Federal Trade Commission
Privacy Impact Assessment

General Support System
(GSS)

Reviewed and Updated
April 2021

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The Federal Trade Commission (FTC, Commission, or Agency) is an independent federal law enforcement and regulatory agency with authority to promote consumer protection and competition through the prevention of unfair, deceptive, and anti-competitive business practices. The FTC pursues vigorous and effective law enforcement; advances consumer interests by sharing its expertise with federal and state legislatures and U.S. and international government agencies; develops policy and research tools through hearings, workshops, and conferences; and creates educational programs for consumers and businesses in a global marketplace with constantly changing technologies. The Commission enforces and administers a wide variety of competition and consumer protection laws.[1]

Agency employees and contractors operate out of offices in Washington, D.C., and regional offices located in Atlanta, Chicago, Cleveland, Dallas, Los Angeles, New York, San Francisco, and Seattle. The Bureaus of Consumer Protection (BCP), Competition (BC), and Economics (BE) conduct the FTC's mission-related work. The Office of General Counsel (OGC) provides legal counsel to Bureaus and handles most appellate litigation. The Office of the Chief Information Officer (OCIO) operates and maintains the necessary Information Technology (IT) services to support the mission, including the network, servers, applications, databases, computers, and communication facilities.

The FTC General Support System (GSS) is the FTC's primary IT infrastructure to host information systems that collect, process, disseminate, and store information in support of the Agency's mission. It is a collection of FTC systems protected by a common set of security controls. The GSS supports the major administrative and mission functions of the Agency and provides for the internal and external transmission and storage of Agency data. It is the IT platform or host for a number of FTC systems of records covered by the Privacy Act of 1974, 5 U.S.C. § 552a.[2] The GSS encompasses all permanent FTC locations and approved remote connections. The OCIO is the business owner for the GSS.

The GSS has dedicated connections with external (non-FTC) entities as necessary to support the FTC mission. Those connections are:

Connection	Purpose
Department of Interior, Interior Business Center (Denver)	Financial & Human Resources management
Department of Justice	HSR Electronic Filing System and Cyber Security Assessment and Management (CSAM)

[1] A list of the statutes enforced or administered by the FTC is available at https://www.ftc.gov/enforcement/statutes.
[2] The GSS itself is not a Privacy Act system of records, even though it supports such systems.

Information is stored in the GSS in centralized storage as well as local storage on servers and user-dedicated systems. The FTC's Shared Network Space Policy (SNSP) governs use of the centralized storage; it outlines employee roles and responsibilities, directory structure and naming conventions, and file permissions. Individual staff and managers are responsible for proper storage, handling, and use of Agency data residing in individually assigned network storage space, as well as compliance with the SNSP, FTC privacy policies, and related records retention, litigation, e-discovery, and information security procedures.

The design and proper operation of the GSS is accomplished using current technology, including switches, routers, firewalls, monitors, and other equipment through which sensitive data may pass or be temporarily retained. Access to these devices is restricted to authorized network operations and operations assurance staff.

The GSS hosts most of the Agency's systems, subsystems, databases, and applications. System and information owners or program managers are responsible for the proper handling, storage, and use of data in specific applications and databases in the GSS. Separate Privacy Impact Assessments (PIAs) cover certain subsystems, applications, and databases hosted on the GSS. Program managers or system owners draft these PIAs, which undergo review by the Chief Privacy Officer, the Chief Information Security Officer, the Office of General Counsel, and the Records and Information Management Office, as well as approval by the Deputy Chief Information Officer. The following list has examples of GSS components with separate Privacy Impact Assessments:

- Correspondence Management System
- Redress Enforcement Database
- Secure Investigations Lab
- Access Control System
- StenTrack Database System
- Matter Management System
- FTC Surveys

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

The information in this system is collected, maintained and disseminated pursuant to the Federal Trade Commission Act, 15 U.S.C. §§ 41-58 and other laws and regulations the Commission enforces.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[3] may be collected or maintained in the system/project. Check all that apply.

As the primary IT infrastructure used by the FTC to host information systems that collect, process, disseminate, and store information in support of the Agency's mission, the GSS collects, stores, and transmits a large volume of sensitive information of many types, including personally identifiable information (PII). This PII may relate to specific defendants, individual targets of investigations, employees of corporate defendants or targets, witnesses, consumers, victims of fraud, FTC employees, FTC contractors, law enforcement partners, and others. Many of these data collections are described in separate PIAs for various systems hosted by the GSS.[4] The table below lists types of PII collected or maintained in the GSS.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.

- ☒ Full Name
- ☒ Date of Birth
- ☒ Home Address
- ☒ Phone Number(s)
- ☒ Place of Birth
- ☒ Age
- ☒ Race/ethnicity
- ☒ Alias
- ☒ Sex
- ☒ Email Address
- ☒ Work Address
- ☒ Taxpayer ID
- ☒ Credit Card Number
- ☒ Facsimile Number
- ☒ Medical Information
- ☒ Education Records
- ☒ Social Security Number
- ☒ Mother's Maiden Name
- ☒ Biometric Identifiers (e.g., fingerprint, voiceprint)
- ☒ Audio Recordings
- ☒ Photographic Identifiers (e.g., image, x-ray, video)
- ☒ Certificates (e.g., birth, death, marriage, etc.)
- ☒ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)
- ☒ Vehicle Identifiers (e.g., license plates)
- ☒ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)
- ☒ Geolocation Information
- ☒ Passport Number
- ☒ User ID
- ☒ Temporary Internet Cookie Containing PII
- ☒ Employment Status, History, or Information
- ☒ Employee Identification Number (EIN)
- ☒ Salary
- ☒ Military Status/Records/ ID Number
- ☒ IP/MAC Address
- ☒ Investigation Report or Database
- ☒ Driver's License/State ID Number (or foreign country equivalent)
- ☐ Other *(Please Specify)*:_____

[3] Per OMB Circular A-130, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

[4] All current Privacy Impact Assessments are available on the FTC's website.

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

The GSS is composed of various other systems as mentioned in Section 1.1. These systems may contain additional non-PII elements; refer to the specific PIAs for these systems for more information. System performance data, such as logs, which contain session connection information, are collected by the GSS.

2.3 What is the purpose for collection of the information listed above?

Information in the GSS is collected, used, disseminated, and maintained for the Commission to perform its law enforcement, policy, personnel management, and other activities. FTC staff members collect and use the information to investigate anti-competitive practices and to enforce statutes protecting consumers from fraudulent, deceptive, and unfair acts and practices in the marketplace. FTC staff also use the information to coordinate law enforcement functions and other activities with federal, state, and local law enforcement partners. In addition, the information is used to assist with consumer redress and to respond to Congressional inquiries.

The FTC Financial Management Office (FMO) maintains financial information in the GSS for the procurement of goods and services and to support internal operations of the agency.

For more information regarding the purposes of information collected by the various systems that comprise the GSS, refer to the specific PIAs for these systems.

2.4 What are the sources of the information in the system/project? How is the information collected?

FTC staff create or obtain information in the GSS in connection with the Agency's law enforcement, policy, and other activities. In some instances, this information is provided voluntarily, such as when individuals submit comments in rulemaking proceedings or send correspondence to Congress that is then forwarded to the FTC, or when investigatory targets agree to provide information to the Commission in lieu of compulsory process. The FTC also obtains information in response to compulsory process, such as subpoenas and civil investigatory demands and via discovery in administrative and federal court litigation.[5] Information in the GSS also may come from other sources, such as public resources on the Internet, nonpublic investigatory databases, other law enforcement agencies, and commercial databases such as Lexis/Nexis. In some instances, individuals – for example, third parties in investigations or witnesses in administrative and federal court matters – may provide information about other individuals.

[5] See the FTC's website for an overview of the Commission's investigative and law enforcement authority.

Typically, information is obtained directly from targets of the FTC's law enforcement activities and from individuals and entities with information that may be relevant to an FTC investigation. Information is generally collected directly from whatever media is used to submit it. This may include copying information from paper-based sources or from removable media such as CDs, DVDs, and hard drives. It may also include copying information that is electronically submitted via the Agency's Secure File Transfer System, email, or other electronic submission mechanism (e.g., through a website form).

Information also may be collected by the FTC, its contractors, and law enforcement partners through a court-sanctioned immediate access, which involves entering the premises where the information is stored and using specialized computer equipment and software to copy the information to removable media (typically hard drives). Information may also be obtained via discovery or from other sources. For example, the FTC may obtain information from adverse parties in litigation or may collect information directly from the Internet, from other law enforcement databases,[6] or from commercial sources. Information collected during investigative activities is stored in the BCP Tech Lab, Relativity, Litigation Support System (LSS).[7] Some information may be transferred to the GSS as required to support mission activities.

Information in the GSS also is obtained from other FTC systems and FTC systems that are hosted by external entities listed below. These systems are not hosted within the GSS; however, information collected from these systems may be maintained in the GSS by FTC staff and contractors as part of their daily job functions. Staff often utilize designated folders on shared drives to store information pulled from various systems that are not hosted within the GSS. The list below provides examples of information systems with data that may be maintained in the GSS and that have their own Privacy Impact Assessments:[8]

- Sentinel Network Services (SNS)
- Redress Contractors (Analytics Consulting, Epiq Class Action, JND Claims Administration System, and Rust Consulting)
- BCP Tech Lab
- Litigation Support System (LSS)
- FTC Public Website (www.ftc.gov)
- ServiceNow Administrative E-Filing System
- Relativity

[6] For example, pursuant to an information-sharing agreement between the FTC and the Consumer Financial Protection Bureau, the two agencies may exchange relevant law enforcement information via OMBMax, a secure interagency information and communication system.

[7] Highly sensitive information also may be stored in the FTC's Secure Investigations Lab (SIL). The SIL is a secure computing environment that is isolated from the FTC's production, development, and test lab networks. Therefore, information stored within the SIL is covered by a separate PIA.

[8] This is not meant to be an exhaustive list and may change over time. To learn more about these systems, refer to the FTC's Privacy Impact Assessments (PIAs). Current PIAs, including those for system shown in this chart, are available on the FTC's website.

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

Information in the GSS may be used to support the FTC's law enforcement, policy, and internal operations to include:

- Managing the agency's personnel and human resource services;
- Managing the agency's financial and contracting operations;
- Maintaining the day-to-day network activities and security operations;
- Investigating potential or alleged violations of anti-competitive practices;
- Investigating and enforcing statutes protecting consumers against fraudulent, deceptive, or unfair practices in the marketplace;
- Resolving consumer complaints; and
- Assisting with consumer redress.

Data Will Be Accessed By and/or Provided To:	***How and Why the Data Will Be Accessed/Shared***
FTC Staff and Contractors	Agency staff and contractors who require information to support FTC law enforcement, policy, and other activities, system administrative activities, and to respond to FOIA and other disclosure requests will have access to the information. Access to information is necessary also to carry out FTC administrative functions related to human resources, security, financial management, and matter and resource management.
Other Federal agencies and law enforcement partners	The GSS may be accessed by other Federal agencies and law enforcement partners directly or by using pre-approved remote access solutions and secured telecommunication portals. Third parties otherwise do not have direct or indirect access to the GSS.

3.2 Do contractors and/or third party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

Authorized FTC contractors have access to information in the various systems that comprise the GSS. FTC contractors are required to sign nondisclosure agreements, complete security and privacy training prior to obtaining access to any systems, and complete annual security and privacy training to maintain network access and access to those systems. Other authorized federal agencies or law enforcement partners that have access to information in the GSS must agree to terms of use and non-disclosure agreements prior to access. Use is subject to the authorization and approval by the FTC.

3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third party service provider.

Contractors who access the GSS are subject to the same rules and policies as FTC staff. The contractor is subject to the FTC's Breach Notification Response Plan.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

The GSS is comprised of various systems (see Section 1.1) that collect and maintain PII; refer to the system-specific PIAs for more information about how each system provides notice. Wherever possible, the FTC provides timely and effective notice to the public about activities that impact privacy, including the collection, use, and disclosure, and disposal of information at the time the information is collected. The FTC's Privacy Act notices are included on all forms, websites, and other instruments by which Privacy Act information is collected from individuals, either in written or oral form. For those occasions where the FTC cannot provide notice at the time the information is collected (e.g., when the information is collected by another law enforcement agency or another organization), the FTC provides notice via its privacy policy, its Privacy Act system of records notices (SORNs), and its PIAs, including this one.

☒ Notice is provided via (*check all that apply*):
- ☒ Privacy Act Statement (☒ Written ☒ Oral)
- ☒ FTC Website Privacy Policy
- ☒ Privacy Notice (e.g., on Social Media platforms)
- ☒ Login banner
- ☐ Other

(*explain*):_____

☐ Notice is not provided (explain):_____

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

The opportunity or right depends on how the information is collected and the purpose for the collection. Those who provide information pursuant to compulsory process do not generally have a right to decline to provide the information. However, individuals who file public comments or requests for advisory opinions, or who send inquiries to members of Congress (which then become part of the Correspondence Management System) provide information about themselves voluntarily and could choose to decline to provide such information. See the

PIAs for systems or other IT functions supported or hosted by the Data Center GSS for further discussion.

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

An individual may make a request under the Privacy Act for access to information maintained by the FTC about themselves in the Privacy Act systems that are hosted on GSS. The FTC's privacy policy provides links to the FTC's SORNs, as well as information about making Freedom of Information Act (FOIA) requests and the online FOIA request form. Individuals must follow the FTC's Privacy Act rules and procedures, published in the Code of Federal Regulations (C.F.R.) at 16 C.F.R. 4.13. Access to information under the Privacy Act is subject to certain exemptions.

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

The FTC provides a process for individuals to correct or amend any inaccurate PII maintained by the Agency. The FTC's privacy policy provides links to the FTC's SORNs, which include information about how to correct or amend records. An individual may make a request under the Privacy Act for access to information maintained by the FTC about themselves in the Privacy Act systems that are hosted on the GSS. Access to the information under the Privacy Act is subject to certain exemptions. Individuals may also file requests under the FTC under the FOIA for agency records that may be about them (if they are not exempt from disclosure to them under those laws).[9] Additionally, individuals may contact the FTC with any complaints, questions or concerns via phone or email available on www.ftc.gov or contact the Chief Privacy Officer directly. Where appropriate, the FTC disseminates corrected or amended PII to other authorized users of that PII, such as external information sharing partners.

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

Information in the GSS that is used by the FTC as part of its law enforcement, policy, and other activities will be reviewed for accuracy and timeliness in accordance with the specific needs of a particular FTC activity, rather than as part of overall GSS activities. For example, staff performing an investigation based upon a "whistleblower" complaint may verify the

[9] See 16 C.F.R. 4.11(a) (FTC FOIA rules), 4.13(m) (FTC Privacy Act rules).

information that is obtained is timely and accurate, and information obtained for use in an economic study may be checked in the aggregate against publicly available information.

Information in the GSS is also subject to appropriate information security controls, as further described below in this PIA. These controls will ensure that sensitive information is protected from any undue risk of loss and that the contents of evidentiary materials remain unchanged from the point-in-time they are included in the GSS.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

All FTC positions are assigned a risk designation that has associated criteria for personnel screening. All potential FTC employees, contractors, and volunteers are subject to background investigations and suitability reviews in accordance with OMB guidance.

Before any new employee, contractor, or volunteer can access any system in the GSS, that individual must first attend new employee orientation and successfully complete the FTC's Privacy and Security Awareness training. All employees are granted basic network access to include email services, the Internet, the Intranet, network shared drives, network-based applications, and are assigned their own home directory. There are specific procedures to address access restrictions for higher-risk categories of employees such as interns and International Fellows.

Supervisors and/or Contracting Officer's Representatives (CORs) must identify and approve employee requests to access network applications and specify the appropriate user role and level of access privileges. Network and application access is based on: (1) a valid access authorization, (2) intended system usage, and (3) other attributes based on the system's business function. All network and application access is based on least-privilege and need-to-know security models.

Auditing measures and technical safeguards are in place commensurate with the National Institute of Standards and Technology (NIST) Recommended Security Controls for Federal Information Systems and Organizations Moderate-Impact Baseline Special Publication (SP) 800-53.

5.3 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

For systems that require the use of PII to conduct testing, production data is copied to a test environment, then scrambled and/or masked to create test data. This process allows for the modification of possibly sensitive live data into fictionalized, usable test records that can be utilized efficiently to test the integrity of the application. User access controls limit application developers' access to data in test applications only, and usage is closely monitored.

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

Records schedules for the disposition of FTC mission and policy records are under development. Disposition of general technology management records and information system security records is authorized under National Archives and Records Administration (NARA) General Records Schedules 3.1 and 3.2.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

Any tracking technologies used on public-facing websites hosted on the GSS are described in the associated PIA for that system or website, as well as the FTC's privacy policy and cookie chart.

8 Privacy Risks and Evaluation

8.1 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

Risk	***Mitigation Strategy***
Malicious Code	Malicious code may be found on servers, client computers, and network shared storage. To address these risks, the FTC employs a suite of tools and systems to detect, remove, and block malicious code and to minimize the risk of network and user exposure.
Hackers	To address this risk, the FTC implements a defense-in-depth strategy in the GSS and participates in the federal government's continuous monitoring initiative.
Unauthorized Access to Data (Logical and Physical Access)	To address these risks, access to information is based on the least privilege security model in which authorized administrators and users are given the smallest amount of system and data access that is necessary to accomplish their authorized tasks. Each new network user receives the most restrictive set of privileges and network access, and additional privileges and access must be authorized when

Risk	*Mitigation Strategy*
	appropriate. Physical access to the GSS is controlled, logged, and monitored.
Misconfigured Information Asset	To address this risk, the FTC has deployed a strict configuration management program to approve and document all configuration changes made to GSS hardware, software, and other components.
Unapproved Sensitive PII Storage	To address this risk, FTC policy states that electronic documents (including emails) containing Sensitive PII may be stored only on individually assigned FTC network storage space, on a shared FTC network drive in an access-restricted file folder, or FTC-provided device.
Lost or Misplaced Tape Backup Media	To address this risk, the FTC encrypts all GSS data stored on NetApp backup storage appliance.
Information Loss through IT Asset Decommissioning	To address this risk, all IT asset hard drives are sanitized before reuse or destroyed before disposal, in accordance with FTC policies and procedures.
Personally Owned IT Equipment	To address this risk, no personally owned devices are allowed to be connected to any IT asset within the GSS.
Unapproved Sensitive PII Transmission	To address this risk, FTC policy generally requires that electronic documents (including emails) containing Sensitive PII must be transmitted using an approved secure file transmission solution.

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

Access to the applications hosted within the GSS occurs via the FTC network, which:

- enforces system lock-out after several failed login attempts;
- logs all session activity with username along with the IP addresses or domain names of the system components accessed; and
- requires two-factor authentication for elevated access to the network.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).

The GSS is not considered a Privacy Act system of record of its own accord. However, the systems and applications supported or hosted by GSS (as mentioned in Section 1.1) have the appropriate SORNs as necessary. As discussed earlier, the GSS hosted systems maintain data generated or compiled in the Commission's law enforcement and regulatory activities, as well as human resources, security, financial management, and matter and resource management data necessary for internal agency administration. Such data, to the extent such data are about an individual and retrieved by that individual's name or other personal identifier, are covered by the Privacy Act of 1974, 5 U.S.C. 552a, under one or more applicable FTC SORNs. A complete list and copies of these SORNs is available online at www.ftc.gov.

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

The collection, use, and disclosure of information in this system are consistent with the FTC's Privacy Policy. Access logs, storage logs, and firewall logs are periodically reviewed to ensure that users are complying with GSS policies and procedures. In addition, all FTC staff and contractors must review and sign the FTC Rules of Behavior form on an annual basis.