Federal Trade Commission

Privacy Impact Assessment

Data Center General Support System

July 2012

1. System Overview

a. 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 three offices in Washington, DC, and eight regional offices located in Atlanta, Georgia; Chicago, Illinois; Cleveland, Ohio; Dallas, Texas; Los Angeles, California; New York, New York; Seattle, Washington and San Francisco, California. 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.

b. Background About the Data Center General Support System (GSS)

The FTC Data Center 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. The Data Center GSS is located in Washington, DC, and extends to two satellite offices in Washington, DC, and to the eight Regional Offices The OCIO is the business owner for the Data Center GSS.

The Data Center GSS interconnects with the Department of the Interior (DOI) National Business Center (NBC) to support Agency timekeeping and human resource management activities, as well as all procurement and contracting activities. An interconnection also exists between the FTC and the Department of Justice (DOJ) and is used to electronically transmit information gathered via FTC's Hart-Scott-Rodino (HSR) Electronic Filing System to DOJ.

The majority of the Data Center GSS information is stored in a Storage Area Network (SAN) with partitioned shared network drives and is managed, in part, by an Electronic Document Management System[2]. The SAN is governed by the FTC's Shared Network Space Policy

[1] A list of the statutes enforced or administered by the FTC is available at http://www.ftc.gov/ogc/stats.shtm
[2] The Electronic Document System PIA is located at http://www.ftc.gov/os/2011/05/110524documentumpia.pdf

(SNSP) that 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 Data Center GSS incorporates a Secure Investigations Lab (SIL)[3], which is a discrete computing environment physically separate from the Data Center GSS. The SIL is configured with statistical and analytic software and sufficient processing power to allow the efficient manipulation of the extremely large data sets that are routinely used to support the Agency's mission and regulatory activities. This environment is accessible through two-factor authentication only and is not accessible from the Internet.

c. Applications and Databases Hosted on the Data Center GSS

The Data Center GSS hosts many of the Agency's core 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 Data Center GSS.

As such, specific subsystems, minor applications, or databases hosted on the Data Center GSS are covered by individual PIAs, which are drafted by program managers and revised by the Chief Privacy Officer (CPO) and Chief Information Officer (CIO). In addition, a separate PIA covers the individual desktop computers, applications, and operating systems deployed by the OCIO[4] and another PIA covers the FTC's primary public-facing website, www.ftc.gov.[5]

Examples of applications hosted in the Data Center GSS to support internal administrative activities and that are covered by individual PIAs include the following systems:

a. The FOIAXpress System[6] is used to support Freedom of Information Act (FOIA) requests received by the Agency and is used to log and track the processing of each FOIA request.
b. The Correspondence Management System (CMS)[7] is used to track Congressional and White House correspondence received by the Agency.
c. The Matter Management System (MMS)[8] is used to record, track, and report administrative and statistical information about FTC matters.

[3] The SIL PIA is located at http://www.ftc.gov/os/2009/05/silpia.pdf
[4] The Desktop Major Application PIA is located at http://www.ftc.gov/os/2011/10/1110ftcdesktoppia.pdf
[5] The ftc.gov PIA is located at http://www.ftc.gov/os/2012/03/1203ftcgovpia.pdf
[6] The FOIAXpress System PIA is located at http://www.ftc.gov/os/2011/06/1106foiaxpresssystem.pdf
[7] The CMS PIA is located at http://www.ftc.gov/os/2009/02/0901cmspia.pdf
[8] The MMS PIA is located at http://www.ftc.gov/os/2007/12/mmspia.pdf

d. The Personal Identity Verification (PIV) [9] System is used to collect and maintain information about employees using PIV cards for physical or logical access to Agency resources.

The Data Center GSS also hosts FTC business applications to include the following systems:

a. The Hart-Scott-Rodino (HSR) Electronic File System[10] provides a secure electronic method for merging parties to submit the documentation necessary to complete a filing.
b. The Redress and Enforcement Database (RED) System [11] is used to support the enforcement of orders obtained in FTC consumer protection actions and enables the Commission to monitor compliance with injunctive orders, collect outstanding judgments, and return the maximum amount possible to victimized consumers.
c. The Bureau of Consumer Protection (BCP) Litigation Committee Blog[12] enables attorneys and staff working on BCP matters the use of a blog-type internal webpage to share information.
d. The Secure Investigations Lab (SIL)[13] is a discrete computing environment configured with statistical and analytic software and sufficient processing power to allow the efficient manipulation of the extremely large data sets that are routinely used to support the Agency's mission and regulatory activities.
e. Documentum[14], the Agency's Electronic Document Management 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.
f. AutoAudit is an internal auditing and investigation tracking tool that allows selected FTC staff, including those in the Financial Management Office (FMO), to create and manage reviews and investigations of internal controls. Issue Track is an included tool that uses a webserver to display information collected in the AutoAudit database via a web browser. Although AutoAudit and Issue Track do not directly elicit or collect PII or Sensitive PII, Auto Audit has the ability to upload or link to pre-existing materials that may themselves contain such information. FTC policy and the accompanying training will bar users from uploading, linking to, or otherwise including personal information.

As part of the FTC's ongoing privacy and information security program, additional privacy impact assessments will be conducted and posted as appropriate.

[9] The PIV PIA is located at http://www.ftc.gov/os/2008/02/hrpd12pia.pdf
[10] The HSR PIA is located at http://www.ftc.gov/os/2011/06/1106hsrpremerger.pdf
[11] The RED PIA is located at http://www.ftc.gov/os/2007/07/Redress_PIA.pdf
[12] The BCP Litigation Committee Blog PIA is located at http://www.ftc.gov/os/2010/09/100923bcplitigationblawg.pdf
[13] The SIL PIA is located at http://www.ftc.gov/os/2009/05/silpia.pdf
[14] The Documentum PIA is located at http://www.ftc.gov/os/2011/05/110524documentumpia.pdf

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 large volume of sensitive information of many types, including both public and nonpublic PII. Sensitive 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. Typically this will include information in various electronic and non-electronic formats, such as word processing files, spreadsheets, databases, emails, images, videos, and audio files. This information includes law enforcement-- related information such as consumer complaints, affidavits, email, correspondence, financial information, health information, and other types of documents produced to the FTC pursuant to compulsory process or in the course of discovery.

Other information may include investigative hearing transcripts; transcripts of depositions in adjudicative proceedings, transcripts of adjudicative hearings and trials; briefs and other documents filed in adjudicative proceedings; orders entered in adjudicative proceedings; briefs and other documents filed in federal court cases; federal court orders to pay consumer redress and financial statements from individuals ordered to pay redress; Federal Register Notices of proposed consents; petitions related to cease and desist orders and FTC responses; and attachments to filings made through the HSR Electronic Filing System. Information stored in the Data Center GSS also includes staff- and Agency-level memoranda; Congressional correspondence; Federal Register notices of rule makings; requests for formal and informal advisory opinions and FTC responses; news releases; and speeches given by FTC officials. This list is not exhaustive, but illustrates the general categories if data that may be stored or handled on the Data Center GSS.

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

Information in the Data Center GSS is obtained by FTC staff in connection with the Agency's law enforcement functions 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 which is then forwarded to the FTC, or when investigatory targets agree to provide information to the Commission in lieu of compulsory process. 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.[15] Information in the Data Center GSS may also be obtained 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

[15] See http://www.ftc.gov.ogc/brfovrvw.shtm for an overview of the Commission's investigative and law enforcement authority.

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 FTC systems hosted by external entities, such as the Sentinel Network Services (SNS)[16] program that gathers, processes, and updates consumer information; the Redress Program[17] that permits redress class members to receive monetary disbursement from defendant-funded settlements or litigated final orders; and the Federal Trade Staffing and Employment Express (FT-SEE) [18] which is an automated recruitment and staffing system that enables the electronic submission and evaluation of applications for positions at the FTC.

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 functions and other activities. For example, FTC staff collect and use the information to investigate anti-competitive practices and to enforce statutes protecting consumers from fraudulent, deceptive, and unfair practices in the marketplace. 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 obtained by the FTC from a variety of sources, including 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[19], email, or some 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, or from commercial sources. The FTC maintains

[16] The SNS PIA is located at http://www.ftc.gov/os/2011/12/1112crss-pia.pdf
[17] The Redress Program PIA is located at http://www.ftc.gov/os/2008/09/0809bcpredresspia.pdf
[18] The FT-SEE PIA is located at http://www.ftc.gov/os/2007/09/ftsee_pia_web.pdf
[19] The Secure File Transfer System PIA is located at http://www.ftc.gov/os/2011/06/1106securefiletransfer.pdf

an Internet Lab[20] used by Agency law enforcers (e.g., attorneys, investigators, paralegals) that is physically and logically separate from the Data Center GSS, and some of the information collected during Internet Lab investigative activities may be stored on the SAN or other application residing in the Data Center GSS. Additionally, the FTC maintains a Litigation Support System (LSS)[21] that is physically and logically separate from the Data Center GSS and is used by Agency attorneys, investigators, and other staff to acquire, analyze, organize, and present large volumes of complex information and evidence. Some of the information collected in the LSS may be stored on the SAN or application residing in the Data Center GSS.

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

Information that is collected and stored in the Data Center GSS will not generally be systematically checked for accuracy and timeliness. However, information that is used by the FTC as part of its law enforcement and other activities will be reviewed for accuracy and timeliness as required by the particular activity. For example, staff performing an investigation based upon a "whistle blower" complaint may check the information that is obtained to ensure that it is timely and accurate and the information obtained for use in an economic study may be checked in the aggregate against publically available information.

While information may not be systematically checked for accuracy and timeliness, it will be subject to appropriate information security controls. 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 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 previously unused technologies, although the establishment of the Data Center GSS centralizes the IT functions for efficiency. The potential impact on individuals' privacy by the operation of the Data Center GSS is discussed in this document below and in the related individual PIAs referenced throughout 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.

[20] The Internet Lab PIA is located at http://www.ftc.gov/os/2011/01/1101bcpinternetlab.pdf
[21] The LSS PIA is located at http://www.ftc.gov/os/2011/03/1103bcplitigationsupportsystem.pdf

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:

- Malicious Code (viruses, trojans, worms, root kits, spyware, and dishonest adware). To address these risks, the FTC deployed a suite of anti-virus tools that remove and block these malicious threats.

- Hackers (individual who accesses a computer system by circumventing its security system). To address this risk, the FTC implemented a defense-in-depth strategy in the Data Center GSS to include the use of firewalls, routers, switches, intrusion prevention and detection systems, and internet filtering. Additionally, the FTC participates in the Office of Management and Budget (OMB) Managed Trusted Internet Protocol Service (MTIPs) initiative that created a secure gateway to protect the FTC's internal network from traffic to/from external networks. Furthermore, the FTC participates in the Department of Homeland Security (DHS) Einstein program, which facilitates identifying and responding to cyber threats and attacks and improves network security, among other things.

- Unauthorized Access to Data (Logical and Physical Access). To address these risks, access to information is based on the least privilege security model. The most restrictive set of privileges are applied to Agency network user IDs upon creation. 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 monitored via closed circuit TV and logged via card key reader.

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

  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 IT assets.
  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. The network storage space is scanned to ensure that Sensitive PII is not stored in an unauthorized file folder.
  Lost or misplaced tape backup media. To address this risk, the FTC encrypts all Data Center data stored on backup tape in Washington, DC and contracted with an information protection and storage vendor who transports the backup tapes in customized, secure vehicles. The Agency also has a chain-of-custody process in place for tape backup media coming to and from the Data Center GSS.
  Information loss through IT asset decommissioning. To address this risk, all IT asset hard drives are sanitized before reuse or degaussed before destruction.

Personally Owned IT Equipment. To address this risk, no personally owned mobile wireless devices (e.g., personal digital assistants, smart phones [iPhone, Blackberry, Droid]), laptops (to include the iPad), printers, ebook readers (e.g., Kindle, Nook) and personal electronic storage devices (e.g., removable media such as Universal Serial Bus (USB) flash drives, memory cards, external hard drives, or other equipment with electronic storage or communications capability such as digital cameras, portable digital music players) are allowed to be connected to any IT asset within the Data Center GSS.

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 functions 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, or assisting with consumer redress.

3.2 Which internal entities will have access to the information?

Agency staff and contractors who require information to support of FTC law enforcement and 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 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 FTC authorized external contractors, other Federal agencies, and law enforcement partners using pre-approved remote access solutions and secured telecommunication portals.

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. For example, 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. An analysis of all data collection activities by the Agency is beyond the scope of this PIA.

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 for 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. An analysis of all data collection activities by the Agency is beyond the scope of this PIA.

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 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 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.

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 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 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).

The FTC external website, www.ftc.gov, automatically collects some temporary information about user visits to help improve navigation of the site or investigate disruption of service attacks. This information includes Internet Protocol (IP) address, the date and time of visit, and the browser software and operating system used by the visitor. Some FTC websites use temporary cookie technology to keep track of visits while users are using the website. The FTC does not use persistent (multi-session) cookies on any website hosted by the Data Center GSS. The www.ftc.gov Privacy Policy includes a chart, http://www.ftc.gov/ftc/cookies.shtm, describing the purpose of any cookies used by Agency websites and alternatives for receiving the same information or services without cookies. The FTC's primary external website, www.ftc.gov, has its own Privacy Impact Assessment.[22]

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

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

Privacy Policy information is available to the public via a hyperlink on every FTC website. The FTC Privacy Policy is machine-readable (i.e., P3P compliant) and handicap accessible pursuant to Section 508 of the Rehabilitation Act.

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

The primary websites maintained on the Data Center GSS are www.hsr.gov and www.ftc.gov,

[22] The ftc.gov PIA is located here: http://www.ftc.gov/os/2012/03/1203ftcgovpia.pdf.

which have their own Privacy Impact Assessments.[23]

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).

None of the websites maintained on the Data Center GSS are directed at children.

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, ensuring the Data Center GSS is appropriately secured. 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 Certification and Accreditation 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 C&A.

6.4 Does the project employ 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 and associated personnel screening criteria. All potential FTC employees, contractors, and volunteers are subject to background investigations and suitability reviews per 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

[23] The hsr.gov PIA is available here: http://www.ftc.gov/os/2011/06/1106hsrpremerger.pdf and the ftc.gov PIA is available here: http://www.ftc.gov/os/2012/03/1203ftcgovpia.pdf

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 Contract Officer's Technical Representatives (COTRs) must identify and approve employee requests to access network applications and specify the appropriate 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 are required to complete a computer security and privacy awareness training annually. The interactive online training covers topics such as properly handling Sensitive 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 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, Rev. 3.

6.8 Questions regarding the security of the system

Any questions regarding the security of the system should be directed to the FTC's Information Assurance Manager.

7. Data Retention

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

Information is retained and destroyed in accordance with applicable schedules and procedures issued or approved by the National Archives and Records Administration (NARA). Information incorporated into FTC records is maintained in accordance with applicable schedules and procedures issued or approved by the NARA.

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

Disposal of information is conducted in accordance with OMB and any applicable technical security standards issued by the National Institute of Standards and Technology (NIST) 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.

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. In addition, 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 (e.g. on a hard drive), or on some form of secondary or backup media (e.g. tape). 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 maintains performs periodic inventories and audits to ensure the information is maintained in a secure manner according to NIST guidelines.

8. Privacy Act

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

Information contained in the Data Center GSS may be retrieved by one or more personal identifiers (e.g. name, physical address, e-mail address, telephone number, etc.).

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

Yes. As discussed earlier, the Data Center GSS maintains 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. Data maintained by the Data Center GSS, 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 has been reviewed to ensure consistency with the FTC's privacy policy.

The collection, use, and disclosure of information in this system is 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, 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 CPO.

11. Approval and Signature Page

Prepared for the Business Owners of the System by:

_____ Date: _____
Jeffrey Smith, Information Security Analyst
Office of the Chief Information Officer

Review:

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

_____ Date: _____
Peter Miller
Acting Chief Privacy Officer

_____ Date: _____
Jeffrey Smith
Information Assurance Manager

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

Approved:

_____ Date: _____
Jeffrey Huskey
Chief Information Officer