EFFECTIVE DATE

(05-04-2022)

PURPOSE

(1) This transmits revised IRM 1.1.27, Organization and Staffing, Privacy, Governmental Liaison and Disclosure (PGLD).

MATERIAL CHANGES

(1) Removed duplicate Related Resources section.

(2) IRM 1.1.27.1(1) - Added authentication of taxpayer information to the mission statement.

(3) IRM 1.1.27.1(4) - Added disclosure and identity assurance-related activities to the policies, procedures and initiatives administered by PGLD.

(4) IRM 1.1.27.5 - Added IRM 10.10.1, IRS Electronic Signature (e-Signature) Program, to the table of related resources.

(5) 1.1.27.3.2(2)-Changed title of Chief Central Processing Unit to reflect new group name of GLDS Support Services.

(6) IRM 1.1.27.3.4(3) - Added the Area Manager and Chief, Safeguards Federal Review Team as new direct reports to the Associate Director, Safeguards.

(7) IRM 1.1.27.3.4(4) - Added the Chief, Strategy and Risk Team and moved the Chief, Safeguards Policy Team as direct reports to the new Area Manager position.

(8) IRM 1.1.27.4(3) - Updated text to indicate that there are now three suboffices within IA.

(9) IRM 1.1.27.4.1(1) - Updated activities performed by Identity Modernization

(10) IRM 1.1.27.4.2 - Updated suboffice name from Identity Strategies to Identity Authorization

(11) IRM 1.1.27.4.2(1) - Updated activities performed by Identity Authorization

(12) IRM 1.1.27.4.2(2) - Updated suboffice name to Identity Authorization

(13) IRM 1.1.27.4.3 - Added subsection for new suboffice Identity Innovations and its activities

(14) IRM 1.1.27.5(2) - Replaced OMB Memorandum M-12-18, Managing Government Records Directive, with OMB Memorandum M-19-21, Transition to Electronic Records, as the current authority for federal electronic records management requirements.

(15) IRM 1.1.27.5(4)(1) - Added reference to the Records Specialist Team and Records Advisory Group under RIM.

(16) IRM 1.1.27.6(3) - Updated wording describing data loss incidents to now be referred to as, ‘breaches’.

(17) IRM 1.1.27.6.2.1(2) - Updated wording to refer to ‘Incidents’ as ‘Breaches’ and to change ‘Victim Notifications’ to ‘notifications of potentially impacted individuals’.

(18) 1.1.27.7(1)&(4)-Changed ‘Program and Operations Support’ group name to ‘Operations and Program Support’.

(19) 1.1.27.7(1) - Added the two groups now under PPS.

(20) 1.1.27.7(4) - Added PPS’ Program and Operations Support responsibilities.

(21) 1.1.27.7(5) - Removed duties no longer performed by PPS or moved to a different location. Added Emergency Preparedness and TIGTA/GAO audit coordination.

(22) IRM Exhibit 1.1.27-2 - Clarified the definition of ‘Breach’. Changed ‘Data loss/breach’ to ‘Data Breach Incident’ and clarified that it covers PII. Removed the word ‘inadvertent’ under ‘Disclosure’. Changed the definition of ‘Incident Management’ to refer to the office within PGLD responsible for the process of managing data breaches involving the loss, theft, or inadvertent unauthorized disclosure of PII by the IRS.

(23) IRM Exhibit 1.1.27-5 - Replaced OMB M-12-18 with OMB M-19-21.

(24) Updated/fixed broken and outdated links.

EFFECT ON OTHER DOCUMENTS

None.

AUDIENCE

All divisions, functions, employees and contractors within the IRS.

Robert Choi
Chief Privacy Officer

1.1.27
Privacy, Governmental Liaison and Disclosure (PGLD)

Table of Contents

1.1.27.1
(05-04-2022)
Program Scope and Objectives

(1) **Mission:** To preserve and enhance public confidence by advocating for the appropriate protection, authentication, retention and disclosure of taxpayer information.

(2) **Purpose:** This IRM provides organizational information about Privacy, Governmental Liaison and Disclosure (PGLD).

(3) **Policy Owner:** PGLD, under the Deputy Commissioner for Operations Support (DCOS).

(4) **Program Owner:** PGLD administers privacy, disclosure, identity assurance and records policies, procedures, and initiatives and coordinates privacy, disclosure, identity assurance and records-related actions throughout the IRS. Each IRS organization is responsible for managing their privacy, disclosure, identity assurance and records requirements based on these Servicewide policies and procedures.

(5) **Contact Information**: To recommend changes to this IRM, see IRM 1.11.6.6, Providing Feedback About an IRM Section - Outside of Clearance, and send your suggestions to the PGLD Internal Management Documents (IMD) Coordinator at *PGLD IMD SPOC.

1.1.27.1.1
(05-07-2019)
Background

(1) PGLD has experienced numerous organizational changes affecting functional statements throughout its current structure. These organizational changes were made to:

- Leverage the workforce's specialized expertise
- Enhance accountability
- Ensure organizational efficiency, effectiveness, and customer service

(2) PGLD stood up as a separate functional business unit effective April 08, 2012. Major organizational changes include:

a. Merging Privacy, Information Protection and Data Security (PIPDS) and Governmental Liaison and Disclosure (GLD) into one unit effective June 19, 2011. Safeguards merged with GLD to become Governmental Liaison, Disclosure and Safeguards (GLDS) on December 12, 2013. PIPDS was formerly known as the Office of Privacy and Information Protection (before that, it was known as the Office of Privacy). GLD and Safeguards were both realigned from Communications, Liaison and Disclosure (CLD), Small Business and Self-Employed Division (SB/SE). They were merged to solidify the common bond of taxpayer and employee privacy information protection in full compliance with the Privacy Act of 1974, 5 U.S.C. 552a, as amended, coupled with the public right to information under the Freedom of Information Act (FOIA) of 1966, 5 U.S.C. 552 , as amended.
b. Creating a new Director level operation titled Governmental Liaison, Disclosure and Safeguards (GLDS) by combining the operations of the same names.
c. Restructuring GLDS offices of Data Services, Disclosure, Governmental Liaison, and Safeguards, by creating, closing, consolidating, and renaming subordinate units and realigning staff accordingly.
d. Creating a new Director level operation titled Strategic Support Office (SSO) and subsequently renamed Program and Planning Support (PPS). The PPS function was created to allow the centralization of support activities under a single point of ownership and accountability.

e. Realigning the Office of Employee Protection (OEP), Collection Policy, Small Business/Self-Employed Division, as a subordinate operating unit to Incident Management (retitled Incident Management and Employee Protection), under the Director, Privacy and Information Protection (PIP) effective February 24, 2014.
f. Migrating victim assistance aspects of identity theft to Wage & Investment (W&I) to centralize identity theft victim assistance under one leadership team and foster process and efficiency improvements.
g. Removing the operating units Identity Protection Technical and Identity Protection Analysis and forming Privacy Policy & Knowledge Management (PPKM), Privacy Compliance and Assurance, and Incident Management/Employee Protection (IM/OEP).
h. Renaming the Director level operation Privacy and Information Protection as Privacy Policy and Compliance (PPC).
i. Realigning the headquarters Records and Information Management (RIM) staff from the former Agency-Wide Shared Services' (AWSS) Real Estate and Facilities Management (now Facilities Management and Security Services (FMSS)) and Information Protection Projects (IPP) into one director-level office named Identity and Records Protection (IRP) effective August 10, 2014.
j. Moving GL's Congressional Affairs Program to Communications & Liaison (C&L) effective October 2, 2016.
k. Moving PGLD's in-house human resources and training staff to the Human Capital Office (HCO) effective February 21, 2016, and its in-house communications staff to C&L effective November 13, 2016.
l. Moving the Identity Assurance (IA) office from Online Services to PGLD on May 27, 2018.

1.1.27.1.2
(02-09-2018)
Terms/Definitions/ Acronyms

(1) See Exhibit 1.1.27-1 for commonly used PGLD acronyms and their definitions.

(2) See Exhibit 1.1.27-2 for commonly used PGLD terms and their definitions.

1.1.27.1.3
(05-07-2019)
Authorities

(1) See Exhibit 1.1.27-3 for significant GLDS authorities.

(2) See Exhibit 1.1.27-4 for significant IA authorities.

(3) See Exhibit 1.1.27-5 for significant IRP authorities.

(4) See Exhibit 1.1.27-6 for significant PPC authorities.

(5) See Exhibit 1.1.27-7 for PGLD's functional delegation order of succession.

1.1.27.1.4
(05-07-2019)
Roles and Responsibilities

(1) The Chief Privacy Officer reports directly to the DCOS and is responsible for ensuring that IRS strives to implement sound policies to protect taxpayer and employee privacy, and personal and sensitive information. Major responsibilities of the Chief Privacy Officer include:

- Establishing the IRS strategic direction regarding privacy protection, retention, and disclosure of taxpayer information
- Directing a core staff of privacy and security subject matter experts, both on the policy front and in information systems
- Promoting consistent implementation of privacy policies and legal record retention and disclosure requirements

- Reporting on IRS's activities to promote privacy protection and information security in accordance with National Institute of Standards and Technology (NIST) guidance
- Leading privacy policy development and providing expert advice on privacy, disclosure of taxpayer data, records management, execution of the FOIA, data protection and data sharing efforts across IRS and with external government partners
- Assessing and supporting plans to mitigate organizational risk from potential data breaches or unauthorized disclosures of IRS records
- Partnering with federal and state agencies to obtain data that supports business unit tax administration and compliance efforts
- Interpreting and administering of IRC 6103 to ensure confidentiality of tax records and the integrity of the tax administration systems
- Providing statutory oversight of IRS security and confidentiality requirements for federal and state agencies receiving tax return information
- Enhancing the privacy expertise and field presence of PGLD through knowledge management practices that expand the privacy knowledge and professional expertise of all PGLD employees

(2) There are five offices or functions within PGLD:

1. Governmental Liaison, Disclosure and Safeguards, or GLDS
2. Identity Assurance, or IA
3. Identity and Records Protection, or IRP
4. Privacy Policy and Compliance, or PPC
5. Program and Planning Support, or PPS

(3) The Director, GLDS reports to the Chief Privacy Officer and is responsible for interpreting and applying laws, regulations, policies, and guidance to provide access to IRS records and information, while ensuring protected information is appropriately disclosed. This includes ensuring the confidentiality of IRS information provided to Federal, state, and local agencies. Major responsibilities of the Director, GLDS include:

- Developing Servicewide policies, standards and guidelines for protecting taxpayer confidentiality and access to agency records under IRC 6103, the FOIA, and other disclosure related regulations and directives, and collaborating with Privacy Policy and Compliance with regard to confidentiality and access matters under the Privacy Act
- Establishing IRS strategic direction regarding data sharing, disclosure, and safeguards
- Examining disclosure and privacy-related legislation and other initiatives proposed by Congress, other agencies, and the public and formulating IRS's position to address the affect of such initiatives. When appropriate, identifies the need for new legislation to strengthen and support IRS's privacy and disclosure policies and to address future issues
- Collaborating with IRS Information Technology to support critical infrastructure improvements and enhance the protection of these systems from unauthorized access and exploitation and ensuring data exchange partners meet these same critical standards
- Overseeing the research, analysis, and data for timely FOIA responses and serves as the liaison to external customers and recipients to clarify and resolve FOIA issues
- Managing the safeguards program to ensure compliance with IRC Section 6103(p)(4) federal safeguarding requirements through the verifi-

cation and monitoring of agency risk mitigation plans, to reduce the threat of loss, breach, or misuse of Federal Tax Information (FTI) entrusted to external government agencies
- Managing relationships with Business and Functional Operating Divisions (BODs/FODs) to identify strategic priorities that may impact national policy in consideration of external stakeholders' needs
- Supporting the BOD/FOD strategic priorities by ensuring Servicewide compliance with statutory disclosure requirements through delivering awareness training, preparing BOD/FOD specific guidance, conducting Quality/Privacy Reviews, reviewing documents, and providing technical guidance
- Processing requests for disclosure of agency records, such as FOIA/Privacy Act, testimony requests and court orders from internal and external stakeholders and the public
- Reporting to Congress and Treasury on FOIA/Privacy Act end of year inventory and IRC 6103 accounting

(4) The Director, IA reports to the Chief Privacy Officer and provides IRS-wide leadership in developing and integrating authentication, authorization and access (A3) policies, including related frameworks and processes. Major responsibilities of the Director, IA include:

- Collaboratively guiding and supporting improved security, data protection, customer access, and enhanced identity assurance posture across IRS
- Establishing and maintaining a Servicewide A3 strategy by developing and maintaining IRS's strategic vision, identifying trends and best practices, and representing IRS's A3 interests with internal and external stakeholders
- Facilitating A3 policy decision-making through the development, approval, and use of policies and related A3 frameworks and processes across the IRS
- Developing and integrating A3 initiatives by coordinating their planning, prioritization, establishment, and integration across channels
- Ensuring consistent oversight of all A3-related processes, frameworks, and policy needs by providing identity assurance policy recommendations and guidance, including at the time of filing, online, face-to-face, telephone, fax, and written correspondence, while monitoring and coordinating the A3 portfolio to ensure its investments and initiatives are consistent with policies and are properly prioritized

(5) The Director, IRP reports to the Chief Privacy Officer and advises IRS senior leadership on the adequacy of documentation and creation and management of agency records, protection of taxpayer data from unauthorized access and by reducing Servicewide use of SSNs, keeping senior management informed on current and projected operational requirements, issues, legislative, and regulatory matters. Major responsibilities of the Director, IRP include:

- Formulating and overseeing the implementation of IRS policy and guidance for recordkeeping in accordance with the strategic plan, Congressional mandates, and the National Archives and Records Administration (NARA) regulations, standards and guidance
- Establishing strategic direction on records and information management for the full range of IRS activities

- Examining records and information management-related legislative and other initiatives proposed by Congress, Treasury, other agencies, and the public and formulating IRS's position to address the affect of such initiatives
- Serving as the IRS agency representative to the Office of Management and Budget (OMB), the Congress, NARA, and the press in matters relating to records management
- Establishing effective working relationships and communication with IRS business units in order to understand operational priorities and initiatives, and identify strategic and tactical issues related to records and information protection
- Ensuring that IRS employees are knowledgeable and kept current about records management principles and requirements, and that they receive records management training appropriate to their needs
- Working with Information Technology to build records management functionality into the enterprise architecture and to ensure all information systems incorporate records management functionality appropriate to the records/information assets they support
- Collaborating with the Enterprise Digitalization and Electronic Case Management Office to embed records requirements into its digitalization strategy
- Collaborating closely with the Department of the Treasury to implement and oversee records and information management processes and initiatives
- Collaborating Servicewide to identify opportunities to reduce or eliminate SSNs in tax administration
- Protecting taxpayer data through the Unauthorized Access (UNAX) program through policy, training, and communication
- Implementing the Controlled Unclassified Information (CUI) program

(6) The Director, PPC reports to the Chief Privacy Officer and is responsible for ensuring the IRS implements sound policies designed to protect the identity and privacy of employees and taxpayers. Major responsibilities of the Director, PPC include:

- Promoting consistent implementation of privacy policies and reporting on IRS' activities to promote privacy protection
- Establishing strategic direction on privacy for the full range of IRS activities, including data protection strategies such as designing privacy into systems and business processes and evaluating the compliance and effectiveness of these strategies
- Examining privacy-related legislative and other initiatives proposed by Congress, other agencies, and the public and formulating IRS's position to address the affect of such initiatives. When appropriate, identifies the need for new legislation to strengthen and support IRS's privacy policies and to address future issues
- Developing a training curriculum regarding privacy for IRS executives, managers, and employees, and contractors who receive taxpayer information. Develops and delivers a training curriculum to ensure a staff of highly skilled privacy professionals. Promotes internal and external awareness of IRS' commitment to privacy and information protection
- Collaborating closely with the Department of the Treasury to implement and oversee privacy and data protection processes and initiatives
- Collaborating with IRS Information Technology to ensure that privacy functionality is included in system design and support critical infrastruc-

ture improvements to enhance the protection of these systems from unauthorized access and exploitation
- Overseeing an incident response plan for data breaches through risk evaluation and measured response
- Ensuring IRS's Privacy and Civil Liberties Impact Assessment (PCLIA) process effectively meets government-wide standards and goals
- Effectively administering programs tracking potentially dangerous taxpayers and those taxpayers that should be approached with caution
- Overseeing the IRS Pseudonym Program
- Leading the IRS Privacy Council to identify emerging issues and develop policies to mitigate privacy risks

(7) The Director, PPS reports to the Chief Privacy Officer and:

- Manages budget and technology issues for PGLD
- Coordinates internal/external communications on privacy issues related to tax administration
- Coordinates PGLD hiring
- Monitors PGLD TIGTA/GAO audits and responses
- Supports the Internal Management Document (IMD) program
- Provides facilities planning and oversight
- Institutes contract procurement and oversight
- Conducts emergency preparedness exercises
- Sponsors PGLD-wide CPE

(8) PGLD's current organization chart is available at *https://portal.ds.irsnet.gov/sites/PGLD/ap/PGLD-Org-Chart.pptx* .

1.1.27.1.5
(05-04-2022)
Related Resources

(1) The Privacy, Governmental Liaison and Disclosure intranet home page can be found at: *Disclosure and Privacy Knowledge Base*.

(2) The following table lists the primary IRM sources of information on PGLD programs:

IRM	Title	Contains
IRM 11.3.1	Introduction to Disclosure	The instructions, guidelines, and procedures necessary to fulfill our obligations under the disclosure laws
IRM 11.4.1	Governmental Liaison Operations	The operating procedures, policy and guidelines for Governmental Liaison employees and managers
IRM 11.4.2	Office of Governmental Liaison, Data Exchange Program	Information on the program which shares federal tax data with state agencies for the purposes of state tax administration
IRM 11.3.36	Safeguard Review Program	Information and procedural guidance for Office of Safeguards staff for ensuring that outside agencies and their contractors maintain adequate safeguards to protect the federal tax data received from IRS

IRM	Title	Contains
IRM 1.15.1	The Records and Information Management Program	Information, including the responsibilities of all IRS employees, for complying with the requirements of maintaining and managing IRS's records and information
IRM 10.5.1	Privacy and Information Protection, Privacy Policy	Information on the Privacy Policy and Compliance office and the uniform policies used by IRS employees and organizations to carry out their privacy responsibilities
IRM 10.5.4	Incident Management Program	Information on incident management guidelines for all divisions, functional units, managers, employees, and contractors within the IRS
IRM 10.5.7	Use of Pseudonyms by IRS Employees	Information, guidance, and procedures for all Service managers and employees on the use of pseudonyms by IRS employees in compliance with Section 3706 of the IRS Restructuring and Reform Act of 1998 (RRA 98) and from the Pseudonym Memorandum of Understanding (MOU) signed by the IRS and NTEU on April 10, 2013
IRM 10.10.1	IRS Electronic Signature (e-Signature) Program	The procedures and policies for implementing e-Signature on external, taxpayer related forms, documents and applications
IRM 10.10.2	Authentication Risk Assessments in Non-Digital Channels	Establishes policy for assessing and documenting risk in authentication processes over non-digital customer contact channels (telephone/voice, in-person, and correspondence) where sensitive information is exchanged with individuals. Provides link to the Form 15295, Non-Digital Channel Authentication Risk Assessment (NDARA) and establishes three-year frequency for completing NDARA
IRM 25.4.1	Potentially Dangerous Taxpayer	Procedures and guidelines for the Potentially Dangerous Taxpayer (PDT) program
IRM 25.4.2	Caution Upon Contact Taxpayer	Procedures and guidelines for the "Caution Upon Contact" Taxpayer program

1.1.27.2
(02-09-2018)
Privacy, Governmental Liaison and Disclosure

(1) PGLD is responsible for safeguarding and protecting sensitive taxpayer and employee information while promoting government transparency and accountability through better access to government information.

(2) PGLD is geographically dispersed across the U.S. with business operations sharing a commitment to privacy, records and information management, and data and employee protection.

(3) To accomplish its mission, PGLD:

- Preserves and enhances public confidence by advocating for the protection and proper use of sensitive information
- Protects the sensitive information and privacy of taxpayers and IRS employees
- Reduces vulnerabilities for identity theft, which promotes identity protection
- Ensures IRS records, including those containing PII, are managed appropriately
- Works with all IRS operations to ensure only authorized disclosures and data sharing
- Partners with federal, state, and local governmental agencies to promote privacy and protect FTI
- Exchanges FTI as authorized by law with external stakeholders
- Safeguards FTI held by data exchange partners
- Protects IRS employees through the use of cautionary indicators on appropriate taxpayer accounts
- Leads development and integration of IRS authentication, authorization and access (A3) policies

(4) The following subsections provide details about the five PGLD offices listed in IRM 1.1.27.1.4(2).

1.1.27.3 (02-09-2018) Governmental Liaison, Disclosure and Safeguards

(1) Governmental Liaison, Disclosure and Safeguards (GLDS) provides timely public access to IRS records in accordance with applicable disclosure laws; strengthens America's tax system by partnering with federal, state, and local governmental agencies; and ensures IRS employees and external partners protect confidential tax information.

(2) GLDS is geographically dispersed throughout the country providing disclosure guidance and support to all IRS employees while interacting with federal, state, and local agencies on data exchanges and other issues.

(3) There are four offices within GLDS:

1. Governmental Liaison
2. Disclosure
3. Safeguards
4. Data Services

(4) GLDS's offices work collaboratively:

- **Disclosure** serves as the taxpayer data gatekeeper and makes IRC 6103 "need and use" determinations regarding what IRS should and should not disclose
- Working with Disclosure and Safeguards, **Governmental Liaison** (GL) helps determine data needs and uses and manages relationships between IRS and a diverse assortment of approximately 300 external agencies
- After Disclosure and GL have determined the data needs, **Data Services** defines and develops the necessary extracts
- **Safeguards** protects the data by verifying the external agencies are using and safeguarding it appropriately

(5) To accomplish its mission, GLDS:

- Provides timely public access to IRS records in accordance with applicable disclosure laws
- Strengthens America's tax system by partnering with federal, state, and local governmental agencies to increase compliance, enforcement, and service to taxpayers
- Ensures IRS employees and external partners protect confidential tax and privacy information
- Provides oversight and outreach to more than 300 federal, state, and local agencies receiving FTI

1.1.27.3.1
(02-09-2018)
Governmental Liaison

(1) Governmental Liaison (GL) is the primary point of contact with federal, state, and local government agencies and partners with them to obtain and exchange data to support IRS efforts related to identity theft, tax compliance, and refund fraud. Cooperation between IRS and other government agencies helps achieve IRS's strategic goals of improved voluntary compliance, increased efficiency of tax administration, and reduced taxpayer burden.

(2) GL facilitates agreements to exchange data and tax and non-tax information with federal, state, and local governmental agencies. These exchanges augment IRS's tax compliance systems by helping IRS better identify where to apply compliance resources, thereby helping to reduce the tax gap, reduce taxpayer burden and optimize use of resources. GL's three partnering programs are:

a. **Fed/State:** Facilitates tax information exchanges through joint tax administration relationships between the IRS and state taxing authorities, such as departments of revenue and state workforce agencies
b. **Federal Intergovernmental Program (FIP):** Strengthens existing partnerships and develops potential reciprocal arrangements across the federal government to enhance effective tax administration and good government
c. **Municipal Agency Partnering Program (MAPP):** Focuses on partnering opportunities with municipalities and other local agencies and offices - sometimes referred to as "non-traditional" agencies

(3) The Associate Director, Governmental Liaison, reports to the Director, GLDS, and oversees the GL program. The following GL managers and offices report to the Associate Director:

- Chiefs, Governmental Liaison - Field East and West
- Chief, Governmental Liaison Headquarters Policy

(4) See IRM 11.4.1, Governmental Liaison Operations, for more information.

1.1.27.3.2
(02-09-2018)
Data Services

(1) Data Services provides support to GL, Safeguards and Disclosure programs through a variety of information technology and data initiatives, including:

- Managing the Governmental Liaison Data Exchange Program (GLDEP), including computation, billing, and receivable process for reimbursable fees
- Managing Disclosure and Safeguards inventory controls and producing statistical management reports and measures
- Working with NARA to obtain documents from Federal Records Centers (FRCs)

- Performing quality review of Disclosure casework and providing feedback

(2) The Associate Director, Data Services, reports to the Director, GLDS, and oversees the Data Services program. The following Data Services managers and offices report to the Associate Director:

- Chief, GLDS Support Services
- Chief, Data Exchange and Quality Initiative
- Chief, Technical Support and Analysis

(3) See IRM 11.4.2, Governmental Liaison Data Exchange Program (GLDEP), for more information.

1.1.27.3.3
(05-04-2022)
Disclosure

(1) Disclosure provides Servicewide guidance to ensures the right information is released to the right persons at the right time by developing policy standards and guidelines for the protection of taxpayer confidentiality and access to IRS records under the Internal Revenue Code 26 USC 6103, the FOIA (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Disclosure helps IRS employees comply with statutory requirements through awareness of access and authentication requirements, disclosure articles and other training materials, quality reviews, document clearances and technical assistance. Disclosure program responsibilities and casework include:

- Processing requests for access to IRS records through the FOIA, Privacy Act, and access provisions of IRC 6103
- Requests and demands for testimony and production of IRS records and information in judicial and administrative proceedings
- Authoring over two dozen IRMs on various disclosure policy topics
- Providing specialized review for all IRS business units' IRMs and training materials containing content designated as Official Use Only (OUO)
- Providing a help desk and awareness training for all IRS employees

(2) The Associate Director, Disclosure, reports to the Director, GLDS, and oversees the Disclosure program. The following Disclosure managers and offices report to the Associate Director:

- Area Manager, Disclosure Areas - East and West
- Chief, Disclosure Policy and Program Operations

(3) See IRM 11.3.1, Introduction to Disclosure, for more information.

1.1.27.3.4
(05-04-2022)
Safeguards

(1) Safeguards is responsible for ensuring that outside agencies and their contractors with access to federal tax returns and return information, collectively referred to as Federal Tax Information (FTI), maintain proper safeguards to adequately protect the data. These agencies receiving return information must protect the confidentiality of return information and are periodically reviewed by Safeguards personnel to ensure they meet the safeguarding requirements of IRC 6103(p)(4). These requirements include:

- Employee awareness programs
- Computer security
- Secure storage
- Proper disposal

(2) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies, contains the specific requirements for those receiving FTI.

(3) The Associate Director, Safeguards, reports to the Director, GLDS, and oversees the Safeguards program. The following Safeguards managers and offices report directly to the Associate Director:

- Area Manager
- Chiefs, Safeguards Review Teams 1 and 2
- Chief, Safeguards Federal Review Team

(4) The following Safeguards managers and offices report directly to the Area Manager:

- Chief, Safeguards Policy Team
- Chief, Strategy and Risk Team

(5) See IRM 11.3.36, Safeguards Review Program, for more information.

1.1.27.4
(05-04-2022)
Identity Assurance

(1) The Identity Assurance (IA) mission is to promote the maturity and innovation of authentication, authorization and access (A3) enterprise capabilities, policies and processes to support the secure delivery of data and services across customer contact channels.

(2) IA's role is to strengthen the IRS authentication posture by enhancing visibility and coordination for identity proofing, authentication, authorization, and access (A3) strategies, processes and capabilities. IA accomplishes this by leveraging, coordinating and integrating approaches to foster enterprise strategies.

(3) There are three offices within IA:

1. Identity Modernization (IM)
2. Identity Authorization (IAz)
3. Identity Innovations (II)

(4) To accomplish its mission, IA:

- Stewards (A3) strategies by: facilitating collaborative decision-making; conducting analytics; and coordinating with A3 stakeholders to identify and implement solutions
- Develops and champions A3 strategies to mature and strengthen capabilities across customer delivery channels (digital, phone, in-person, correspondence, point of filing)
- Serves as steward for enterprise e-Signature Services, setting policy and business strategy for Servicewide capabilities
- Conducts analytics and monitoring for A3 processes, such as user identity proofing and authenticating through the Secure Access online authentication platform
- Brings organizational awareness and subject matter expertise to A3-related stakeholder efforts and empowers business owners to carry out their projects
- Guides integration of identity assurance policy decisions for compliance and risk management
- Ensures compliance with authentication and authorization solutions with Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) guidance

- Advises and guides the identification, establishment, integration and ongoing refinement of new or existing A3 capabilities and processes
- Acts as a Servicewide expert for identity assurance related policies, practices, risks, and initiatives regardless of functional origination or process ownership

1.1.27.4.1
(05-04-2022)
Identity Modernization

(1) Identity Modernization (IM) activities include:

- Coordinating the development of processes and analyses for A3 in accordance with government standards and guidance
- Overseeing and maintaining the online identity proofing and authentication requirements for Secure Access
- Leading the development of Secure Access Digital Identity (SADI) to ensure compliance with Office of Management and Budget (OMB) Memorandum 19-17 and the National Institute of Standards and Technology (NIST) Special Publication 800-63-3 Digital Identity Guidelines
- Coordinating servicewide and cross-agency efforts for identity proofing capabilities with Credential Service Providers (CSP)
- Overseeing the migration of online applications from Secure Access to SADI

(2) The Associate Director, Identity Modernization, reports to the Director, IA and oversees IM programs.

(3) See IRM 10.10.2, Authentication Risk Assessments in Non-Digital Channels, for more information.

1.1.27.4.2
(05-04-2022)
Identity Authorization

(1) Identity Authorization (IAz) activities include:

- Facilitating the evaluation of identity assurance efforts and policy decisions to mitigate risk, while also focusing on cost, time-to-market, and taxpayer usability
- Identifying trends, best practices, lessons learned, etc., and shares information in support of authentication, authorization, and access (A3) efforts
- Monitoring and coordinating the A3 portfolio ensuring A3 investments and initiatives are consistent with policies and are prioritized and delivered against the most critical opportunities, gaps, and program/initiative risks and/or emerging priorities
- Leading the e-Signature Program by providing policy guidance and business rules to prepare for implementation of the e-Signature solution
- Overseeing the IRS Identity Assurance and Authorization Strategies to identify priorities to be integrated into the Service's Business and IT Strategic Plans
- Managing contracts and funding needs to support IA

(2) The Associate Director, Identity Authorization, reports to the Director, IA and oversees IAz programs.

(3) See IRM 10.10.1, IRS Electronic Signature (e-Signature) Program, for more information.

1.1.27.4.3
(05-04-2022)
Identity Innovations

(1) Identity Innovations (II) activities include:

- Developing and collecting performance metrics for A3
- Coordinating the development of processes and analyses for A3 in accordance with government standards and guidance
- Leading omni-channel (phone, in-person, and correspondence) authentication and authorization efforts by identifying opportunities to increase security in coordination with A3 strategies and stakeholder plans
- Coordinating servicewide and cross-agency efforts to identify and implement Innovation Studies that support A3 strategies
- Conducting data analytics, monitoring, and identifying process improvements

(2) The Associate Director, Identity Innovations, reports to the Director, IA and oversees II programs.

(3) See IRM 10.10.2 Authentication Risk Assessments in Non-Digital Channels for more information.

1.1.27.5
(05-04-2022)
Identity and Records Protection

(1) Identity and Records Protection (IRP) provides Servicewide records management expertise and protection of taxpayer and employee identities through the Unauthorized Access (UNAX) and Social Security Number Elimination and Reduction (SSN ER) programs. IRP also leads Servicewide efforts to implement Controlled Unclassified Information (CUI).

(2) IRP leads Servicewide efforts to implement the federal electronic records management requirements of OMB Memorandum M-19-21, Transition to Electronic Records, and address recordkeeping requirements for:

- Email
- Social media
- Electronic messaging, e.g.,Skype, Webex
- The future vision for taxpayer digital communications

(3) IRP also promotes coordinated awareness, communication and educational efforts designed to reinforce understanding of:

- What is and what is not a federal record
- Consequences of not complying with Federal Records Act requirements
- Individual employees' and IRS's joint obligation to manage records appropriately

(4) There are two offices within IRP:

1. Records and Information Management, or RIM, comprised of a Records Specialist Team and a Separating Employee Clearance (SEC) Records Advisors group
2. Information Protection Projects, or IPP

(5) To accomplish its mission, IRP:

- Provides guidance and oversees functions related to recorded IRS information throughout the life cycle of a document
- Protects taxpayer data by managing the Unauthorized Access (UNAX) and Social Security Number Elimination and Reduction (SSNER) programs

- Provides oversight for the Controlled Unclassified Information (CUI) Program which seeks to standardize the way the Executive branch handles unclassified information. The authority of CUI comes from Executive Order 13556, 32 CFR 2002 and the CUI Registry, which set forth the parameters and requirements for implementing, designating, safeguarding, disseminating, marking, destructing, and decontrolling CUI.

1.1.27.5.1
(02-09-2018)
Records and Information Management

(1) Records and Information Management (RIM) helps business units apply sound management practices and techniques throughout the life cycle of all IRS records by:

- Planning, developing and promoting IRS records management policy standards, procedures and guidelines that provide for effective controls over IRS records and information - see IRM 1.15, Records and Information Management, series
- Working with NARA, Department of the Treasury, other governmental agencies and private industry on all records and information management matters affecting IRS
- Promoting awareness and understanding of RIM principles to all IRS employees
- Providing oversight and monitoring of IRS electronic records dispositions
- Providing technical guidance and assistance to business units in fostering the mission of the RIM program
- Overseeing and monitoring all off-site NARA Records Center Program services, including the off-site storage of IRS records

(2) Servicewide records specialists and business unit information resource coordinators have oversight responsibilities for implementing an effective RIM program nationwide. They assist the IRS Records Officer by:

- Supporting and providing assistance to designated information resource coordinators assigned to the IRS functional organizations
- Participating in local area or business function studies and providing recommendations to improve the RIM program
- Resolving local RIM matters
- Elevating Servicewide RIM issues to the IRS Records Officer
- Serving as a liaison with NARA, FRCs, and IRS business units on all records disposition matters
- Tracking and monitoring records requests to and from FRCs
- Assisting customers with maintaining records control schedules, including the identification of new or revised authorities for electronic records

(3) The Associate Director, Records and Information Management, reports to the Director, IRP, and oversees the RIM program. The following managers and officers report to the Associate Director:

- Chief, Records Specialist Team
- Supervisory Management Analyst, SEC Records Advisors
- IRS Records Officer

(4) See IRM 1.15.1, The Records and Information Management Program, for more information.

1.1.27.5.2
(02-09-2018)
Information Protection Projects

(1) Information Protection Projects (IPP) manages the Servicewide Unauthorized Access to Taxpayer Accounts (UNAX), Social Security Number Elimination and Reduction (SSNER), and Controlled Unclassified Information (CUI) programs.

(2) The Associate Director, Information Protection Projects, reports to the Director, IRP, and oversees the IPP office.

(3) See IRM 10.5.5, IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance and Requirements, and IRM 10.5.1.7.18, Privacy and Information Protection, Privacy Policy, Social Security Number Elimination and Reduction (SSN ER). .

1.1.27.6
(05-04-2022)
Privacy Policy and Compliance

(1) Privacy Policy and Compliance (PPC) promotes and integrates privacy into business practices, behaviors and technology solutions. PPC serves as IRS's primary office for:

- Privacy-related inquiries
- eAuthentication policy
- Personally Identifiable Information (PII) in email guidance
- Federal Information Security Management Act (FISMA) compliance
- General protections for sensitive information

(2) There are three offices within PPC:

- Incident Management and Employee Protection (IMEP)
- Privacy Compliance and Assurance (PCA), which includes the sub-office of Privacy Review
- Privacy Policy and Knowledge Management (PPKM)

(3) To accomplish its mission, PPC:

- Manages data breaches involving the loss, theft or inadvertent unauthorized disclosure of SBU data
- Ensures data breaches are investigated, analyzed and resolved
- Oversees the Data Breach Notification process for notifying impacted taxpayers and employees
- Issues privacy policy to promote privacy protection, compliance and awareness
- Administers programs tracking potentially dangerous taxpayers and those taxpayers who should be approached with caution
- Manages breaches involving intentional accesses and disclosures resulting in an administrative determination of disciplinary or adverse action against an employee
- Administers and manages the IRS Pseudonym Program

(4) See IRM 10.5.1, Privacy and Information Protection, Privacy Policy, for more information.

1.1.27.6.1
(02-09-2018)
Privacy Compliance and Assurance

(1) PCA processes Privacy and Civil Liberties Impact Assessments (PCLIAs) for IRS's:

- Computer systems
- SharePoint sites containing PII
- Social media
- Surveys

(2) A PCLIA ensures program and project managers, system owners, and developers have consciously incorporated privacy and civil liberties protections throughout the entire life cycle of a system.

(3) PCA also conducts business PII risk assessment reviews, which focus on the areas of greatest risk to the IRS for data loss or disclosure. The reviews identify risks and provide business units with mitigation strategies. PCA also is the parent organization for Privacy Review.

(4) The Associate Director, Privacy Compliance and Assurance, reports to the Director, PPC and oversees the PCA program.

(5) See IRM 10.5.2, Privacy and Information Protection, Privacy Compliance and Assurance, for more information.

1.1.27.6.1.1
(02-09-2018)
Privacy Review

(1) Privacy Review processes Privacy and Civil Liberties Impact Assessments (PCLIAs) for IRS's:

- Computer systems
- SharePoint sites containing PII
- Social media
- Surveys

(2) A PCLIA ensures program and project managers, system owners, and developers have consciously incorporated privacy and civil liberties protections throughout the entire life cycle of a system.

(3) The Chief, Privacy Review, reports to the Associate Director.

1.1.27.6.2
(02-09-2018)
Incident Management and Employee Protection

(1) Incident Management and Employee Protection (IMEP) is comprised of the Incident Management office, and the Office of Employee Protection.

(2) The Associate Director, Incident Management and Employee Protection, reports to the Director, PPC, and oversees the IMEP program.

1.1.27.6.2.1
(05-07-2019)
Incident Management

(1) Incident Management administers and manages agency program requirements for ensuring incidents involving the following are investigated, analyzed and resolved:

- The loss or theft of an IRS asset containing SBU data
- The loss, theft or disclosure of PII (data loss incidents)

(2) IM activities include:

- Data Breach intake and risk assessment
- Notification of potentially impacted individuals
- Follow-up and support
- Functional interaction and support related to incident and breach data
- Facilitating the data loss prevention working group
- Maintaining the Data Breach Response Playbook
- Managing the Servicewide pseudonym program

(3) See IRM 10.5.4, Privacy and Information Protection, Incident Management Program, and IRM 10.5.7, Use of Pseudonyms by IRS Employees, for more information.

1.1.27.6.2.2
(02-09-2018)
Office of Employee Protection

(1) The Office of Employee Protection (OEP) tracks potentially dangerous taxpayers and those taxpayers who should be approached with caution through two main programs:

a. Potentially Dangerous Taxpayer (PDT)
b. Caution Upon Contact (CAU)

(2) OEP Mission: To effectively administer programs tracking potentially dangerous taxpayers and those taxpayers that should be approached with caution.

(3) OEP Vision: OEP is dedicated to top quality customer service by:

- Committing to continual process improvement
- Actively seeking customer feedback and acting upon it
- Periodically providing program development awareness and trend analyses
- Conducting quarterly program area reviews

(4) The Chief, Office of Employee Protection, reports to the Associate Director, IMEP, and oversees the OEP program.

(5) See IRM 25.4.1, Employee Protection, Potentially Dangerous Taxpayer, and IRM 25.4.2, Caution Upon Contact Taxpayer, for more information.

1.1.27.6.3
(02-09-2018)
Privacy Policy and Knowledge Management

(1) Privacy Policy and Knowledge Management (PPKM) engages in multiple initiatives to implement directives from the Office of Management and Budget (OMB), and both legislation and directives from:

- Privacy Act (1974)
- Computer Matching and Privacy Protection Act (1988)
- Freedom of Information Act (1974)
- IRC 6103
- The Taxpayer Browsing Protection Act (1997) (UNAX)
- Federal Information Security Management Act of 2014 (FISMA)
- E-Government Act (2002)
- Health Insurance Portability and Accountability Act (1996) (HIPAA)

(2) PPKM resolves privacy-related inquiries and provides policy and procedural guidance for:

- Email containing PII
- FISMA compliance
- General protections for sensitive information

(3) PPKM leads the PGLD:

- IRS Privacy Council (and corresponding Privacy Advisory Group)
- PGLD Policy Board

(4) The Associate Director, Privacy Policy and Knowledge Management, reports to the Director, PPC, and oversees the PPKM program.

(5) See IRM 10.5.1, Privacy and Information Protection, Privacy Policy, for more information.

1.1.27.7
(05-04-2022)
Program and Planning Support

(1) Program and Planning Support (PPS) provides guidance, oversight and coordination for PGLD organizational matters, and serves as liaison for HCO, training and communications efforts. PPS includes the Financial Planning and Technology Support (FP&TS) and Operations and Program Support (O&PS) groups.

(2) PPS's budget and contract management responsibilities include:

- Managing resources across multiple appropriations (Operations Support, Affordable Care Act, Taxpayer Services and Reimbursables)
- Providing contracting guidance and contract management services
- Managing the purchase card program

(3) PPS's Business Systems Planning responsibilities include coordinating:

- Operation Support (OS) Get Services Tickets through Knowledge Incident/Problem Service and Asset Management (KISAM)
- Unified Work Requests
- IT Budget Funding Process
- FISMA Testing
- Wireless devices
- IT initiated enterprise wide projects

(4) PPS's Operations and Program Support responsibilities include:

- Hiring, training and retention activities
- Coordination of PGLD's Internal Management Document (IMD) and non-IRM publishing programs
- Facilities planning and oversight
- Performance management and strategic planning

(5) PPS is also involved in:

- Coordination of all IT-initiated Servicewide projects for PGLD
- SharePoint management and oversight
- Emergency preparedness
- TIGTA/GAO audit coordination

(6) The Chief, Financial Planning and Technical Support, and the Chief, Operations and Program Support, report to the Director, PPS.

Exhibit 1.1.27-1 (05-07-2019)
Acronyms

The following table contains definitions for the acronyms used in this IRM:

Acronym	Definition
A3	Authentication, authorization and access
CAP	Corrective Action Plan
CAU	Caution Upon Contact
CUI	Controlled Unclassified Information
DCOS	Deputy Commissioner for Operations Support
ESIGN	Electronic Signatures in Global and National Commerce Act
FIP	Federal Intergovernmental Program
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FTI	Federal Tax Information
FRC	Federal Records Center
GL	Governmental Liaison
GLDEP	Governmental Liaison Data Exchange Program
GLDS	Governmental Liaison, Disclosure and Safeguards
GPEA	Government Paperwork Elimination Act
IA	Identity Assurance
IMEP	Incident Management and Employee Protection
IPP	Information Protection Projects
IRP	Identity and Records Protection
MAPP	Municipal Agency Partnering Program
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OEP	Office of Employee Protection
OMB	Office of Management and Budget
OUO	Official Use Only
PCA	Privacy Compliance and Assurance
PCLIA	Privacy and Civil Liberties Impact Assessment
PDT	Potentially Dangerous Taxpayer
PGLD	Privacy, Governmental Liaison and Disclosure

Exhibit 1.1.27-1 (Cont. 1) (05-07-2019)
Acronyms

Acronym	Definition
PIAMS	Privacy Impact Assessment Management System
PII	Personally Identifiable Information
PPC	Privacy Policy and Compliance
PPS	Programming and Planning Support
PPKM	Privacy Policy and Knowledge Management
RMSA	Record Management Self-Assessment
RIM	Records and Information Management
SAO	Senior Agency Official
SRR	Safeguards Review Report
SSNER	Social Security Number Elimination and Reduction
UNAX	Unauthorized Access [to taxpayer accounts]

Exhibit 1.1.27-2 (05-04-2022)
Defined Terms

The following table contains definitions for the significant terms used in this IRM:

Term	Definition
Access	The right or permission to view or receive information. Access by an individual is determined by sensitivity of the data and authority to receive it.
Authorization	The process of establishing the rights or privileges of users to interact with the IRS on behalf of themselves, other individuals, businesses, or other organizations and allowing those users to exercise rights that have been previously established.
Authentication	The process IRS employees should use to make sure that the person to whom returns or return information are released has authorized access.
Breach	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.
Civil liberties	The basic rights guaranteed to individual citizens by law.
Data Breach Incident	An incident involving a loss, theft, breach, or inadvertent unauthorized disclosure of PII.
Disclosure	The making known to any person, in any manner, a return or return information. For example, confirming whether a tax return is on file or not (i.e., fact of filing) is a disclosure.
Federal tax information	Any return or return information protected by IRC 6103 confidentiality whether received from the IRS, or secondary source such as the Social Security Administration, etc. FTI includes any information created by the recipient that is derived from return or return information.
Incident Management (IM)	Incident Management (IM) refers to the Office within Privacy, Government Liaison and Disclosure responsible for the process of managing data breaches involving the loss, theft, or inadvertent unauthorized disclosure of PII by the IRS.
Loss	Any event where an item is misplaced and/or neither the official owner nor the intended recipient has possession of the item in the expected time frame.
Non-record	Work-related documents that do not qualify as records such as duplicate copies, convenient/reference copies, and stocks of publications.

Exhibit 1.1.27-2 (Cont. 1) (05-04-2022)
Defined Terms

Term	Definition
Personally Identifiable Information	Any information that: a. can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and b. is linked or linkable to an individual, such as medical, educational, financial, and employment information.
Privacy	Privacy at the IRS reflects the combined effort of the IRS, its personnel, and individual taxpayers to protect, control, and exercise rights over the collection, use, retention, dissemination, and disposal of personal information.
Record	All recorded information such as books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them. See 44 U.S.C. 3301.
Return	Any tax or information return, estimated tax declaration, or refund claim - including amendments, supplements, supporting schedules, attachments, or lists - required by or permitted under the IRC and filed with the IRS by, on behalf of, or with respect to any person or entity.
Return information	Generally any information collected or generated by the IRS with regard to any person's liability or possible liability under the IRC. IRC 6103(b)(2)(A) defines return information very broadly.
Risk	The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Safeguard	Any action, device, procedure, technique, or other measure that reduces a system's vulnerability to a threat.
Unauthorized access	The willful unauthorized access and/or inspection of tax returns and return information.
Theft	An asset, electronic or hardcopy, thought or known to have been taken without permission from the individual who is responsible for the asset.

Exhibit 1.1.27-2 (Cont. 2) (05-04-2022)
Defined Terms

Term	Definition
Unauthorized disclosure	An unlawful disclosure of any return or return information to an individual not authorized to receive it or for a purpose not authorized by Title 26. A willful unauthorized disclosure is a felony.

Exhibit 1.1.27-3 (02-09-2018)
Governmental Liaison, Disclosure and Safeguards Authorities

The following table reflects the authorities and their general descriptions for GLDS activities:

Authority	Description
IRC 6103	Confidentiality and disclosure of returns and return information
IRC 7213	Unauthorized disclosure of information
IRC 7213A	Unauthorized inspection of returns or return information
5 U.S.C. 552	The Freedom of Information Act (FOIA)
5 U.S.C. 552a	The Privacy Act
Policy Statement 11-13	IRM 1.2.1.11.1, Freedom of Information Act Requests
Treasury Directive 25-05	Provides policy and assigns responsibilities for carrying out the requirements of the FOIA
NIST Special Publication 800-53 Rev. 5	Security and Privacy Controls for Information Systems and Organizations

Exhibit 1.1.27-4 (05-07-2019)
Identity Assurance Authorities

The following table reflects the authorities and their general descriptions for IA activities:

Authority	Description
IRC 6061(b)	Signing of Returns and Other Documents - Electronic Signatures
NIST Special Publication 800-53 Rev. 5, Appendix E	Security and Privacy Controls for Information Systems and Organizations -- Assurance and Trustworthiness, Measures of Confidence for Information Systems
NIST Special Publication 800-63-3	Digital Identity Guidelines
Public Law 105-277, Title XVII	Government Paperwork Elimination Act (GPEA) 1703 and 1705
Public Law 106-229	Electronic Signatures in Global and National Commerce Act (ESIGN)
Uniform Electronic Transactions Act	Uniform state-level law finalized by the National Conference of Commissioners on Uniform State Laws in 1999 and subsequently adopted by 47 states. May be applicable to commercial, consumer, or governmental affairs transactions involving federal organizations in certain cases
Public Law No: 115-336, *21st Century Integrated Digital Experience Act (IDEA Act)*	Requires executive agencies to submit a “plan to accelerate the use of electronic signature standards established under the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq)”
Office of Management and Budget (OMB) Memorandum (M) 19-17	Sets forth the Federal Government’s Identity, Credential, and Access Management (ICAM) policy

Exhibit 1.1.27-5 (05-04-2022)
Identity and Records Protection Authorities

The following table reflects the authorities and their general descriptions for IRP activities:

Authority	Description
44 U.S.C. Chapter 21	National Archives and Records Administration (NARA)
44 U.S.C. Chapter 29	Records Management by the Archivist of the United States
44 U.S.C. Chapter 31	Records Management by Federal Agencies
44 U.S.C. Chapter 33	Disposal of Records
36 CFR Chapter XII, Subpart B - Part 1222	Agency Recordkeeping Requirements
36 CFR Chapter XII, Subpart B - Part 1235	Transfer of Records to the National Archives of the United States
36 CFR Chapter XII, Subpart B - Part 1236	Electronic Records Management
OMB M-19-21	Transition to Electronic Records
NARA Bulletin 2012-02	Guidance on Managing Content on Shared Drives
NARA Bulletin 2014-04	Revised Format Guidance for the Transfer of Permanent Electronic Records
NARA Bulletin 2015-04	Metadata Guidance for the Transfer of Permanent Electronic Records
Protecting Americans from Tax Hikes (PATH) Act of 2015, Section 402	IRS Employees Prohibited from Using Personal Email Accounts for Official Business
Public Law 105-35	Taxpayer Browsing Protection Act (UNAX)

Exhibit 1.1.27-6 (02-09-2018)
Privacy Policy and Compliance Authorities

The following table reflects the authorities and their general descriptions for PPC activities:

Authority	Description
5 U.S.C 552	The Freedom of Information Act (FOIA)
5 U.S.C. 552a	The Privacy Act
IRC 6103	Confidentiality and disclosure of returns and return information
Public Law 100-503	Computer Matching and Privacy Protection Act of 1988
Public Law 107-347	E-Government Act of 2002
18 U.S.C. 2510, et seq.	Electronic Communications Privacy Act
NIST Special Publication 800-53 Rev. 4	Security and Privacy Controls for Federal Information Systems and Organizations
NIST Special Publication 800-122	Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
Treasury Directive Publication 25-07	Privacy Impact Assessment
Treasury Directive Publication 85-01	Treasury Information Technology (IT) Security Program

Exhibit 1.1.27-7 (05-07-2019)
Functional Delegation Order PGLD-1-23-1

(1) **Authority to Act in the Absence of the Chief Privacy Officer and other Privacy, Governmental Liaison and Disclosure Executives**

(2) **Authority:** To act in the absence of the Chief Privacy Officer.
The management officials who occupy the positions listed below are delegated authorization to the position of Chief Privacy Officer.
The official named as successor will be vested with all authority given the Chief Privacy Officer until relieved of the responsibility.

(3) **Delegated to:**

- Director, Governmental Liaison, Disclosure and Safeguards
- Director, Identity Assurance
- Director, Identity and Records Protection
- Director, Privacy Policy and Compliance

(4) **Redelegation:** This authority may not be redelegated.

(5) **Authority:** To act in the absence of the Director, Governmental Liaison, Disclosure and Safeguards.
The management officials who occupy the positions listed below are delegated authorization to the position of Director, Governmental Liaison, Disclosure and Safeguards.
The official named as successor will be vested with all authority given the Director, Governmental Liaison, Disclosure and Safeguards until relieved of the responsibility.

(6) **Delegated to:**

- Associate Director, Data Services
- Associate Director, Disclosure
- Associate Director, Governmental Liaison
- Associate Director, Safeguards

(7) **Redelegation:** This authority may not be redelegated.

(8) **Authority:** To act in the absence of the Director, Identity Assurance.
The management officials who occupy the positions listed below are delegated authorization to the position of Director, Identity Assurance.
The official named as successor will be vested with all authority given the Director, Identity Assurance until relieved of the responsibility.

(9) **Delegated to:**

- Associate Director, Identity Modernization
- Associate Director, Identity Strategies
- Associate Director, Identity Innovations
- Assistant to the Director, Identity Assurance

(10) **Redelegation:** This authority may not be redelegated.

(11) **Authority:** To act in the absence of the Director, Identity and Records Protection.
The management officials who occupy the positions listed below are delegated authorization to the position of

Exhibit 1.1.27-7 (Cont. 1) (05-07-2019)
Functional Delegation Order PGLD-1-23-1

Director, Identity and Records Protection.
The official named as successor will be vested with all authority given the Director, Identity and Records Protection until relieved of the responsibility.

(12) **Delegated to:**

- Associate Director, Information Protection Projects
- Associate Director, Records and Information Management

(13) **Redelegation:** This authority may not be redelegated.

(14) **Authority:** To act in the absence of the Director, Privacy Policy and Compliance.
The management officials who occupy the positions listed below are delegated authorization to the position of Director, Privacy Policy and Compliance.
The official named as successor will be vested with all authority given the Director, Privacy Policy and Compliance until relieved of the responsibility.

(15) **Delegated to:**

- Associate Director, Incident Management and Employee Protection
- Associate Director, Privacy Compliance and Assurance
- Associate Director, Privacy Policy and Knowledge Management

(16) **Redelegation:** This authority may not be redelegated.

(17) **Source of Authority:** Servicewide Delegation Order 1-23 (see IRM 1.2.2.20)

(18) This order supersedes Delegation Order PGLD-1-23-1, dated May 7, 2019. To the extent that the authority previously exercised consistent with this order may require ratification, it is hereby approved and ratified.

(19) **Signed:** Robert Choi, Chief Privacy Officer, Privacy, Governmental Liaison and Disclosure.