United States
International Trade Commission

Information Resource Management Strategic Plan

v1.0

Contents

Version History

Revised on	Version	Description
7/30/2025	1.0	Initial Version

Introduction

In support of the agency mission and business needs, and as part of the agency's overall strategic and performance planning processes, the United States International Trade Commission (USITC or Commission or agency) has developed and maintains this Information Resource Management (IRM) strategic plan that describes its technology and information resources processes and goals.

This plan was developed in accordance with and supports the goals of the USITC Strategic Plan available at https://www.usitc.gov and illustrates how the technology and information resources goals map to the mission and organizational priorities, specifically those objectives found in strategic objectives 3.3 and 3.4 of the Strategic Plan. These goals are specific, verifiable, and measurable, so that progress against these goals can be tracked, as shown in the Annual Performance Plan and Annual Performance Review.

About USITC

The U.S. International Trade Commission is an independent, nonpartisan, quasi-judicial federal agency established by Congress with a range of trade-related mandates. The Commission:

- Adjudicates whether: (1) dumped or subsidized imports injure a domestic industry; (2) surges of fairly traded imports injure a domestic industry; and (3) imports infringe a domestic intellectual property right or otherwise unfairly injure a domestic industry
- Provides independent, objective, and timely analysis of trade and competitiveness issues to the President, the U.S. Trade Representative (USTR), and Congress
- Maintains the Harmonized Tariff Schedule of the United States.

The USITC is headed by six Commissioners who are nominated by the President and confirmed by the U.S. Senate. The Commissioners' terms are set at nine years by statute and are staggered such that a different term expires every 18 months. However, a Commissioner may serve until replaced. As such, a Commissioner may begin serving after the nine-year term has begun and may continue to serve after the term has expired.

No more than three Commissioners may be members of the same political party. The Chair and the Vice Chair are designated by the President and serve for a statutory two-year term in those roles. The Chair may not be of the same political party as the preceding Chair, nor may the President designate two Commissioners of the same political party to serve as the Chair and Vice Chair.

To support its mission, the USITC maintains a professional staff of trade and nomenclature analysts, investigators, financial analysts, statisticians, attorneys, economists, information technology specialists, and administrative support personnel.

USITC Mission Statement

As established by Congress, the Commission's mission is to apply its expertise in international trade matters to serve policymakers and the public, by assessing and addressing unfair imports and other trade practices that injure U.S. industries, providing information and analysis of international trade and competitiveness issues, and maintaining the Harmonized Tariff Schedule of the United States.

IT Vision Statement

What: To provide the ideal work environment necessary to support the mission regardless of location.

How (strategic): By implementing reliable and secure systems that promote resilience, innovation, efficiency, and portability.

How (tactical): Take advantage of current and future technologies to ensure that our IT architecture is flexible, accessible, secure, reliable, and portable. Solutions do not need to be overly complicated and should be scaled to our environment. Costs can be controlled using automation and process.

To achieve this, we will:

- Ensure that our IT services and organizational model are properly aligned with the mission
- Ensure that stakeholders are fully engaged
- Follow business best practices
- Provide the highest level of customer support possible while still complying with mandates and directives, as well as maintaining the necessary levels of administrative control.

Ongoing IT Priorities:

1. Availability and accessibility of production systems
2. System security and vulnerability management
3. Compliance with mandates
4. Enhancements to infrastructure and systems

USITC Strategic Plan

The USITC Strategic Plan sets forth the strategic goals and objectives that underpin the Commission's work over the next five years. In its second century, the Commission will continue to provide high-quality, leading-edge analysis of international trade issues to the President and the Congress, and to remain a highly regarded forum for the adjudication of intellectual property and trade disputes. These goals and objectives are:

Strategic Goal 1 Investigate: Conduct Efficient and Effective Investigations

Strategic Objective 1.1 Efficient: Conduct expeditious and transparent proceedings

Strategic Objective 1.2 Effective: Engage the public, including stakeholders and experts, and collect relevant data to inform and support investigations

Strategic Goal 2 Inform: Develop Sound and Informed Analysis

Strategic Objective 2.1 Sound: Provide comprehensive, evidence-based analysis and determinations

Strategic Objective 2.2 Informed: Provide clear and accurate information

Strategic Goal 3 Perform: Continuously Advance Organizational Excellence

Strategic Objective 3.1 People: Attract, recruit, develop, and retain a qualified, accountable, and versatile workforce

Strategic Objective 3.2 Money: Ensure vigilant, responsible, and transparent stewardship of taxpayer funds

Strategic Objective 3.3 Technology: Implement and maintain reliable and secure systems that promote efficiency, resilience, innovation, and portability

Strategic Objective 3.4 Data: Manage, use, and release data to inform decision making

Strategic Objective 3.5 Operational Efficiency: Evaluate and improve processes and communications

While Strategic Goals 1 and 2 are specific to USITC operations, Strategic Goal 3 underpins the Commission's commitment to continuous process improvement and support for the Commission's other strategic goals and mission. The Commission has established five strategic objectives in support of this goal. The objectives align with five areas: human resources; budget, acquisitions, and finance; IT; data governance; and operational effectiveness.

This plan sets forth the principles and guidelines that shape the current and future IT activities at the USITC and relates directly to the USITC Strategic Plan.

Strategic Objective 3.3

Technology: Implement and maintain reliable and secure systems that promote efficiency, resilience, innovation, and portability.

Reliable and secure IT services are crucial to accomplishing USITC's mission. The Commission will continue to provide and enhance the technologies, security, infrastructure, and IT management resources necessary to support the Commission and government-wide goals and objectives.

The Commission will provide technology leadership, strategy, resource management, and processes necessary to ensure success. It will ensure that all IT activities properly align with priorities, strategic goals, and strategic objectives, both Commission- and government-wide. It will communicate internally regarding IT activities and continuously advance communication, coordination, and service delivery to external and internal stakeholders.

The key strategies to implement this objective include:

- Implementing reliable IT solutions and programs that promote resilience. This will be accomplished by ensuring the availability and accessibility of networks and applications
- Promote innovation and resilience by providing modern technology solutions that align with and support the Commission's business environment, policy goals, and statutory requirements
- Continuously enhancing the Commission's technical architecture to support the automation of business processes to improve efficiency and productivity
- Capitalizing on its risk-based information security program to predictively protect the infrastructure and information assets entrusted to the Commission
- Maintaining a sustainable balance between performance, security, availability, and accessibility
- Maturing IT management using best practices to improve collaboration with stakeholders, continuously implementing strengthened IT controls through effective policies and procedures and promoting transparency in budgeting for IT resources.

To monitor the success of these strategies, measurable performance goals will be established and tracked. These goals include ensuring a robust security posture by successfully implementing capabilities consistent with government-wide cybersecurity priorities, improving the delivery of IT solutions to better support Commission users, and using cloud services where feasible to reduce infrastructure resource requirements, increase flexibility to scale solutions, and expand solution options for Commission users.

Strategic Objective 3.4

Data: Manage, use, and release data to inform decision making

Managing and leveraging data as an asset is critical to accomplishing the USITC's mission. To support Commission and government-wide goals and objectives, the Commission will continue to enhance its data governance policies and practices.

Over the course of this strategic plan, the Commission will institute and apply government-wide data governance best practices. In doing so, the key strategies to implement this objective include:

- **Strengthening Commission-wide data governance by establishing enterprise-wide strategies, objectives, and policies for managing data:** The Commission requires sound data governance processes to administer the data that it uses to meet operational needs, answer important questions, and comply with legal requirements. Public trust is paramount, and data governance must support transparency while protecting privacy and confidentiality. The Commission recognizes the strategic and critical need for consistent governance and management of its data assets. This objective seeks to strengthen data governance by establishing and evolving foundational data governance processes. It seeks to improve coordination and planning of agency-wide data initiatives, and it mandates and provides mechanisms for escalating data-policy issues to ensure holistic strategies for resolution. Importantly, the Commission will emphasize elevating data maturity across the organization
- **Advancing the strategic use of data:** The Commission's strategic use of data depends on its ability to leverage insights from data and analytics to drive better policy, program, and operational decision-making. Key information may come from a variety of sources, including data internal to the Commission, data sourced from the private sector, and data from other agencies. This objective seeks to improve the Commission's use of all data to support and communicate insights, program evaluation, and operational management. The Commission must be able to connect fragmented data from disparate sources if it is to successfully answer its most critical questions and effectively make sound decisions
- **Improving data access, transparency, and data protections:** To effectively leverage data as a strategic asset, it must be discoverable. To ensure that all data is discoverable, the Commission will deploy appropriate data search and data extraction tools; ensure that data assets are identified, described, documented, and inventoried; ensure that data search and extraction tools are maintained and periodically upgraded; foster transparency by developing and deploying cutting-edge technologies to improve the flow of information; and develop controls to ensure data is appropriately protected from creation through destruction.

To monitor the success of these strategies, the USITC will establish and track measurable performance goals. These goals pertain to:

- Issuance and management of data governance policies that implement governmentwide best practices.
- Advancement of the strategic use of data in decision-making by deploying effective business intelligence tools that enable decision-maker to answer priority questions.
- Improvement of data access, transparency, and protections by deploying appropriate data systems that safeguard data while making it discoverable.

Data Sharing

The USITC recognizes that federal information is both a strategic asset and a valuable national resource that enables the government to carry out its mission and programs effectively. Data provides the public with knowledge of the government, society, economy, and environment – past, present, and future. Federal information is also a means to ensure the accountability of government, to manage government operations, and to maintain and enhance the performance of the economy, the public health, and welfare. Appropriate access to federal information significantly enhances the value of the information and the return on the nation's investment in its creation.

The USITC has been at the forefront of data sharing via its Open Data Portal. Open Data refers to publicly available data structured in a way that enables data to be discoverable and usable by end users. Making information about government operations more readily available and useful is core to the promise of a more efficient and transparent government. USITC provides an open data catalog at https://www.usitc.gov/data/index.htm, which uses the common core metadata schema for federal agency open data listings.

Improving data access, transparency, and data protections is integral to the Commission's strategic goals. To effectively leverage data as a strategic asset, it must be discoverable. To ensure that all data is discoverable, the Commission continues to deploy data search and data extraction tools; ensures that data assets are identified, described, documented, and inventoried; ensures that data search and extraction tools are maintained and periodically upgraded; fosters transparency by developing and deploying cutting-edge technologies to improve the flow of information; and maintains controls to ensure data is appropriately protected from creation through destruction.

The USITC has established and tracks measurable performance goals to measure the success of these strategies. The Commission continues to issue and manage data governance policies that implement government-wide best practices; advance the strategic use of data in decision-making by deploying effective business intelligence tools that enable decision-makers to answer priority questions; and improve accessibility, availability, transparency, and security of data by deploying appropriate data systems that safeguard data while also making it discoverable.

Inventories

System Inventory

USITC maintains an inventory of the major information systems. Information System Security Officers (ISSO) document and maintain the Commission's inventory of major systems in a networked file repository. This inventory details: the system name, the system owner, the assigned ISSO, the system scope, and the authorization status (to include the authorization dates) for all Commission defined systems. The Commission's inventory of major systems is reviewed and updated when there is any major system update, but at least annually.

Privacy Inventory

The USITC has implemented and continues to enhance a mature agency-wide privacy program led by the Senior Agency Official for Privacy (SAOP). The SAOP has overall responsibility and accountability for ensuring implementation of information privacy protections, including compliance with federal laws,

regulations, and policies relating to information privacy. The privacy program is based on the Privacy Act of 1974, the E-Government Act of 2002, Office of Management and Budget (OMB) Circular A-130, OMB memorandums, and USITC policies.

As part of this program the USITC maintains an inventory of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information (PII). This inventory allows the Commission to regularly review its PII and ensure, to the extent practical, that such PII is accurate, relevant, timely, and complete. The inventory also facilitates reducing the PII inventory to the minimum necessary for the proper performance of authorized functions. The privacy inventory is updated as necessary to maintain its accuracy and is formally reviewed annually by the privacy officer.

Data Inventory

The USITC maintains a data inventory in support of its mission to investigate, make determinations, and provide information to policy makers on tariffs, trade, and competitiveness. The Commission pursues its mission by ensuring its independence, integrity, trust, and transparency. Data is essential to all the Commission work. The data inventory is managed by the Data Governance Board, that updates the inventory as necessary to maintain its accuracy. Each data asset in the inventory is maintained near-real time by the asset owned and certified annually. The complete data inventory is reviewed at least annually by the Chief Data Officer.

Information Management

USITC continually adopts new and emerging technologies, and regularly assesses:

- the inventory of the physical and software assets associated with the system
- the maintainability and sustainability of the information resources and infrastructure supporting the system
- the ability of systems to effectively support the USITC's mission and business functions
- The ability to adequately protect Commission assets.

USITC ensures the terms and conditions of contracts and other agreements involving the processing, storage, access to, transmission, and disposition of Federal information are reviewed to enable the agency to meet its policy and legal requirements.

Risk Management

USITC manages its IT related risks in compliance with National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and NIST Special Publications (SPs) (e.g., 500, 800, and 1800 series guidelines), via its Enterprise Risk Management system. USITC considers information security, privacy, records management, public transparency, and supply chain security issues for all resource planning and management activities throughout the system development life cycle so that risks are appropriately managed.

The Chief Information Officer (CIO) is designated as the Senior Agency Official for Records Management (SAORM) and SAOP. In these capacities, the CIO regularly reviews and addresses risk regarding processes, people, and technology and apprises Commission management of risk mitigation strategies at least monthly, unless otherwise warranted.

Planning, Programming, and Budgeting

In accordance with the Federal Information Technology Acquisition Reform Act (FITARA) and related OMB policy, the USITC ensures that IT resources are distinctly identified and separated from non-IT resources during the planning, programming, and budgeting processes in a manner that affords the CIO appropriate visibility and specificity to provide effective management and oversight of IT resources.

The USITC utilizes an agencywide Budget and Finance Committee (BFC) to manage a mature budget development and execution process. The BFC is chaired by the Chief Financial Officer (CFO) and includes the Chief Administrative Officer (CAO), CIO, General Counsel (GC), and Director of Operations (OPS) in the planning, programming, and budgeting for all agency programs, including those involving IT resources. The BFC convenes at least monthly and reports out on its activities to the Chair and other Commissioners. BFC activities culminate in the annual Budget Review Board (BRB) which is led by the USITC Chair. During the BRB process the Chair of the Commission, in consultation with senior leadership, evaluates the output of the processes by which program leadership works with the CIO to plan an overall portfolio of IT resources that achieve program and business objectives efficiently and effectively by:

- Weighing potential and ongoing IT investments and their underlying capabilities against other proposed and ongoing IT investments in the portfolio
- Identifying gaps between planned and actual cost, schedule, and performance goals for IT investments and developing a corrective action plan to close such gaps.

The CIO approves the IT components of any Commission projects and provides guidance as to how the agency uses information resources to achieve its objectives. In the preparation of related budget requests, the CIO:

- Reviews and approves the IT investments portion of the budget request
- Ensures that privacy requirements, as well as any associated costs, are explicitly identified and included with respect to any IT resources that will be used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII
- Includes appropriate estimates of all IT resources included in the budget request
- Collaborates with the CFO to define agency-wide policy for the level of detail of planned expenditure reporting for all transactions that include IT resources.

Business Continuity Planning

The USITC continuity of operations plan (COOP) is dependent on the ability of staff to effectively telework. For this plan to be successful, the infrastructure must support this capability on a full-time basis. The USITC has continued to modernize its technical architecture and business processes to enable the agency to accomplish its mission with either an in-person or remote workforce.

Governance

The USITC Chief Information Officer is responsible for:

- Defining, implementing, and maintaining processes, standards, and internal administrative policies applied to all information resources at the agency, in accordance with OMB guidance

- Defining processes and administrative policies in sufficient detail to address information resources appropriately. These processes and administrative policies require that:
    - Investments and projects in development are evaluated to determine the applicability of agile development
    - Open data standards are used to the maximum extent possible when implementing IT systems
    - Appropriate measurements are used to evaluate the cost, schedule, and overall performance variances of IT projects across the portfolio leveraging processes such as IT investment management, enterprise architecture, and other agency IT or performance management processes
    - There are agency-wide administrative policies and procedures for conducting IT investment reviews, operational analyses, or other applicable performance reviews to evaluate IT resources, including projects in development and ongoing activities
    - Working with the CDO, data and information needs are met through agency-wide data governance policies that clearly establish the roles, responsibilities, and processes by which agency personnel manage information as an asset and the relationships among technology, data, agency programs, strategies, legal and regulatory requirements, and business objectives
- Ensuring unsupported information systems and system components are phased out as rapidly as possible
- Being a member of governance boards that inform decisions regarding IT resources to provide for early matching of appropriate information resources with program objectives
- Requiring that information security and privacy be fully integrated into the system development process
- Conducting reviews to evaluate and make recommendations on the use of agency information resources
- Establishing and maintaining a process for the CIO to regularly engage with business units to evaluate the effectiveness of IT resources supporting each agency strategic objective and mission goals
- Working with system owners, ensuring that legacy and ongoing IT investments continue to deliver customer value and meet the business objectives of the agency and the programs that support the agency
- Measuring performance in accordance with the GPRA Modernization Act and OMB Circular A-11, Preparation, Submission, and Execution of the Budget.

Leadership and Workforce

The USITC requires that the Chief Human Capital Officer (CHCO), CIO, CAO, and SAOP develop and maintain a set of competency requirements for information resources staff, including program managers, information security, privacy, and IT leadership positions. The Commission has developed and maintains a current workforce planning process to ensure that the agency can:

- Anticipate and respond to changing mission requirements
- Maintain workforce skills in a rapidly developing IT environment
- Recruit and retain the IT talent needed to accomplish the mission, when permitted.

The Commission ensures that the workforce supporting the acquisition, management, maintenance, and use of information resources, has the appropriate knowledge and skills to facilitate the achievement of

the portfolio's performance goals. The Commission tracks performance of workforce development training, cross-functional training, and training and education used by the private sector, to maintain and enhance skills or obtain additional skills as necessary.

At the USITC, the CHCO and CIO (with additional human resources staff) work jointly to establish agency-wide critical elements to be included in all IT personnel performance evaluations. Likewise, the CIO is involved in the recruitment, approves the selection, and provides input for the performance review of all IT staff. As the designated SAOP, the CIO is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy. The CIO and CHCO take advantage of all flexible hiring authorities for specialized positions, as established by the Office of Personnel Management (OPM).

IT Investment Management

The USITC has a mature and well-developed IT investment strategy based on practical experience applying all appropriate guidance and controls. The Commission makes use of adequate competition, analyzes risks (including supply chain risks) associated with potential contractors and the products and services they provide, and allocates risk responsibility between the government and contractors when acquiring IT. When making IT investments, the USITC:

- Conducts definitive technical, cost, and risk analyses of alternative design implementations, including the full life-cycle costs of IT products and services such as planning, analysis, design, implementation, sustainment, maintenance, re-competition, and retraining costs
- Considers existing Federal contract solutions or shared services when developing planned information systems, available within the same agency, from other agencies, or from the private sector to meet agency needs to avoid duplicative IT investments
- Acquires IT products and services in accordance with government-wide requirements
- Ensures that decisions to improve existing information systems with custom-developed solutions or develop new information systems are initiated only when no existing alternative private sector or governmental source can efficiently meet the need
- Structures acquisitions for major IT investments into useful segments, with a narrow scope and brief duration, to reduce risk, promote flexibility and interoperability, increase accountability, and better match mission need with current technology and market conditions
- Requires firm delivery dates with agreed upon milestones for all IT investments
- Aligns IT procurement requirements with larger agency strategic goals
- Promotes innovation in IT procurements, including conducting market research to maximize utilization of innovative ideas
- Includes security, privacy, accessibility, records management, and other relevant requirements in solicitations.

All acquisition strategies, plans, and requirements (as described in FAR Part 7), or interagency agreements (such as those used to support purchases through another agency) that include IT are reviewed and approved by the CIO. These approvals consider the following factors:

- Alignment with mission and program objectives in coordination with program leadership
- Appropriateness with respect to the mission and business objectives supported by the IRM Strategic Plan
- Inclusion of innovative solutions
- Appropriateness of contract type for IT-related resources

- Appropriateness of IT-related portions of statement of needs or statement of work
- Ability to deliver functionality in short increments
- Inclusion of government-wide IT requirements, such as information security
- Opportunities to migrate from end-of-life software and systems, and to retire those systems.

The Commission designates IT investments according to relevant statutes, regulations, and guidance in OMB Circular A-11, and executes processes commensurate with the size, scope, duration, and delivery risk of the investment. The IT investment process encompasses planning, budgeting, procurement, management, and assessment.

The USITC considers the current and future goals and needs of the prospective IT service to strengthen the understanding of requirements when analyzing IT expenditures. All decisions concerning the selection of information system technologies and services, including decisions to acquire or develop custom or duplicative solutions are merit-based and consider factors such as the ability to meet operational or mission requirements, life-cycle cost of ownership, performance, security, interoperability, privacy, accessibility, the ability to share or reuse, potential resources required to switch vendors (when applicable), and availability of quality internal and external support. All software development contracts are consistent with the FAR. Additionally, the Commission considers the use of suitable existing federal and commercially available information technology resources to deliver a mature product at a potential cost-savings to the government.

The CIO ensures that all information systems security levels are commensurate with the impact that may result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information consistent with NIST standards and guidelines. All IT systems support machine-readable formats, are section 508 compliant, and include records management functions.

Information Management and Access

The USITC has appointed a CDO and created a data governance board (DGB) chaired by the CDO. The DGB was established as a sub-committee to the Performance and Management Strategic Planning Committee. Voting members of the DGB are the CDO, CAO, CFO, CIO, COO, and GC. Non-Voting members of the DGB include the Performance Improvement Officer, Director of Internal Controls and Risk Management, Assistant General Counsel for Administrative Law, the Chief Freedom of Information Act (FOIA) officer and the Deputy Chief of Staff.

The DGB was created to ensure the effective collection, management, compilation, and presentation of agency data; effective data governance; transparency, accessibility, and release of agency data; ensuring appropriate controls and use of sensitive data; and the application of strong internal controls to optimize and leverage the value of Commission data assets. The DGB ensures that information is managed with clearly designated roles and responsibilities to promote effective and efficient design and operation of information resources management processes throughout the Commission. Finally, the DGB establishes policy, procedure, and standards that enable data governance to ensure information is managed and maintained according to relevant statute, regulations, and guidance.

Under the purview of the DGB, the USITC provides information to the public consistent with its mission and subject to Federal law and policy. The USITC:

- Publishes non-sensitive, publicly accessible, machine-readable, appropriately described, complete, and timely information online in a manner that promotes analysis and reuse
- Ensures published data is provided in a format accessible to employees and members of the public with disabilities

- Avoids establishing, or permitting others to establish on their behalf, exclusive, restricted, or other distribution arrangements that interfere with the agency's ability to disseminate its public information on a timely and equitable basis
- Does not charge fees or royalties for public information
- Makes Government publications available to depository libraries through the Government Publishing Office
- Takes advantage of all dissemination channels, including Federal, State, local, tribal, and territorial governments, libraries and educational institutions, for-profit and nonprofit organizations, and private sector entities, in discharging agency information dissemination responsibilities
- Considers the impact of providing agency information and services over the Internet for individuals who do not own computers or lack Internet access and, to the extent practicable, pursuing additional or alternative modes of delivery to ensure that such information and services are accessible to, and their availability is not diminished for, such individuals.

Privacy

The USITC maintains a comprehensive privacy program that ensures compliance with applicable privacy requirements, develops and evaluates privacy policy, and manages privacy risks. The Chair of the Commission has designated the CIO as the SAOP who has agency-wide responsibility and accountability for developing, implementing, and maintaining an agency-wide privacy program to ensure compliance with all applicable statutes, regulations, and policies regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems, developing and evaluating privacy policy, and managing privacy risks at the agency. The SAOP has designated an agency privacy officer to assist in the tactical implementation of the Commission privacy program.

The SAOP and agency privacy officer:

- Monitor Federal law, regulation, and policy for changes that affect privacy
- Limit the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII to that which is legally authorized, relevant, and reasonably deemed necessary for the proper performance of agency functions.
- Ensure that PII is accurate, relevant, timely, and complete, and reduce all PII to the minimum necessary for the proper performance of authorized agency functions
- Take steps to eliminate unnecessary collection, maintenance, and use of social security numbers, and explore alternatives to the use of social security numbers as a personal identifier
- Comply with all applicable privacy-related laws, including the requirements of the Privacy Act and ensure that system of records notice (SORN) is published, revised, and rescinded, as required
- Maintain all records with PII in accordance with applicable records retention or disposition schedules approved by the National Archives and Records Administration (NARA)
- Conduct privacy impact assessments when developing, procuring, or using IT, in accordance with the E-Government Act and make the privacy impact assessments available to the public in accordance with OMB policy
- Maintain and post privacy policies on all agency websites, mobile applications, and other digital services, in accordance with the E-Government Act and OMB policy
- Coordinate with the CISO and other agency offices and officials, as appropriate.

Information Security

To provide proper safeguards, the USITC:

- Has designated a senior agency information security officer (Chief Information Security Officer) to develop and maintain an agency-wide information security program in accordance with the Federal Information Security Modernization Act of 2014 (FISMA)
- Protects information in a manner commensurate with the risk that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information
- Implements security policies issued by OMB, as well as requirements issued by the Department of Commerce, the Department of Homeland Security (DHS), the General Services Administration (GSA), and OPM. This includes applying the standards and guidelines contained in the NIST FIPS, NIST SPs (e.g., 800 series guidelines), and where appropriate and directed by OMB, NIST Interagency or Internal Reports (NISTIRs)
- Provides annual cybersecurity training and guidance to all agency employees and contractors.

The USITC has implemented and maintains a zero-trust based architecture in compliance with guidance and best-business practices.

Electronic Signatures

The USITC fully supports the use of electronic signatures. The Commission allows individuals or entities that deal with the agency the option to submit information or transact with the agency electronically, when practicable. The USITC maintains all electronic submissions in their electronic format in compliance with agency record management policies. The Commission has also developed and implemented processes to support the use of digital signatures, a form of electronic signature, for employees and contractors.

Records Management

The USITC has implemented and maintains a very mature, robust, and successful records management program. The Commission has designated the CIO as the SAORM who has overall agency-wide responsibility for records management. The USITC manages its electronic records in full compliance with government-wide requirements:

- Manages all permanent electronic records electronically for eventual transfer and accessioning by NARA in an electronic format
- Manages all email records electronically and retains them in a system that supports records management and litigation requirements, including the capability to identify, retrieve, and retain the records for as long as they are needed
- Ensures the ability to access, retrieve, and manage records throughout their life cycle regardless of form or medium
- Ensures agency records managed by the SAORM are treated as information resources and treated accordingly
- Ensures retention schedules are approved by the Archivist of the United States
- Ensures records are disposed on in accordance with approved retention schedules

- Provides annual training and guidance to all agency employees and contractors regarding their Federal records management responsibilities.

Leveraging the Evolving Internet

The USITC recognizes that in a global and connected economy, it is essential for the United States and the Federal Government to strive to ensure that internet-based technologies remain competitive. Networking demands, escalating with the continued emergence of connecting technologies, has grown well beyond initial capabilities. The use of the newest internet protocol (currently, Internet Protocol Version 6 [IPv6]) is an essential part of accomplishing these goals and ensuring that the network infrastructure can meet our needs for growing capacity, security, and privacy, and keep the United States competitive in the ever-escalating global electronic economy. Therefore, the USITC ensures all IT acquisitions using internet protocol conform to the FAR and all public-facing Internet services and enterprise networks fully support the newest version of internet protocol as required by OMB policy.