Director for Privacy and Civil Liberties

The PTR Privacy and Civil Liberties (PCL) program is led by the Director for Privacy & Civil Liberties (PCL Director), who reports directly to the DASPTR. The PCL Director assists the ASM/CPCLO and the DASPTR by identifying and mitigating PCL compliance issues by:

- Serving as the Privacy and Civil Liberties Officer for Treasury's Departmental Offices
- Serving as the Treasury Privacy Officer for the Terrorist Finance Tracking Program agreement between the U.S. and the European Union
- Working closely with Treasury leadership and Treasury BPCLOs to develop, implement, and monitor agency-wide privacy policies and procedures in compliance with the U.S. Constitution and relevant federal statutes
- Reviewing Privacy Act System of Records Notices (SORNs)
- Ensuring the maintenance of the departmental PII holdings
- Reviewing Privacy and Civil Liberties Threshold Assessments for Departmental Offices (and other Treasury bureaus, as requested)

- Conducting and reviewing Privacy and Civil Liberties Impact Assessments (PCLIAs) for Departmental Offices (and other Treasury bureaus, as requested)
- Reviewing and obtaining approval for computer matching agreements (CMAs)
- Managing PII incident identification, inquiries, and remediation for Departmental Offices
- Identifying Treasury-wide PII incidents that may require escalation to the Treasury Personally Identifiable Information Risk Management Group (PIIRMG) pursuant to TD 25-08, and
- Working with the Bureau Privacy and Civil Liberties Officers or other Privacy personnel on reports to Congress, the General Accountability Office (GAO), and OMB, as required.

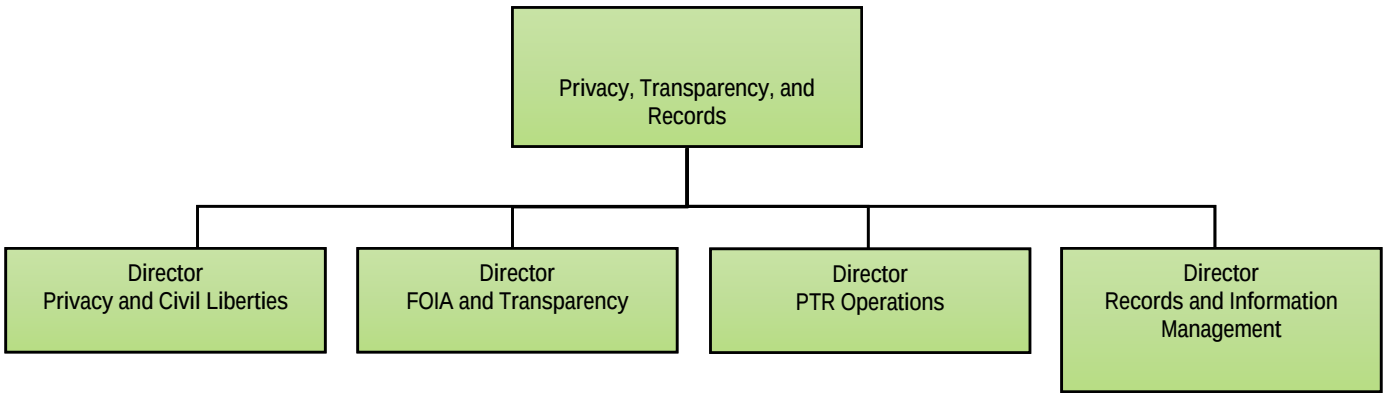

Figure 2.1 DASPTR PTR Staff Supporting the ASM/CPCLO

2.4.3 Other Treasury Privacy Stakeholders

The Treasury-wide privacy program is to some extent decentralized. Treasury is comprised of seven bureaus, the Departmental Offices (DO), and the Office of the Comptroller of the Currency (OCC). These bureaus and offices are responsible for implementing this PPP and establishing internal procedures to ensure the effectiveness of their bureau's privacy program:

1. Alcohol and Tobacco Tax and Trade Bureau (TTB)
2. Bureau of Engraving and Printing (BEP)
3. Bureau of the Fiscal Service (Fiscal Service)
4. Departmental Offices (DO)[6]
5. Financial Crimes Enforcement Network (FinCEN)

[6] DO includes the Officers of the Secretary, Domestic Finance, Economic Policy, Financial Research, General Counsel, International Affairs, Legislative Affairs, Management, Public Affairs, Tax Policy, Terrorism and Financial Intelligence, and the Treasurer of the United States.

6. Internal Revenue Service (IRS)
7. Office of the Comptroller of the Currency (OCC)
8. Treasury Inspector General for Tax Administration (TIGTA)
9. United States Mint (Mint)

The ASM/CPCLO supports and consults with the following department and bureau officials/stakeholders, as needed:

- **Bureau Heads:** Bureau heads are responsible for establishing internal procedures to ensure the effectiveness of their bureau's privacy program and conformity with Treasury-wide privacy requirements.
- **Bureau Privacy and Civil Liberties Officers (BPCLOs) and other Privacy Personnel:** Each Treasury bureau head assigns its own BPCLOs to work collaboratively with PTR to implement PCL protections at the bureau level. Each bureau has its own mission and unique PCL concerns that may not be shared by all bureaus. Therefore, as the experts with respect to their respective missions, BPCLOs manage their bureaus' day-to-day privacy and civil liberties compliance issues, and engage PTR as necessary to address issues that require ASM/CPCLO attention. The BPCLOs:
    - serve as the PCL point of contact for their bureau
    - maintain primary oversight and responsibility for ensuring continued policy implementation, training, monitoring, and compliance at their respective bureaus
    - determine whether bureau-specific training procedures should be required to address issues unique to their bureau
    - assist subcomponents within their bureau to facilitate adoption and implementation policies and procedures required to address unique bureau (and bureau component) privacy issues
    - routinely review bureau level information privacy and civil liberties procedures to ensure they are current, comprehensive and fully comply with local, state, and federal laws, regulations, and policies
    - mitigate reported errors and violations of Treasury and bureau privacy policies, including management of incidents and breaches implicating privacy and/or civil liberties
    - assist PTR in identifying issues that may require escalation to the ASM/CPCLO or the PIIRMG for resolution, and
    - identify and engage the necessary bureau stakeholders to assist PTR in meeting all statutory, OMB, GAO, Inspector General, or other external reporting requirements.

BPCLOs are not required to be experts on all PCL issues. They do, however, need to be able to identify the stakeholders in their bureau to consult as particular issues arise (for example, engaging bureau Office of General Counsel (OGC)/legal counsel on certain legal issues, including impacts to privacy and civil liberties).

- **Office of General Counsel/Legal Counsel (OGC):** OGC is involved in all privacy processes that require interpretation of federal statutes or regulations. Each bureau has its own embedded representative(s) from OGC, who addresses privacy and civil liberties legal issues as they arise. OGC also reviews documents before PTR or Treasury bureaus post them on public Treasury websites or share them outside Treasury (for example, disclosure to another federal agency) or inside Treasury for general applicability to all Treasury bureaus and offices (for example, proposed TOs, TDs and TDPs). The Treasury IGs do not have an embedded OGC representative and they do not conduct a review of documents before they are shared outside of Treasury with regard to the IGs.
- **Chief Information Officers, Program Managers, and Information System Owners:** These Treasury officials are responsible for the overall procurement, development, integration, modification, and/or operation and maintenance of information systems. They are responsible for identifying privacy issues and drafting required privacy compliance documentation (PCLTAs, PCLIAs, SORNs, and CMAs) when warranted. They also identify stakeholders within their bureau (e.g., BPCLOs and OGC) who can assist them in ensuring legal and regulatory compliance during the privacy documentation review/approval process.

The individuals performing the functions referenced above are referred to as "Treasury privacy stakeholders" or "privacy stakeholders" throughout this PPP.

2.5 Treasury-wide Privacy Staff Resources

The DASPTR, the PCL Director, the BPCLOs, and other privacy stakeholders assist the ASM/CPCLO's privacy oversight efforts. The DASPTR is a member of the Senior Executive Service. The PTR PCL team is staffed with a GS-15 (PCL Director), a GS-12 (Senior Privacy Analyst), and a GS-13 (Privacy Act Officer).

Treasury is comprised of seven bureaus, the Departmental Offices (DO), and the Office of the Comptroller of the Currency (OCC) that are responsible for policy formulation and overall management and implementation of privacy functions within their mission. The bureaus, DO, and OCC are staffed at the levels reflected in Table 2.2 below.

Bureau/Component	Privacy Staffing Level
Bureau of Engraving and Printing (BEP)	2
Departmental Offices (DO)	7
Financial Crimes Enforcement Network (FinCEN)	1
Fiscal Service (FS)	6
Internal Revenue Service (IRS)	44
Office of the Comptroller of the Currency (OCC)	3
Treasury Inspector General for Tax Administration (TIGTA)	1
Alcohol and Tobacco Tax and Trade Bureau (TTB)	0

U.S. Mint	2
TOTAL	66

Table 2.2 Treasury Privacy Staff Resources by Bureau/Component (as of January 2020)

3.0 Privacy Program Controls and Requirements

The NIST Special Publication (SP) 800-53 Rev. 4, Appendix J, provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber-attacks, natural disasters, structural failures, and human errors.

As required by NIST, the ASM/CPCLO, working in conjunction with the Treasury's Chief Information Officer (CIO) and other Treasury privacy stakeholders, identified a set of NIST controls to be implemented as common controls across Treasury. These common controls are the primary mechanism for ensuring the consistent Treasury-wide implementation of privacy requirements.

3.1 Privacy Controls

Privacy controls are the operational, technical, and management safeguards used to maintain the integrity, confidentiality, and security of PII maintained in federal information systems. The Privacy Act, Section 208 of the E-Government Act, and OMB policies impose collection, maintenance, use, and disposal requirements for executive branch agencies that maintain PII. Privacy controls are based on the Fair Information Practice Principles (FIPPs) embodied in the Privacy Act. The FIPPs provide the foundation and guiding principles for Treasury's privacy program controls.

At Treasury, the FIPPs are embodied in the following set of principles:

1. **Openness/Transparency**: Treasury will be transparent and provide notice to the public regarding its collection, use, sharing, and maintenance of PII.

2. **Individual Participation**: Treasury will involve the individual about whom information is collected in the process of collecting and using PII and, to the extent practicable and necessary, seek individual consent for the collection, use, sharing, and maintenance of PII. Treasury will also provide mechanisms for appropriate access, correction, and redress regarding Treasury's use of PII.

3. **Purpose Specification**: Treasury will specifically articulate the authority that permits the collection of PII and the purpose or purposes for which the PII is intended to be used.

4. **Collection Limitation/Data Minimization**: Subject to relevant exemptions, Treasury will only collect PII that is directly relevant and necessary to accomplish the specified purposes and only retain PII for as long as is necessary to fulfill the purposes specified in applicable notices.

5. **Use Limitation**: Treasury will use PII solely for the purposes specified in required notices (e.g., SORNs, PCLIAs, and CMAs). Sharing of PII outside the Department will be done in a manner compatible with the purpose for which the PII was originally collected.

6. **Data Quality/Integrity**: Treasury will, to the extent practicable and consistent with the purposes for which the information is used (e.g., for making vs. not making determinations about individuals), ensure that PII is accurate, relevant, timely, and complete.

7. **Security/Safeguards**: Treasury will protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

8. **Accountability/Auditing**: Treasury will be accountable for complying with these principles to the extent required by law, providing training to all employees and contractors who potentially have access to PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

There are eight privacy control families, each aligning with one of the FIPPs. Each family consists of one or more privacy controls, and each control contains one or more requirements. Treasury compliance with the NIST SP 800-53 Rev. 4, Appendix J privacy families is detailed under the column titled "How Treasury Meets the Privacy Control" in Appendix C. Compliance with all privacy controls is required at the agency, bureau, office, program, and information system level. The ASM/CPCLO, PTR, and all Treasury privacy stakeholders assist the bureaus and offices, to the greatest extent possible, in uniformly implementing the controls.

Table 3.2 (in Section 3.2 below) summarizes the classes and families in the security control catalog and the associated family identifiers. The objectives of the privacy program controls are to:

- Protect PII collected, used, maintained, shared, and disposed of by programs and information systems
- Provide a structured set of privacy controls that help organizations enforce requirements resulting from federal privacy legislation, policies, regulations, directives, standards, and guidance
- Establish a relationship between these controls to enforce privacy and security requirements within federal information systems, programs, and organizations,
- Demonstrate the applicability of the NIST Risk Management Framework (RMF) in the selection, implementation, assessment, and monitoring of privacy controls used in federal information systems, programs, and organizations, and
- Promote closer cooperation between privacy and security officials to help achieve the objectives of senior leaders in enforcing the requirements in federal privacy legislation, policies, regulations, directives, standards, and guidance.

3.2 Program Management Controls

OMB Circular A-130 and NIST SP 800-53 Rev. 4, Appendix J, provide significant assistance to federal agencies in implementing privacy requirements consistently throughout the organization. At Treasury, the ASM/CPCLO, working with Treasury privacy stakeholders, designates which privacy controls the agency will treat as program management, common, information system-specific, or hybrid controls.

Privacy Program Management controls are generally implemented at the agency/departmental level and are essential for managing the privacy programs across the organization. These controls are designed to facilitate privacy compliance with applicable federal laws, EOs, directives, policies, regulations, and standards across the organization. They also are designed to complement programmatic, organization-wide information security requirements.

Privacy Program Management controls also implicate multiple information management disciplines, including cybersecurity, records management, PRA, and FOIA. These controls are distinct from common, information system-specific, and hybrid controls because they apply to all information systems. Therefore, the ASM/CPCLO and Treasury privacy stakeholders must maintain a close partnership with other information management disciplines and the CIOs to ensure the proper implementation of these controls.

Table 3.2 below lists the control families that must be maintained across all Treasury organizations.

Appendix J – Privacy Controls		
Management	Authority and Purpose	AP
Management	Accountability, Audit, and Risk Management	AR
Management	Data Quality and Integrity	DI
Management	Data Minimization and Retention	DM
Management	Individual Participation and Redress	IP
Management	Security	SE
Management	Transparency	TR
Management	Use Limitation	UL

Table 3.2 Treasury Privacy Management Controls

The ASM/CPCLO and other Treasury privacy stakeholders work closely with the CIOs to ensure the confidentiality, integrity, and availability of Treasury data. The ASM/CPCLO must also collaborate with Records Management, PRA, Section 508 of the Rehabilitation Act, and FOIA personnel to implement these controls. For example, engagement with:

- The FOIA team may be required to implement transparency controls
- Records management staff may be required on data minimization and retention matters
- PRA staff may be required on authority and purpose, data minimization and data quality matters, and
- Section 508 staff may be required on individual participation matters.

3.3 Common Controls

The ASM/CPCLO, working with Treasury privacy stakeholders, is responsible for designating which controls the agency treats as common controls to meet the privacy requirements. Risk management is the process of identifying, assessing, and mitigating risk to an acceptable level. A risk assessment is the first step in the risk management process. During this assessment, the agency determines the extent of potential threats, vulnerabilities, and risks associated with its IT.

In NIST 800-53 Rev. 4, Appendix J, NIST explains that under existing OMB policy, the SAOP has overall responsibility for implementing privacy protections and ensuring that all privacy requirements are met. Accordingly, the ASM/CPCLO must collaborate with the CIOs and other Treasury privacy stakeholders to develop a privacy continuous monitoring strategy for bureau implementation, including approving the categorization of information systems, designating privacy controls, approving the information system-level privacy plan, conducting privacy control assessments, and reviewing authorization packages for information systems.

Common, information system-specific, and hybrid controls are implemented, at least in part, at the information system level:

- **Common controls** are controls that provide security/privacy capabilities for multiple information systems. These controls are referred to as "inherited controls" when applied to support a specific information system. When a common control is applied to a particular information system, that common control is deemed "inherited" for that system. The control itself is developed, implemented, assessed, authorized, and monitored by programs or officials other than those responsible for the information system.
- **Information system-specific controls** provide security/privacy for a particular information system or the portion of a hybrid control that is implemented for a particular information system.
- **Hybrid controls** are security/privacy controls where one part of the control is common and another part of the control is system-specific. These controls are implemented for an information system in part as a common control and in part as an information system-specific control.

Context determines if a privacy control is a common, hybrid, or information system-specific. By assigning privacy controls to an information system as information system-specific, hybrid, or common, the agency assigns accountability to specific agency programs or officials for the overall development, implementation, assessment, authorization, and monitoring of those controls.

The ASM/CPCLO designates common privacy controls. Common privacy controls are not managed by information system owners, but are managed at a higher level because they affect multiple systems. That means, in most cases, an agency program or official other than the information system owner manages them. Moreover, privacy controls designated as information system-specific may be the primary responsibility of information system owners and their respective authorizing officials. In all cases, the management of privacy controls are subject to the coordination and oversight of the ASM/CPCLO.

A security risk assessment helps management decide which controls to use to mitigate network risk to an acceptable level. These controls, in turn, need to be periodically reviewed to ensure they are effectively implemented.

Common controls are security controls that are primarily the responsibility of the CIOs. The security controls family protects organizational information systems (for example, contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls) and are key controls for the protection of privacy.

Treasury maintains an inventory of systems that maintain PII. These systems are identified through the PRA, cybersecurity documentation and Cybersecurity system operation authorization, and PCLIA processes to ensure the implementation of effective administrative, technical, and physical security policies and procedures to protect PII and mitigate risk. Treasury privacy stakeholders review PRA information collection requests (ICR), ensure that they include Privacy Act Statements (where applicable), and provide guidance to the PRA team for scrutinizing answers to the privacy questions in the PRA template (for example, relevance and necessity statements) before the ICR is submitted to OMB.

Information regarding all Treasury FISMA systems is maintained in the Treasury FISMA Inventory Management System (TFIMS), which serves as the repository for all Treasury cybersecurity documentation. The chart identifying these systems includes a column identifying whether the system maintains PII.

The primary tool for assessing privacy program/system compliance with common and system level privacy controls is the PCLIA. Treasury uses the PCLIA process to identify, address, and, where necessary, remediate issues/inconsistencies in compliance documentation, including SORNs, CMAs and formal agreements such as memoranda of understanding and memoranda of agreement. Treasury also conducts informal reviews to ensure continued compliance when system owners and personnel raise *ad hoc* issues for resolution. Treasury PCLIA templates scrutinize Privacy Act legal and OMB policy compliance issues that mitigate the potential risk of substantial harm, embarrassment, inconvenience, or unfairness to affected individuals as well as the financial and reputational risk to Treasury if PII is exposed. Additionally, Treasury PCLIAs address common controls by inquiring about technical and process solutions available to ensure the accuracy, completeness, and timeliness of PII maintained in information systems. PCLIAs are updated regularly as part of Treasury's continuous monitoring program.

The ASM/CPCLO collaborate with Treasury privacy stakeholders as necessary to ensure that appropriate protections are implemented and monitored. The BPCLOs assist the ASM/CPCLO with this responsibility by managing the PCLIA process and other privacy control implementation requirements at the bureau level.

The ASM/CPCLO is responsible for helping privacy stakeholders to identify and mitigate privacy risks related to PII loss. Meeting this responsibility requires close coordination with an organization's Information Technology (IT) security functions. It also requires a creative communication program and training that reinforces the information security message and the employee's responsibility for protecting privacy and all PII entrusted to the organization.

4.0 Privacy Program Plan Execution

The ASM/CPCLO serves as the primary privacy steward for Treasury. To be effective, the ASM/CPCLO has the full support of the Deputy Assistant Secretary for Privacy, Transparency, & Records (DASPTR), the Director for Privacy and Civil Liberties, the Bureau Privacy and Civil Liberties Officers (BPCLOs), and other Treasury privacy stakeholders. The ASM/CPCLO (as SAOP) also has the authority necessary to implement privacy policy for Treasury.

Due to the breadth of overseeing these functions for a large organization, the ASM/CPCLO works in partnership with the Treasury privacy stakeholders to ensure compliance with privacy requirements and implementation of the FIPPs throughout the Department.

4.1 Privacy Awareness and Training

Employees and contractors can be the weak link in the chain if not properly trained and educated to protect privacy. Privacy training and awareness programs are key elements of building a culture of privacy awareness throughout Treasury. Training programs test and reinforce privacy policy knowledge, an essential part of an effective privacy program. The ASM/CPCLO, working together with other Treasury privacy stakeholders, is responsible for ensuring that employees and contractors receive mandated annual privacy training.

Under Office Management and Budget (OMB) M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information,* training is mandatory and all agencies must initially train employees and contractors to ensure they understand their privacy and security responsibilities before permitting access to organization information and information systems. Treasury provides annual refresher training to ensure employees and contractors continue to understand their responsibilities. Both initial and refresher training include acceptable rules of behavior and consequences when the rules are not followed.

Training also addresses privacy risks unique to telework and other remote access programs. Treasury bureaus and offices use a variety of methods to remind employees of the need to take the annual Privacy Awareness refresher training. For example, Departmental Offices uses "Treasury Ticker" notifications to remind employees of annual refresher privacy training. Each bureau uses similar reminders to ensure employees and contractors complete the training.

As needed, the bureaus provide additional or advanced training for employees commensurate with increased responsibilities, changes in duties, or access to PII that is subject to particular statutory requirements.

4.2 Incident Response

OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, requires agencies to report all suspected or confirmed incidents involving PII to the National Cybersecurity and Communications Integration Center (NCCIC)/United States Computer Emergency Readiness Team (US-CERT). In order to comply with this requirement,

Treasury employees are instructed to report a suspected or confirmed breach as quickly as possible without delay pursuant to the Treasury Departmental Incident Response Plan (or the applicable bureau incident response plan). This includes a breach in any medium or form, including paper, oral, and electronic.

The Department has outlined, in TDP 85-01, incident response program requirements tasking bureau CIOs with maintaining proper incident response programs to facilitate bureau capabilities for responding to, investigating, mitigating, and reporting incidents involving bureau resources and infrastructure. Furthermore, TD 85-03 establishes the authorities of the Departmental Offices Chief Information Officer to coordinate with bureau officials to take appropriate action in the event of an actual, suspected, or threatened IT security incident or a significant IT vulnerability. This includes both PII and non-PII incidents.

TD 25-08, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, provides a high-level overview of Treasury and its bureaus' responsibilities when responding to a breach involving PII. These roles are further defined in the Treasury Departmental Incident Response Plan (DIRP) which provides more in-depth descriptions of the roles and responsibilities of various Treasury personnel for incidents involving PII as well as non-PII incidents.

The ASM/CPCLO collaborates with the bureau and departmental Chief Information Officer (CIO), and the Treasury Government Security Operations Center (GSOC) to report incidents to the NCCIC/US-CERT via the Treasury Computer Security Incident Response Capability (TCSIRC). The ASM/CPCLO and bureau privacy stakeholders also assist the CIOs in identifying, investigating, and mitigating any PII breaches resulting from a security incident. Treasury ensures the effectiveness of its incident response program by training all personnel and contractors on when and how to report PII and non-PII incidents.

4.3 Privacy Reporting

Treasury is required to report to OMB and Congress on various aspects of its privacy program activities. Reporting efforts are initiated by the PTR PCL Director or other members of the PTR PCL team through data calls sent to the BPCLOs. PTR then incorporates the data call responses into the relevant report and obtains departmental clearance before delivery to the required recipient(s). The following is a list of privacy reporting requirements that apply to Treasury at the departmental level:

- The Privacy Act and OMB Circular A-108 require that agency Data Integrity Boards (DIB) (required for agencies that participate in matching programs) report data summarizing that calendar years matching activity.
- Under Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, the Chief Privacy and Civil Liberties Officer (CPCLO) must submit semiannual reports covering the agency's privacy protection activities.
- FISMA requires federal agencies to conduct an annual review of their information security programs and report to OMB. This includes Privacy Act and PII reporting requirements.

- EO 13636, *Improving Critical Infrastructure Cybersecurity*, Section 5, requires the ASM/CPCLO to consult with the Privacy and Civil Liberties Oversight Board (PCLOB) to annually assess the PCL effects of activities related to information Treasury's Office of Critical Infrastructure shares with the Financial Services Sector. The ASM/CPCLO is required to submit these assessments to the Department of Homeland Security's (DHS) Office for Civil Rights and Civil Liberties and the DHS Privacy Office for compilation and publication in a single government-wide report.

- Section 522 of the *Consolidated Appropriations Act of 2005*, requires Treasury to prepare an annual report to Congress covering the Department's activities that affect privacy. These activities include public complaints of alleged Privacy Act and other privacy violations originating from Treasury programs,

- The *Federal Agency Data Mining Reporting Act of 2007* provides that "the head of each department or agency of the Federal Government that is engaged in an activity to use or develop data mining shall submit a report to Congress on all such activities of the department or agency." "Data mining" is defined under the act as a:

  > program involving pattern-based queries, searches or other analyses of one or more electronic databases, where a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals; the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases.

- The ASM/CPCLO is required to report all significant changes to SORNs to OMB and Congress following the requirements identified in OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*.

- FISMA requires all federal agencies to notify the appropriate Congressional Committees no later than seven days after the date on which there is a reasonable basis to conclude that a breach that constitutes a "major incident" has occurred. Agencies must also supplement their initial seven-day notification to Congress with a report no later than 30 days after the agency discovers a "major" breach.

- OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information,* requires that agencies report PII and non-PII incidents to the NCCIS/US-CERT as required by the US CERT Federal Incident Notification Guidelines. The US CERT Guidelines require that federal agencies report potential compromises to the confidentiality, integrity, or availability of information maintained in federal information systems to the NCCIC/US-CERT within one hour of identification by Treasury's Government Security Operations Center (GSOC).

- External reporting may also include responding to requests from an organization's OIG or from the Government Accountability Office (GAO) seeking information and documentation that demonstrates compliance with applicable privacy laws and regulations.

5.0 Privacy Control Requirements

The privacy controls are based on the FIPPs derived from the Privacy Act, Section 208 of the E-Government Act of 2002, and from OMB guidance. The FIPPs are designed to build public trust and help agencies avoid tangible and intangible costs resulting from privacy incidents. There are eight privacy control families, each aligning with one of the FIPPs. Each family consists of one or more privacy controls, and each control imposes one or more requirements. All privacy families, including their controls and requirements, are implemented at the agency, bureau, program, or information system level. Treasury privacy controls are implemented under the leadership of the Senior Agency Official for Privacy (ASM/CPCLO) by PTR and other Treasury privacy stakeholders.

Internally, PTR and Treasury privacy stakeholders enforce compliance through the Privacy and Civil Liberties Threshold Analysis (PCLTA) and Privacy and Civil Liberties Impact Assessment (PCLIA) processes. Both processes originate from the requirements in OMB Memorandum 03-22, *OMB Guidance for Implementing the Privacy provisions of the E-Government Act of 2002.* Treasury emphasized civil liberties in its privacy impact assessment process to reflect the expanded roles and responsibilities of federal agencies in this area and to acknowledge the relationship between the implementation of the FIPPS and the protection of civil liberties.

5.1 Privacy and Civil Liberties Threshold Analysis

Some systems and projects do not require a PCLIA, either because they do not collect PII or because an OMB M-03-22 exemption applies. A PCLTA is used to determine if a PCLIA is required. If a system owner is uncertain whether a PCLIA is required, they must use the Departmental PCLTA template (or a bureau-specific alternative) to assist them in making this determination.

Treasury BPCLOs assess the bureau's information systems and determine whether a PCLIA is required. A PCLTA also documents the BPCLO's reasons for determining that a PCLIA was or was not required. A PCLTA must be reviewed and updated as necessary where an IT system or information collection modification creates new privacy risks or to reflect changed information collection authorities, business processes, or other factors affecting the collection and handling of PII.

5.2 Privacy and Civil Liberties Impact Assessment

A PCLIA is a process conducted to: (i) analyze how information is handled: (ii) to ensure handling conforms with applicable legal, regulatory, and policy requirements regarding privacy; (iii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and (iv) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. The goal in conducting the PCLIA is to identify and mitigate privacy risks. The PCLIA also ensures that the information system has the controls in place to ensure compliance with applicable privacy and records and information management laws, policies, and regulations. The

PCLIA also provides the public with notice at the system level regarding the PII Treasury is collecting, why the PII is being collected, and how the PII will be collected, used, accessed, shared, safeguarded and stored.

PCLIAs are typically approved at the bureau level by the BPCLO, who acts as the reviewing official for bureau PCLIAs. The BPCLO provides the certification because they have the unique knowledge of the information, the systems and the bureau mission that are necessary to conduct a thorough assessment. For example, at Departmental Offices, PCLIAs are certified and reviewed by the PTR Director for Privacy and Civil Liberties (as the DO BPCLO). The PTR DASPTR acts as the reviewing official to approve PCLIAs that cover Treasury-wide and multi-bureau system PCLIAs.

5.3 System of Records Notice (SORN)

The SORN is the vehicle by which Treasury notifies individuals that the agency maintains information about them in a system of records, what categories of records are maintained about them, the category of individuals covered by the system, how the information is shared externally by Treasury (routine uses), and how long the information is retained. The Privacy Act defines a "system of records" as "a group of any records under the control of any agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier." When Treasury maintains information about an individual in a system of records and retrieves the information by a personal identifier, it must publish a SORN in the *Federal Register*

The ASM/CPCLO oversees Treasury's development and publication of SORNs, but the processing of all departmental SORNS is the responsibility of PTR. The drafting of SORNS and the required OMB and statutory documentation is the responsibility of the Treasury privacy stakeholder who operates the system of records.

During SORN review, the ASM/CPCLO, through PTR, collaborates with the bureau proponent of the SORN to determine whether records used in the system or by the program receive coverage from an existing SORN or whether a new SORN is required. If exemptions from certain Privacy Act provisions are claimed for a system of records for law enforcement or national security reasons, the bureau or office proposing the exemption also drafts a Notices of Proposed Rulemaking ("NPRM") (and the Final Rule, as needed) for publication in the *Federal Register*. All SORNs receive a stringent legal review before they are sent to the PTR DASPTR for approval and transmission to OMB/OIRA.

OMB Circular A-108, *Federal Agencies Responsibilities for Review, Reporting, and Publication under the Privacy Act*, requires that all federal agencies submit their SORNs to OIRA for comment and approval before the SORN is published in the *Federal Register*. Circular A-108 also requires that agencies send notice to Congress 30 days before publication in the Federal Register. After receiving approval from OMB (and in the absence of comment from Congress), Treasury publishes its SORNs in the *Federal Register* before the system becomes operational. If no comments are received from the public, the SORN becomes final without the publication of a final rule. If comments are

received, the ASM/CPCLO will review them with the program manager and legal counsel before the final rule is published. An updated SORN (to address public comments) can be republished along with the final rule. After the SORN publication requirements are completed, the system of records becomes operational.

Agencies are required to establish and maintain an agency-wide privacy continuous monitoring (PCM) program. The PCM program replaced the former requirement that agencies conduct Privacy Act reviews of their SORNs on an annual basis. Information systems that maintain systems of records are required to monitor the effectiveness of their privacy controls on an ongoing basis, document changes to the information system, and determine whether the applicable SORN(s) remains accurate or requires updating.

If a system of records is no longer needed, Treasury begins the process to remove it from its inventory. The ASM/CPCLO, through PTR, works with the program managers to determine if a system of records should be retired. If the ASM/CPCLO determines that rescission is appropriate, the relevant bureau drafts a Notice of Rescindment of a Privacy Act SOR. The rescindment notice summarizes what information system is being retired, what the system was originally designed to collect, and why it is being retired. The notice must also provide an account of what will happen to the records that were previously maintained in the system. The ASM/CPCLO and legal counsel approve the rescindment notice before it is submitted to OMB and before publication in the *Federal Register*.

5.4 Privacy Act Statement

Under Section (e)(3) of the Privacy Act, if an agency asks individuals to supply information that will become part of a system of records, the agency must provide a Privacy Act Statement (PAS) on the form used to collect the information or on a separate form that can be retained by the individual. The agency is required to provide the PAS regardless of whether the information is collected on paper or an electronic form, on a website, on a mobile application, over the telephone, or through some other medium. The PAS ensures that the individual is provided with the following information about the request for information:

> (1) the authority (whether granted by statute or EO) that authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;
>
> (2) the principal purpose(s) for which the information is intended to be used;
>
> (3) the published routine uses to which the information is subject;
>
> (4) the effects on the individual, if any, of not providing all or any part of the requested information (for example the loss or denial of a privilege, benefit, or entitlement sought as a consequence of not furnishing the requested information); and
>
> (5) an appropriate citation (and, if practicable, a link) to the relevant SORN(s)

The PAS is drafted and reviewed by various privacy stakeholders. The Office of General Counsel representative for the relevant bureau reviews the PAS before it is added to a form or other method of delivery to the individual from whom Treasury collects information.

5.5 Computer Matching Agreements

In 1988, Congress passed the Computer Matching and Privacy Protection Act (CMPPA), amending the Privacy Act to require that individuals receive due process when their information is used to make decisions about them in "*matching programs*." A matching program is any comparison of two or more automated computerized federal or non-federal system of records for the purpose of "establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirement by applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit program or recouping payments or delinquent debts under such Federal benefits programs." (5 U.S.C. § 552a(a)(8)). The CMPPA required that federal agencies that maintain matching programs establish a Data Integrity Board to oversee and coordinate the implementation of the Act.

In compliance with the CMPPA, Treasury established Treasury Directive 25-06, *The Treasury Data Integrity Board*, setting forth the policy for the DIB's membership, operations, and responsibilities, as well as the procedures for engaging in computer matching activities. The DIB is chaired by the Deputy Assistant Secretary for PTR (DASPTR), who reports directly to the ASM/CPCLO. The DASPTR conducts oversight (in partnership with the bureaus and offices represented on the DIB) by reviewing and approving Treasury's Computer Matching Agreements (CMAs) and reporting regularly to the ASM/CPCLO on all matters related to matching agreements. The Treasury DIB is comprised of: the Treasury Inspector General, the Deputy Assistant Secretary for Privacy, Transparency, and Records (DASPTR), the Departmental Privacy Act Officer, and representatives from each Treasury bureau that conducts matching agreements (as designated by the Secretary). The DIB board ensures that CMAs include the required procedural and other protections necessary to manage the recipient agency's use of information and procedures regarding notifications to individual, information verification, record retention, and safeguarding.

OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, discusses the content of a "*matching notice*" as follows:

> A matching notice identifies the agencies involved, the purpose(s) of the matching program, the authority for conducting the matching program, the records and individuals involved, and additional details about the matching program. The requirement for agencies to publish a matching notice allows the Federal Government to foster transparency and accountability with respect to agencies' matching programs.

TD 25-04, *The Privacy Act of 1974, as amended*, at Section 6.b., requires the DASPTR to "submit reports on new or altered systems of records notices to the Office of Management and Budget (OMB) and Congress when required by Section (r) of the Privacy Act." Section r requires that agencies that participate in matching programs must provide notice of new matching programs or significant changes to existing programs to "the Committee on Government Operations of the House of Representatives, the Committee on Governmental Affairs of the Senate, and the Office of Management and Budget in order to permit an evaluation of the probable or potential effect of such proposal on the privacy or other rights of individuals."

The Inspector General Empowerment Act of 2016[7] (IGEA) exempts certain computerized data comparisons performed by or in coordination with Inspectors General (IGs) from the CMPPA's restrictions and requirements (the "CMPAA Exemption").

5.6 Contractors and Third Parties

The Treasury Office of the Procurement Executive (OPE) collaborates with the ASM/CPCLO to ensure that appropriate provisions (contract clauses) are added to contracts where contractors will have access to PII in Treasury systems or store Treasury PII on contractor systems. The DASPTR, the PTR Director of Privacy and Civil Liberties, and other Treasury privacy stakeholders work with the OPE to ensure that such contracts include contract clauses to ensure that contractors and service providers are obligated to comply with all applicable privacy and related records management laws and policies.

The OPE also collaborates closely with the ASM/CPCLO, through PTR and the OCIO, when making new purchases, revising existing purchase orders, and considering alternative ways for handling information systems that reduce costs or improve efficiency. Through collaboration and consultation between the OPE, ASM/CPCLO, PTR, OCIO, contracting officers and other Treasury privacy stakeholders, Treasury ensures statutory, regulatory and policy compliance, including the insertion of appropriate privacy clauses in Treasury contracts and other agreements.

The ASM/CPCLO, working with OPE, PTR and other Treasury privacy stakeholders, identified or developed the following clauses prescribed by the Federal Acquisition Request (FAR) and Department of the Treasury Acquisition Procedure (DTAP):

- FAR subpart 4.19 - Basic Safeguarding of Covered Contractor Information Systems
- FAR Clause 52.204-21 - Basic Safeguarding of Covered Contractor Information Systems Contract Clause
- FAR subpart 24.1 Protection of Individual Privacy
- FAR clause 52.224 - 1 "Privacy Act Notification"
- FAR clause 52.224 - 2 "Privacy Act"
- FAR subpart 24.3 Privacy Training
- FAR clause 52.224 - 3 "Privacy Training"
- FAR subpart 27.4 Rights in Data and Copyrights
- FAR subpart 39.1 General
- FAR clause 52.239 - 1 "Privacy or Security Safeguards"
- DTAP subpart 1024.1 Protection of Individual Privacy
- DTAP subpart 1024.3 Privacy Training

[7] Pub. L. No. 114-317, codified at 5 U.S.C. Section 552a(6)(j)(2).

- DTAP subpart 1024.70 Privacy Requirements
- DTAP subpart 1027.4 Rights in Data and Copyrights

Treasury BPCLOs provide the same scrutiny to all contracts and agreements proposed at the bureau level, ensuring that privacy requirements and clauses are included in the terms and conditions of contracts and other bureau-level contracts and agreements.

Treasury also ensures that contractors who create, collect, use, process, store, maintain, disseminate, disclose, or dispose of information on behalf of the Treasury, or who operate or use information systems on behalf of the Treasury, comply with mandated privacy requirements. For example, contractors, like Treasury employees, must comply with Treasury privacy training requirements by completing applicable training required by Treasury or its bureaus. Lastly, contractors who require access to Treasury PII and other high risk information are required to protect and safeguard the information, report breaches, and cooperate with Treasury officials in the event of a breach.

Appendix A: Frequently Used Acronyms and Abbreviations

Acronym List	
API	Application Programming Interface
ASM	Assistant Secretary for Management
BPCLO	Bureau Privacy and Civil Liberties Officer
CAA	Consolidated Appropriations Act
CFO	Chief Financial Officer
CFAA	Computer Fraud and Abuse Act
Ch.	Chapter
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMA	Computer Matching Agreement
CMPPA	Computer Matching and Privacy Protection Act
CPCLO	Chief Privacy and Civil Liberties Officer
CPO	Chief Privacy Officer
CTO	Chief Technology Officer
DASPTR	Deputy Assistant Secretary for Privacy, Transparency, and Records
DHS	Department of Homeland Security
DIB	Data Integrity Board
DPCLO	Director of Privacy and Civil Liberties Officer
DO	Departmental Offices
DOJ	Department of Justice
DTAP	Department of the Treasury Acquisition Procedure
EIT	Electronic and Information Technology
EO	Executive Order
FAR	Federal Acquisition Regulation
FIPPs	Fair Information Practice Principles
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
FR	Federal Register
FRA	Federal Records Act
GAO	Government Accountability Office
GSOC	Government Security Operations Center
HIPAA	Health Insurance Portability and Accountability Act
ISCM	Information Security Continuous Monitoring
ISE	Information Sharing Environment
ISEPO	Information Sharing Environment Privacy Official
IT	Information Technology
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
No.	Number
NPRM	Notice of Proposed Rule Making

OCIO	Office of Chief Information Officer
OCRCL	Office of Civil Rights and Civil Liberties
OPCL	Office of Privacy and Civil Liberties
OGC	Office of General Counsel
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
PCLOB	Privacy and Civil Liberties Oversight Board
PCLTA	Privacy and Civil Liberties Threshold Analysis
PCLIA	Privacy and Civil Liberties Impact Assessment
PCM	Privacy Continuous Monitoring
PCR	Privacy Compliance Review
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIRP	Privacy Incident Response Plan
PITTF	President's Identity Theft Task Force
P.L.	Public Law
POTUS	President of the United States
PRA	Paperwork Reduction Act
PTR	Privacy, Transparency, and Records
Rev.	Revision
RIM	Records Information Management
RM	Risk management
RMF	Risk Management Framework
ASM/CPCLO	Senior Agency Official for Privacy
SOR	System of Records
SORN	System of Records Notice
SPP	Security Program Plan
SP	Special Publication
TCSSIRC	Treasury Computer Security Incident Response Capability
TD	Treasury Directive
TDP	Treasury Directive Publications
TFIMS	Treasury FISMA Inventory Management System
TO	Treasury Order
U.S.	United States

Appendix B: Legislative, OMB, NIST, GAO, and Treasury Guidance

Each organization has its own statutory and policy-based compliance requirements. The following is an extensive but not complete list of the sources from which most federal privacy and civil liberties requirements originate. Their applicability depends on the organization's mission and mandates.

Legislative Guidance and Authorities

- Privacy Act of 1974, as amended (5 U.S.C. § 552a)
- Federal Information Security Modernization Act of 2014 (44 U.S.C. § 3541, et seq.)
- E-Government Act of 2002 (Pub. L. No. 107-347, 116 Stat. 2899)
- Freedom of Information Act (5 U.S.C. § 552)
- Paperwork Reduction Act of 1995 (44 U.S.C. § 3501, et seq.)
- Children's Online Privacy Protection Act of 1998 (15 U.S.C. §§ 6501 et seq., 16 C.F.R. § 312)
- Federal Agency Data Mining Reporting Act of 2007 (42 U.S.C. § 2000ee-3)
- Federal Records Act of 1950 (44 U.S.C. Ch. 31)
- Health Insurance Portability and Accountability Act of 1996 (Pub. L. No. 104-191)
- Homeland Security Presidential Directive-12 (HSPD-12): Policies for Common Identification Standard for Federal Employees and Contractors
- 42 U.S.C. § 2000ee–1 Privacy and civil liberties officers
- Section 1061 of the Intelligence Reform and Terrorism Prevention Act (Pub. L No. 108-458)
- Internal Revenue Code (26 U.S.C. §§ 6103, 6108, and 7609)
- Section 522 of the Transportation, Treasury, and Independent Agencies, and General Government Appropriations Act of 2005 (Pub. L. No. 108-447, div. H, Dec. 8, 2004, 118 Stat. 2809)

OMB Guidance

- OMB Memorandum for Privacy Act Officers of Departments and Agencies, Status of Biennial Reporting Requirements under the Privacy Act and the Computer Matching and Privacy Protection Act (June 21, 2000)
- OMB M-01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy (December 20, 2000)
- OMB M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 26, 2003)

- OMB M-05-04, Policies for Federal Agency Public Websites (December 17, 2004)
- OMB M-05-08, Designation of Senior Agency Officials for Privacy (February 11, 2005)
- OMB M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors (August 5, 2005)
- OMB M-06-16, Protection of Sensitive Agency Information (June 23, 2006)
- OMB M-07-20, FY 2007 E-Government Act Reporting Instructions (August 14, 2008)
- OMB M-08-09, New FISMA Privacy Reporting Requirements for FY 2008 (January 18, 2008)
- OMB M-10-06, Open Government Directive (December 8, 2009)
- OMB Memo M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies (June 25, 2010)
- OMB M-10-23, Guidance for Agency Use of Third-Party Websites and Applications (June 25, 2010)
- Model Privacy Impact Assessment for Agency Use of Third-Party Websites and Applications, (December 29, 2011)
- OMB M-13-13, Open Data Policy-Managing Information as an Asset (May 9, 2013)
- OMB M13-20, Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative (August 16, 2013)
- OMB M-14-06, Guidance for Providing and Using Administrative Data for Statistical Purposes, (February 14, 2014)
- OMB M-16-24, Role and Designation of Senior Agency Officials for Privacy (September 15, 2016)
- OMB M-17-09, Management of Federal High Value Assets, (December 9, 2016)
- OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017)

OMB Circulars

- OMB Circular A-130, Managing Information as a Strategic Recourse (July 28, 2016)
- OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act (December 23, 2016)
- OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control (July 15, 2016)

NIST Guidance

- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems (February 2004)
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems (March 2006)
- NIST Special Publication (SP) 800-12 Rev. 1, An Introduction to Information Security (June 2017)
- NIST SP 800-16, Information Technology Security Training Requirements: a Role- and Performance-Based Model (April 1998)
- NIST SP 800-30 Rev. 1, Risk Management Guide for Information Technology Systems (September 2012)
- NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (December 2018)
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View (March, 2011)
- NIST SP 800-50, Building Information Technology Security Awareness and Training Program (October 2003)
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations (January 2015)
- NIST SP 800-53A Rev. 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans (December 2014)
- NIST SP 800-59, Guideline for Identifying an Information System as a National Security System (August 2003)
- NIST SP 800-60 Vol. 1 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories (August 2008)
- NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide (August 2012)
- NIST SP 800-83 Rev. 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops (July 2013)
- NIST SP 800-100, Information Security Handbook: A Guide for Managers (March 2007)
- NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (April 2010)

Office of Information and Regulatory Affairs (OIRA) Governing Authorities

- 44 U.S.C. Chapter 35 – Paperwork Reduction Act
- 5 U.S.C. § 552a – Privacy Act

- 5 U.S.C. Chapter 8 – Congressional Review Act
- 44 U.S.C § 3501 – Confidential Information Protection and Statistical Efficiency Act
- 44 U.S.C § 3516 – Information Quality Act
- 5 U.S.C. § 601 – Regulatory Flexibility Act
- Executive Order 13783 – Promoting Energy Independence and Economic Growth
- Executive Order 13777 – Enforcing the Regulatory Reform Agenda
- Executive Order 13771 – Reducing Regulation and Controlling Regulatory Costs
- Executive Order 13610 – Identifying and Reducing Regulatory Burdens
- Executive Order 13609 – Promoting International Regulatory Cooperation
- Executive Order 13579 – Regulation and Independent Regulatory Agencies
- Executive Order 13563 – Improving Regulation and Regulatory Review
- Executive Order 12866 – Improving the Planning and the Coordination of Federal Regulation
- Executive Order 9397 – Numbering Systems for Federal Accounts Relating to Individual Persons

Appendix C: Treasury Compliance with NIST SP 800-53 Rev. 4, Appendix J

This appendix is provided as a separate document.

Appendix D: Summary of Key Federal Privacy Statutes

- **The Privacy Act of 1974, as amended (5 U.S.C. § 552a)**, available at: https://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf . The Privacy Act allows U.S. citizens and persons admitted to the U.S. for permanent residence to review personal information that is maintained about them in paper and electronic form by the federal government unless such information is specifically exempted from the access provisions. It allows these individuals to seek amendment of their records and provides for relief in federal court if the government wrongly refuses to amend, unless specifically exempted from this provision. This law requires agencies to publish systems of records notices whenever they collect personally identifiable information (PII) that is retrieved (either manually or electronically) by a unique personal identifier.

- **CMPPA of 1988, P.L. 100-503,** available at: https://www.gpo.gov/fdsys/pkg/STATUTE-102/pdf/STATUTE-102-Pg2507.pdf . The CMPPA amended the Privacy Act to add several new provisions: 5 U.S.C. § 552a (a) (8) - (13), (e) (12), (o), (p), (q), (r), (u) (2006). The CMPPA added procedural requirements that federal agencies must follow when engaging in computer-matching activities. This includes civil liberties protections that require federal agencies to provide individuals an opportunity to receive notice and to refute adverse information before the government denies or terminates rights, benefits, or privileges. The CMPPA require that agencies engaged in matching activities establish Data Integrity Boards to oversee those activities.

- **Clinger-Cohen Act of 1996 also known as the ITMRA, P.L. 104-106**, available at: https://www.treasury.gov/privacy/Documents/Clinger-Cohen_Act_of_1996.pdf . The ITMRA together with the Federal Acquisition Reform Act became known as the Clinger-Cohen Act. ITMRA is designed to improve the way the federal government acquires, uses, and disposes of information technology. The Clinger-Cohen Act supplements the information resources management policies of the executive agencies by ensuring a comprehensive approach to improve the acquisition and management of the agency's information resources.

- **Computer Fraud and Abuse Act (CFAA) of 1986, P.L. 104-106**, available at: https://www.law.cornell.edu/uscode/text/18/1030. CFAA was enacted by Congress as an amendment to existing computer fraud law (18 U.S.C. § 1030), which had been included in the Comprehensive Crime Control Act of 1984. The law prohibits accessing a computer without authorization, or in excess of authorization.

- **Consolidated Appropriation Act (CCA) of 2005, P. L. 108-447**, available at: https://www.gpo.gov/fdsys/pkg/PLAW-108publ447/pdf/PLAW-108publ447.pdf . Section 522(a) of the CCA requires each agency to have a Chief Privacy Officer (CPO) with the responsibility of protecting privacy and safeguarding data collected from individuals. It also prescribes other roles and responsibilities of the CPO. Additionally the Chief Privacy Officer must ensure that PII contained in a system of records is handled pursuant to the Privacy Act and adhere to the privacy reporting requirements.

- **Rehabilitation Act of 1998, Section 508,** available at: https://section508.gov/content/learn/laws-and-policies. In 1998, Congress amended the Rehabilitation Act of 1973 (*29 U.S. C. § 794 (d)*) to require federal agencies to make their Electronic and Information Technology (EIT) accessible to people with disabilities. This law applies to all federal agencies as they develop, procure, maintain, or use information technology. Under Section 508, agencies must give disabled employees and disabled members of the public access to information that is comparable to the access available to employees and members of the public who do not have disabilities.

- **The E-Government Act of 2002, P.L. 107-347**, available at: https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/html/PLAW-107publ347.htm . The E-Government Act requires every federal agency to conduct a Privacy Impact Assessment (PIA) on its IT Systems. A PIA is required when designing and developing a new information system or amending an old system that contains personally identifiable information (PII). The purpose of the PIA is to ensure that privacy protections and Privacy Act requirements are considered in developing information systems. The OMB Office of Information and Regulatory Affairs (OIRA) drafted guidelines for conducting PIAs: M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (September 30, 2003). Treasury has expanded the coverage of its PIA to include civil liberties. Therefore, Treasury refers to them as Privacy and Civil Liberties Impact Assessments (PCLIA).

- **The Paperwork Reduction Act (PRA) of 1995**, available at: https://www.gpo.gov/fdsys/pkg/PLAW-104publ13/html/PLAW-104publ13.htm . Congress enacted the PRA to minimize the paperwork burden that the government imposes on the public and to improve the quality of its information. PRA requires federal agencies to establish an independent review process for information collection. In the PRA, Congress established the OIRA within OMB and required that it provide guidance to and oversight of federal agencies' information collection practices. OMB has used this authority to require the posting of privacy policies on federal agencies' websites and developed restrictions on the use of "cookies" on federal websites. Federal agencies must get OMB approval before undertaking a collection of information directed to 10 or more individuals.

- **The Federal Records Act (FRA) of 1950,** available at: http://www.archives.gov/about/laws/fed-agencies.html. FRA requires the head of each federal agency to make and preserve records containing proper documentation of its functions, policies, decisions, procedures, and essential transactions to furnish the information necessary to protect the legal and financial rights of the government and of individuals directly affected by the agency's activities. This Act requires agencies to establish and maintain an active program for the efficient management of the agency's records. The program must provide for:

- Effective control over the creation, maintenance, and use of records in the conduct of current business;

- Cooperation with the archivist at the National Archives and Records Administration (NARA) in applying standard procedures, and techniques designed to improve the management of records; and

- Promote the maintenance and security of records, and facilitate the segregation and disposal of records of temporary value.

- **The Freedom of Information Act (FOIA) of 1996, P.L. 104-231**, available at: https://www.justice.gov/oip/blog/foia-update-freedom-information-act-5-usc-sect-552-amended-public-law-no-104-231-110-stat . FOIA requires that government agencies disclose agency records unless that information is exempt from disclosure. FOIA provides two separate exemptions to protect privacy;

    - Exemption 6 authorizes agencies to withhold information contained in medical files and personnel records "the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;" and

    - Exemption 7 (C) protects collected in connection with a law enforcement investigation where disclosure "would constitute an unwarranted invasion of privacy."

- **The Children's Online Privacy Protection Act (COPPA) of 1998, P.L. 105-277,** available at: https://www.gpo.gov/fdsys/pkg/USCODE-2011-title15/html/USCODE-2011-title15-chap91.htm . Federal agencies were not covered by the COPPA statute itself. OMB OIRA, however, extended the COPPA requirements to federal agencies as a matter of federal policy. OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provision of the E-Government Act of 2002*, reinforced COPPA compliance by federal agencies and provided more detailed guidance. COPPA regulates the collection, use, and disclosure of information received from children under the age of 13 via the internet. It applies to any operator of a website who directs its material toward children under 13 and any general website operator who knows that it is collecting information from children under 13. It requires parental notice, consent, and review of information. Sites must post privacy policies and detail the personal information they collect and how they will use it. Website operators who violate COPPA could be liable for civil penalties.

- **The Health Insurance Portability and Accountability Act (HIPAA) of 1996, P.L. 104-191,** available at: https://www.congress.gov/104/plaws/publ191/PLAW-104publ191.pdf . Before HIPAA, health care providers routinely transferred patient medical information for reasons that had nothing to do with medical treatment or reimbursement for treatment. The HIPAA Privacy Rule applies to health information created or maintained by health care providers who participate in certain electronic transactions, health plans, and health care clearinghouses. The HIPAA Privacy Rule requires organizations to notify all patients in writing about the uses of their health information and to whom such information will be disclosed and to give patients full access to their own medical records to ensure the information in the records is only related to health care and not for marketing purposes. To ensure HIPAA compliance, organizations must establish privacy procedures, designate a privacy officer, and train

employees in privacy compliance. The HIPAA Privacy Rules applies to government-operated health plans and health care providers.

- **The Federal Information Security Modernization Act (FISMA) of 2002,** 44 U.S.C. § 3541, et seq. is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (P.L. 107–347, 116 Stat. 2899) available at: https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf . FISMA (2014) requires OMB to define the term "major incident"; directs agencies to notify Congress in the event of a "major incident"; and further instructs agencies to submit an annual report regarding major incidents to OMB. The Department of Homeland Security (DHS) is to assist the OMB Director in administering the implementation of agency information and security practices for federal information systems. DHS reports to Congress on an annual basis the effectiveness of Treasury information security policies and practices that include a summary of information security incidents, thresholds for reporting major information security incidents, a summary of the results of federal agency information system risk assessments, and agency compliance with data breach notification policies and procedures. The Government Accountability Office (GAO) and Comptroller General provide technical assistance to Treasury if needed.

- FISMA requires government agencies to develop and implement a robust security programs to protect and safeguard their information and information systems. The ASM/CPCLO with the CIO, the CISO, the Chief Security Officer, and other officials having privacy related responsibilities play an important role in identifying and mitigating risks to PII lost.

FISMA reports must include:

  - Threats and threat actors, vulnerabilities, and impacts;
  - Risk assessments of affected systems before, and the status of compliance of the systems at the time of, major incidents;
  - Detection, response, and remediation actions;
  - Total number of major incidents; and
  - Description of the number of individuals affected by, and the information exposed by major incidents involving a breach of PII.