Federal Trade Commission

Privacy Impact Assessment

Data Center General Support System

April 2014

1. System Overview

1.1. The Federal Trade Commission

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]

The Agency staff of approximately 1,400 employees and contractors operates out of offices in Washington, DC, and regional offices located in Atlanta, Chicago, Cleveland, Dallas, Los Angeles, New York, San Francisco, and Seattle. The mission-related work of the FTC primarily is conducted by professional staff in the Bureaus of Consumer Protection (BCP), Competition (BC), and Economics (BE). The Office of the Chief Information Officer (OCIO) operates and maintains the necessary Information Technology (IT) services to support the mission, including the Agency's network, servers, applications, databases, computers, and communication facilities.

1.2. Datacenter General Support System (GSS) Architecture

The FTC Datacenter General Support System (GSS) is 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. It 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 Datacenter GSS encompasses all permanent FTC locations and approved remote connections. It also incorporates an Auxiliary Data Center facility, which provides supplementary storage and supports contingency operations for critical applications and capabilities. The OCIO is the business owner for the Datacenter GSS.

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

Connection	Purpose

[1] A list of the statutes enforced or administered by the FTC is available at http://www.ftc.gov/ogc/stats.shtm

[2] *See* section 8 of this PIA for further discussion. The Datacenter GSS itself is not a Privacy Act system of records, even though it supports such systems.

Department of Interior, Interior Business Center (Denver)	Financial & Human Resources management
AT&T MTIPS TICAP	Trusted Internet Connection Service
Department of Justice	HSR Electronic Filing System

Information is stored in the Data Center GSS in centralized storage as well as local storage on servers and user-dedicated systems. Use of the centralized storage is governed by the FTC's Shared Network Space Policy (SNSP), which outlines employee roles and responsibilities, directory structure and naming conventions, and the file permissions to be applied to directories and files. 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 Data Center 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.

1.3. Associated Systems Hosted on the Datacenter GSS

The Data Center GSS hosts most of the Agency's databases and applications.[3] 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 Data Center GSS. Certain subsystems, applications, and databases hosted on the Data Center GSS are covered by their own separate Privacy Impact Assessments (PIA). These PIAs are drafted by program managers and reviewed by the Chief Privacy Officer (CPO), Chief Information Security Officer, and Chief Information Officer (CIO), among others. The following table lists the current components for which separate PIAs have been developed:[4]

Name	Function	System of Records[5]
FOIAXpress	Supports, logs, and tracks the processing of each Freedom of Information Act (FOIA) request received by the Agency	Yes
Correspondence Management System (CMS)	Tracks Congressional and White House correspondence received by the Agency	Yes

[3] See Appendix 1 for a list of FTC systems that contain or interact with PII, are not hosted on the Data Center GSS, but are supported by it.
[4] All current Privacy Impact Assessments are at: http://www.ftc.gov/ftc/privacyimpactassessment.shtm.
[5] A "no" in this column indicates that the named IT function (like the Data Center GSS) is not itself a "system of records" as defined by the Privacy Act but may support or host other Privacy Act systems in whole or part, as described in the separate PIA for that IT function.

Name	Function	System of Records[5]
Matter Management System (MMS)	Records, tracks, and reports administrative and statistical information about FTC matters	Yes
Hart-Scott-Rodino (HSR) Electronic File System	Provides a secure electronic method for parties to a merger to submit the required documentation	Yes
Redress and Enforcement Database (RED)	Supports the enforcement of consumer protection orders and enables the Commission to monitor compliance with injunctive orders, collect outstanding judgments, and return the maximum amount possible to victimized consumers	Yes
BCP Litigation Committee Blog	Enables attorneys and staff working on BCP matters to share general information internally	Yes
Documentum (DOC-SMART)	Electronic Document Management System that allows staff to track, search, and access various types of Agency documents, such as staff memoranda to the Commission, Commission-approved reports, filings and orders in FTC adjudicative proceedings, and filings in federal court cases	Yes
Secure Investigations Lab (SIL)	Isolated computing environment configured with statistical and analytic software and sufficient processing power to support FTC work with large data sets	No
Desktop	The individual desktop computers, applications, and operating systems deployed by the OCIO	No
Secure File Transfer System (SFTS)	System that enables authorized FTC employees and non-FTC users to send and receive copies of electronic data over the Internet using enhanced encryption and authentication methods	No

Name	Function	System of Records[5]
Sentinel Network Services (SNS)	Supports BCP's Do Not Call, Consumer Complaint, and Spam programs; the Military Sentinel component is hosted within the Data Center GSS	Yes
FTC Wireless Access	802.11 wireless networks (WiFi) supporting FTC operations	No
Unified Communications	Component communications systems including VoIP, voicemail, VTC, IPTV, and mobility	No
Digital Signage	Component visual display systems including video wall and conference room scheduling	No
Access Control	Physical access control, PIV, security and monitoring systems	Yes

2. Information Collected and Stored within the System

2.1. What information is to be collected, used, disseminated, or maintained by the system?

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 Data Center 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. These data collections are described in PIAs for various systems hosted by the Data Center GSS.[6]

2.2. What are the sources of the information in the system?

Information in the Data Center GSS is created or obtained by FTC staff 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 rule making 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.[7] Information in the Data Center GSS may also be obtained from other sources, such as public resources on the Internet, nonpublic investigatory databases,

---

[6] All current Privacy Impact Assessments are at: http://www.ftc.gov/ftc/privacyimpactassessment.shtm.
[7] See http://www ftc.gov.ogc/brfovrvw.shtm for an overview of the Commission's investigative and law enforcement authority.

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.

Information in the Data Center GSS is also obtained from other FTC systems and FTC systems hosted by external entities as shown in the following chart:[8]

Name	Function	System of Records[9]
Sentinel Network Services (SNS)	An externally hosted program that gathers, processes, and updates consumer information	Yes
Redress	Permits redress class members to receive monetary disbursement from defendant-funded settlements or litigated final orders	Yes
Federal Trade Staffing and Employment Express (FT-SEE)	An automated recruitment and staffing system that enables the electronic submission and evaluation of applications for positions at the FTC	Yes
Internet Lab	Used by Agency law enforcers (e.g., attorneys, investigators, paralegals) that is physically and logically separate from the Data Center GSS	No
Litigation Support System (LSS)	Isolated system used by Agency attorneys, investigators, and other staff to acquire, analyze, organize, and present large volumes of complex information and evidence	Yes
FTC public website (www.ftc.gov)	Primary tool for disseminating public information about FTC activities, including content about the FTC's customer-facing departments; links to published cases, reports, events, and resources; downloadable audio and video education files; RSS feeds; and links to the Commission's social media accounts	No

2.3. Why is the information being collected, used, disseminated, or maintained?

Information in the Data Center GSS is collected, used, disseminated, and maintained for the Commission to perform its law enforcement, policy, and other activities. FTC staff members collect and use the information to investigate anti-competitive practices and to

[8] All current Privacy Impact Assessments, including those shown in this chart, are at: http://www ftc.gov/ftc/privacyimpactassessment.shtm.
[9] See footnote 5 for an explanation of this column.

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 correspondence.

2.4. How is the information collected?

Data Center GSS information is created or obtained by the FTC from a variety of sources, including information obtained from law enforcement partners, information provided to the FTC voluntarily, as well as information obtained via compulsory process, discovery, or through other investigative sources. 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 collection mechanism).

Information may also be collected by the FTC, its contractors, and law enforcement partners by 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,[10] or from commercial sources. Information collected during investigative activities is stored on the Internet Lab or Litigation Support System. Some information may be transferred to the Data Center GSS as required to support mission activities.

2.5. How will the information be checked for accuracy and timeliness (currency)?

Information in the Data Center 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 Data Center GSS activities. For example, staff performing an investigation based upon a "whistle blower" complaint may verify the information that is obtained to ensure that it 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 Data Center 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

[10] 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.

materials remain unchanged from the point-in-time they are included in the Data Center GSS.

2.6. Is the system using technologies in ways that the FTC has not previously employed (e.g., monitoring software, Smart Cards, etc.)? If so, how does the use of this technology affect individuals' privacy?

The Data Center GSS does not employ technologies in previously unused ways. It centralizes the IT functions for efficiency, and periodic revisions and upgrades to hardware, software, and Data Center GSS-related technologies improve privacy, security, and operational efficiency. The potential impact on individuals' privacy by the operation of the Data Center GSS is discussed below and also in the related individual PIAs referenced in this document.

2.7. What law or regulation permits the collection of this information?

The FTC Act, the Commission's Rules of Practice, and other laws and regulations the Commission enforces permit the collection of the information. For more information, see http://www.ftc.gov/ogc/stats.

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

The following privacy risks were considered during the development of the Data Center GSS:

a. Malicious Code
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.

b. Hackers
To address this risk, the FTC implements a defense-in-depth strategy in the Data Center GSS and participates in the federal government's continuous monitoring initiative.

c. 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 appropriate. All network activity is closely audited and monitored, and unauthorized activity is referred to the appropriate official for action. Physical access to the Data Center GSS is controlled, logged, and monitored.

d. Data Leakage/Breach (unintentional release of PII to an untrusted environment)

   i. 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 Data Center GSS hardware, software, and other components.

ii. 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 or on a shared-FTC network drive in a file folder to which access has been restricted to authorized individuals..

iii. Lost or misplaced tape backup media
To address this risk, the FTC encrypts all Data Center data stored on backup tapes. The Agency also has a chain-of-custody process in place for transporting backup tapes and media to and from the Data Center GSS.

iv. 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.

v. Personally Owned IT Equipment
To address this risk, no personally owned devices are allowed to be connected to any IT asset within the Data Center GSS.

vi. Unapproved Sensitive PII transmission
To address this risk, FTC policy states that electronic documents (including emails) containing Sensitive PII must be transmitted using an approved secure file transmission solution.

3. Use and Access to Data in the System

3.1. Describe how information in the system will or may be used.

Information in the Data Center GSS may be used to support the FTC's law enforcement, policy, and other activities, to include:

- 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
- Assisting with consumer redress.

3.2. Which internal entities will have access to the information?

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. Information also is used to carry out FTC administrative functions related to human resources, security, financial management, and matter and resource management.

3.3. Which external entities will have access to the information?

The Data Center GSS may be accessed by authorized FTC contractors, 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 Data Center GSS.

4. Notice and Access for Individuals

4.1. How will individuals be informed about what information is collected, and how this information is used and disclosed?

Wherever possible, the FTC provides notice to individuals about its policies regarding the collection, use, and disclosure of information at the time the information is collected. For information that is collected pursuant to a request from the FTC, notice is provided as part of that request (e.g., in a letter request or in the document outlining the compulsory process request). 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.

4.2. Do individuals have the opportunity and/or right to decline to provide information?

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. Please see the PIAs for systems or other IT functions supported or hosted by the Data Center GSS for further discussion.[11]

4.3. Do individuals have the right to consent to particular uses of the information? If so, how would an individual exercise this right?

The opportunity or right to consent to particular uses of the information depends on how the information is collected and the purpose its collection. For example, those who provide information pursuant to compulsory process do not generally have a right to consent to particular uses of 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 may have the opportunity to consent to particular uses of the information. Please see the PIAs for systems or other IT functions supported or hosted by the Data Center GSS for further discussion.[12]

---

[11] All current PIAs are at: http://www ftc.gov/site-information/privacy-policy/privacy-impact-assessments.
[12] All current PIAs are at: http://www.ftc.gov/site-information/privacy-policy/privacy-impact-assessments.

4.4. What are the procedures that allow individuals to gain access to their own information?

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 Data Center GSS. Individuals must follow the FTC's Privacy Act rules and procedures, which are published in the Code of Federal Regulations (C.F.R.) at 16 C.F.R. 4.13. Access to the information under the Privacy Act is subject to certain exemptions. In addition, there is public information in the Data Center GSS that also appears on the FTC's website and is accessible to the public there or in paper format through the public reading room at FTC Headquarters in Washington, DC.

4.5. Discuss the privacy risks associated with the process of providing individuals access to their own records and how those risks are mitigated.

Individuals do not have direct access to the Data Center GSS so there are no associated privacy risks. As noted above, 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 Data Center GSS. Individuals must follow the FTC's Privacy Act rules and procedures which are published in the Code of Federal Regulations (C.F.R.) at 16 C.F.R. 4.13. Access to the information under the Privacy Act is subject to certain exemptions. In addition, there is public information in the Data Center GSS that also appears on the FTC's website and are accessible to the public there or in paper format through the public reading room at Headquarters.

5. Web Site Privacy Issues

5.1. Describe any tracking technology used by the Web site and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, Web beacon). Currently, persistent tracking technology is not approved for use by the FTC (see 5.2).

Not applicable (N/A). The Data Center GSS is not a website. Characteristics of public-facing websites hosted on the Data Center GSS are described in the associated PIA for the website.[13]

5.2. If a persistent tracking technology is used, ensure that the proper issues are addressed (issues outlined in the FTC's PIA guide).

N/A

5.3. If personal information is collected through a Web site, page, or online form accessible through the Internet, is appropriate encryption used? If not, explain.

N/A

---

[13] All current PIAs are at: http://www ftc.gov/site-information/privacy-policy/privacy-impact-assessments.

5.4. Explain how the public will be notified of the Privacy Policy.

N/A

5.5. Considering any Web site or Internet issues, please describe any privacy risks identified and how they have been mitigated.

N/A

5.6. If the Web site will collect personal information from children under 13, or be directed at such children, explain how it will comply with the Children's Online Privacy Protection Act (COPPA).

N/A

6. Security of Information in the System

6.1. Are all IT security requirements and procedures required by federal law being followed to ensure that information is appropriately secured?

The FTC follows all applicable Federal Information Security Management Act (FISMA) requirements and other applicable federal guidance to secure the Data Center GSS. The Data Center GSS is categorized as moderate using Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.

6.2. Has a Security Assessment and Authorization been completed for the system or systems supporting the program?

Yes.

6.3. Has a risk assessment been conducted on the system?

Yes, a risk assessment was completed as part of the Security Assessment and Authorization. An overall discussion of the privacy risks associated with the Data Center GSS and the steps that the FTC has taken to mitigate those risks is provided in section 2.8, above.

6.4. Does the project employ any new technology that may raise privacy concerns? If so, please discuss its implementation.

No.

6.5. What procedures are in place to determine which users may access the system and are they documented?

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 Data Center GSS, they 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 procedures to address access restrictions for higher-risk 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.

6.6. Describe what privacy training is provided to users either generally or specifically relevant to the program or system.

All FTC staff members are required to complete a computer security and privacy awareness training annually. The interactive online training covers topics such as properly handling PII and other data, online threats, social engineering, and the physical security of documents and electronics, such as laptops and mobile devices. Individuals with significant security responsibilities are also required to undergo additional training tailored to their respective responsibilities.

6.7. What auditing measures and technical safeguards are in place to prevent the misuse of data?

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.

6.8. Questions regarding the security of the system

Any questions regarding the security of the Data Center GSS should be directed to the FTC's Chief Information Security Officer.

7. Data Retention

7.1. For what period of time will data collected by this system be maintained?

Information in the Data Center GSS, including information, if any, that may be incorporated into or otherwise required to be preserved as Federal records, is retained and destroyed in accordance with applicable schedules and procedures issued or approved by the National Archives and Records Administration (NARA).

7.2. What are the plans for destruction or disposal of the information?

All information will be securely and irreversibly disposed of/destroyed in accordance with applicable FTC policies and procedures, OMB, NARA, and NIST regulations and guidelines.

7.3. Describe any privacy risks identified in the data retention and disposal of the information, and describe how these risks have been mitigated.

The privacy risks associated with the Data Center GSS and the steps that the FTC takes to mitigate those risks are described in section 2.8, above. Data that is retained in the Data Center GSS may be stored on external media, either in the form in which it was originally submitted, or on some form of secondary or backup media. Storage of information on external media does raise an additional risk of loss and/or unauthorized access. To mitigate these risks, all media that is not in active use is maintained in locked cabinets and offices and is subject to chain-of-custody controls and logging procedures. The FTC performs periodic inventories and audits to ensure that the information is maintained in a secure manner according to NIST guidelines. Regarding risks identified in the disposal of the information, all information will be destroyed in a matter that makes it impossible to recover.

8. Privacy Act

8.1. Will the data in the system be retrieved by a personal identifier?

The Data Center GSS is a supporting infrastructure and as such will not retrieve information by a personal identifier. As noted earlier, however, the Data Center GSS does support or host a number of Privacy Act systems of records (i.e., containing information retrieved by name or other personal identifier of the subject individuals) in whole or part.

8.2. Is the system covered by an existing Privacy Act System of Records notice (SORN)?

Yes, as to certain systems and applications supported or hosted by GSS. As discussed earlier, the Data Center 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 at: http://www.ftc.gov/foia/listofpaysystems.shtm.

9. Privacy Policy

9.1. Confirm that the collection, use, and disclosure of the information in this system have been reviewed to ensure consistency with the FTC's privacy policy.

The collection, use, and disclosure of information in this system are consistent with the FTC's Privacy Policy.

10. Scope of Data Center GSS PIA and Future Modifications

OCIO is constantly improving and expanding the technological capabilities of the Data Center GSS to enable the Agency to more effectively and efficiently carry out its mission. Consistent with the requirements of the E-Government Act of 2002, this PIA will be revised to reflect any significant changes to the Data Center GSS that impact the collection, storage, maintenance, or dissemination of PII. The PIA will not be modified to reflect routine application changes and modifications, version upgrades, feature patching, ongoing maintenance, new instances of existing products, or routine hardware upgrades such as the procurement of additional servers or additional memory or storage space. Changes to the Data Center GSS are closely managed by OCIO, and the decision to update this PIA will be made on case-by-case basis in consultation with the CISO, CPO, and others.

11. Approval and Signature Page

Prepared for the Business Owners of the System by:

_____ Date: _____
Jacalyn Johnson, Assistant Director for Infrastructure
Office of the Chief Information Officer

Review:

_____ Date: _____
Alexander C. Tang, Attorney
Office of the General Counsel

_____ Date: _____
Peter B. Miller
Chief Privacy Officer

_____ Date: _____
Jeffrey Smith
Chief Information Security Officer

_____ Date: _____
Jeffrey Nakrin
Director, Records and Filings Office

Approved:

_____ Date: _____
Bajinder Paul
Chief Information Officer

APPENDIX 1

List of Systems containing PII that are contained in or interact with the Data Center GSS

Name	Function
Accellion	Accellion is the FTC's preferred method to securely send and receive confidential Agency files containing sensitive information.
Accession	Maintains inventory of Commission records stored in off-site facilities.
Acquisition Files (paper)	Paper records pertaining to acquisitions.
AutoAudit	A tool for managing reviews and investigations of internal controls.
BCP Director's Office Matter Tracking	Tracks matters that BCP staff forward to the Director's Office staff.
BMC Group/Analytics	The Bureau of Consumer Protection's (BCP) Redress Administration Office (RAO) administers and coordinates redress activities. BMC Group/Analytics Inc. is one of four redress contractors that have been awarded a contract supporting RAO's goals.
CADapult	Tool for maintaining FTC office space in headquarters, satellite buildings, and regional offices.
CICOM	Check-in/Check-out management tool that provides approval and departure information, accounts for FTC property, and supports secure, authorized access to computer systems and buildings.
Clearance System	Used by the FTC and DOJ to communicate regarding competition investigations.

Name	Function
Collection of Public Comments Filed Electronically	Mechanism for collecting electronic comments concerning rulemakings and other proceedings from members of the public and for storing those comments in a secure database.
Commissioner's Agenda	Tracks matters, related attorneys, and circulations for each Commissioner.
Comprizon Suite	Tracks contract-related and other FTC financial obligations.
Concordance	Discovery and litigation document management system for identifying, organizing, and analyzing case critical information.
COR Training	Provides web-based required training for prospective Contracting Officer's Representatives (COR).
Contractor Performance Assessment Reporting System (CPARS)	Web-based system used to input data on contractor performance.
Cuadra Star	Used by the FTC Library for cataloging and acquisitions.
Denver Data Center	Department of Interior's data center, which supports certain FTC business processes.
Documentum	The system allows staff to track, search and access various types of agency documents, such as staff memoranda to the Commission; Commission approved reports; filings and orders in FTC adjudicative proceedings; and filings in federal court cases.
E-Discovery Survey	System that stores basic information about each database reviewed by the E-Discovery team.

APPENDIX 1

List of Systems containing PII that are contained in or interact with the Data Center GSS

Name	Function
Epiq Systems	The Bureau of Consumer Protection's (BCP) Redress Administration Office (RAO) is responsible for administering and coordinating redress activities. Epiq Systems is one of four redress contractors that have been awarded a contract supporting RAO's goals.
e-Train	Provides online training programs and tracks employee trainings.
FCRA Complaint Referral Program	Refers consumer complaints to the three major national credit reporting agencies.
Federal Docket Management System (FDMS)	Government-wide web-portal system that allows interested parties to search, view, download, and comment on actions and items listed in the Federal Register.
Federal Personnel/Payroll System (FPPS)	System that handles all aspects of personnel and payroll transactions.
FedTraveler.com	Travel management system.
FOIA Xpress	Electronically stores, retrieves, redacts, and prints documents for delivery to FOIA requesters. Tracks FOIA processing statistics and fees, and generates reports on the number, types, and nature of FOIA requests processed, as required by the US Department of Justice.
FTC Access Control System	System to manage physical access to the FTC facilities.
FTC Alert	System to provide FTC staff and contractors with timely information about emergencies that affect FTC facilities or operations.
FTC Bulk Distribution System	System that permits consumers to effectively and efficiently order FTC publications.
FTC Data Warehouse	System that stores program information and financial data for use in management analyses of FTC operations.
FTC Online Corporate Unified System (FOCUS)	Accounting application.
FT-SEE	Enables the electronic submission and evaluation of applications for positions at the FTC.
Gilardi LLC	The Bureau of Consumer Protection's (BCP) Redress Administration Office (RAO) administers and coordinates redress activities. Gilardi is one of four redress contractors that have been awarded a contract supporting RAO's goals.
Human Resources Personnel Records	Personnel records.
Internet Lab	Internet Lab computers are for the purposes of conducting investigations and other purposes for which BCP might need an off-network computer (e.g., observing the behavior of a malware program).
Law Enforcement Files	Records relating to law enforcement actions.
Matter Management System 2 (MMS2)	Records, tracks, and reports administrative and statistical information about FTC investigations, litigation, rulemakings, and other FTC law enforcement and regulatory projects, such as studies and workshops.

APPENDIX 1

List of Systems containing PII that are contained in or interact with the Data Center GSS

Name	Function
Medicare Modernization Act Database System	System that stores information submitted by pharmaceutical companies who enter into agreements with competitors regarding generic versions of branded medications.
Office of International Affairs (OIA)	Database that includes international contact lists and information, panelists from Cross Border Protection workshops, country clearances, and a log of foreign meetings and visitors to OIA.
Office of the Secretary Correspondence Tracking	Records the receipt of Congressional correspondence by the Office of the Secretary (OS) and tracks all referrals from OS to other organizations within the Commission.
ORC PKI Shared Service Provider	ORC provides (Public Key Infrastructure) PKI services that meets the FTC's HSPD-12 requirements.
ORCA	Secure federal hosting solution for litigation databases.
PAY.GOV	Allows members of the public to submit forms online and to make online payments to federal agencies.
Personnel Security Records	Used to identify and conduct background checks on FTC employees and contractors.
Premerger	Used to log, track, analyze, and respond to filings made under the Hart-Scott-Rodino Premerger Notification Act (HSR).
Redress and Enforcement Database	Improves the Agency's ability to gather and use data to ensure efficient, timely administration of redress to consumers and detail the status of individual redress matters, as well as to monitor compliance, track recidivist defendants, ensure compliance reports are filed, and enforce Commission orders.
Remedy	Tracks and routes service requests and manages inventory.
RN Number	Allows businesses to apply online for a Registered Identification (RN) Number and maintains a database of companies that have been assigned RN numbers.
RUST Consulting	The Bureau of Consumer Protection's (BCP) Redress Administration Office (RAO) administers and coordinates redress activities. RUST Consulting is one of four redress contractors that have been awarded a contract supporting RAO's goals.
SAFE	Secure, web-based connection to the FTC network for staff.
Secure Investigations Lab (SIL)	Allows staff to work with certain data sets obtained to support the Agency's investigations, litigation, and studies. Allows for the efficient manipulation of extremely large data sets that are routinely used to support the Agency's mission and regulatory activities.
STAFF ID	System that contains information about FTC employees for use in administrative functions such as the interactive FTC Directory and role-

APPENDIX 1

List of Systems containing PII that are contained in or interact with the Data Center GSS

Name	Function
	based access to FTC resources.
Staff Time and Activity Reporting System (STAR)	Tracks time spent by FTC staff on specific matters.
Strategic Management System (SMS)	Stand-alone, web-based application for performance reporting.
Transit Subsidy Tracking System	Tracks participants in the Agency's transit subsidy program.
Unofficial Human Resources Personnel Records	Evaluations and other personnel records, on paper.
Video Hosting	System that publishes and distributes FTC videos and provides online streaming of FTC events.
Web Customer Satisfaction Surveys	Tool that allows website visitors to provide feedback about their experience.
WEBT&A	WebT&A is a product of the Department of Interior's (DOI) National Business Center. It is a mainframe-based, integrated, web-based personnel and payroll system, which creates and generates the full life cycle of personnel and payroll transactions, enabling the FTC to maintain records electronically.
Zylab	Discovery and litigation document management system for identifying, organizing, and analyzing case critical information.