Federal Trade Commission
Privacy Impact Assessment
for the: Litigation Support System

April 2009

1 Introduction

The Federal Trade Commission (FTC or Commission) works to prevent business practices that are anticompetitive, deceptive, or unfair to consumers and to enhance informed consumer choice and public understanding of the competitive process, without standing in the way of legitimate business activity. The FTC engages in numerous activities that support this work, including engaging in law enforcement activities such as performing investigations and litigating cases. Increasingly, these activities involve electronically stored information (ESI) and the use of electronic discovery (e-discovery) tools and services, including computer forensics.

In addition to the FTC's law enforcement work, the agency periodically has a need to perform internal investigations, and to defend against suits brought against the agency. These activities require e-discovery tools and services similar to those used in the FTC's law enforcement work.

To support the agency's growing need for e-discovery tools and services, the FTC has created a Litigation Support System (LSS).

1.1 Law Enforcement Activities

The agency's law enforcement activities are supported by the FTC's Bureaus of Competition (BC), Consumer Protection (BCP), and Economics (BE), as well as by staff in offices throughout the agency.[1]

The FTC's Bureau of Competition (BC) enforces the nation's antitrust laws, promoting the interests of consumers and supporting unfettered markets resulting in lower prices and more choices. The Federal Trade Commission Act and the Clayton Act, both passed by Congress in 1914, give the Commission authority to enforce antitrust laws, which prohibit anticompetitive mergers and business practices that seek to prevent hard-driving competition, such as monopolistic conduct, attempts to monopolize, and conspiracies in restraint of trade.

The FTC's Bureau of Consumer Protection (BCP) enforces the nation's consumer protection laws, and works to protect consumers from a variety of fraudulent, deceptive, and unfair practices in the marketplace, including identity theft, telemarketing fraud, Internet fraud, and consumer credit issues. To further its consumer protection mission, the FTC brings civil and administrative law enforcement actions to enforce its laws and provides consumer and business education to enable the public to avoid common harms. The FTC works to ensure that consumers have accurate information for purchasing decisions, and confidence in the traditional and electronic marketplaces.

The FTC's Bureau of Economics (BE) supports BC's and BCP's law enforcement activities through the delivery of advanced economic and data analysis. In the antitrust area, BE participates in the investigation of alleged anticompetitive acts or practices and provides advice on the economic merits of alternative antitrust actions. In the consumer protection area, BE provides economic support and analysis of potential Commission actions in both cases and

[1] For a more detailed discussion of the mission of each Bureau and the FTC's law enforcement activities, see *About the Federal Trade Commission* at: http://www.ftc.gov/ftc/about.shtm

rulemakings. In addition, BE provides BC and BCP with analysis regarding remedies and appropriate penalty levels.

Other offices within the FTC also provide support to the agency's law enforcement activities. The Office of International Affairs (OIA) serves as an internal resource to Commission staff on international aspects of their work and as an FTC representative with international organizations. The Office of the General Counsel (OGC) is the FTC's chief legal officer and adviser, and represents the agency in court and provides legal counsel to the Commission, the operating bureaus, and other offices. The FTC's Office of the Executive Director (OED) serves as the operational backbone of the agency, providing financial and acquisitions management, human resources management, building management, information technology management, records management, and a myriad of administrative and managerial support tasks. In addition, the Offices of Policy and Planning (OPP), Congressional Relations (OCR), Public Affairs (OPA), and Inspector General (OIG), all provide direct and indirect support to the FTC's law enforcement mission.

2 System Overview

The FTC's LSS comprises various customized commercial off-the-shelf (COTS) hardware and software tools and resources that are used to accomplish e-discovery tasks. These e-discovery tasks typically include the following:

- capturing and/or obtaining information in a secure and forensically sound manner, including electronic and non-electronic (e.g. paper) information;
- storing / maintaining information in a secure and forensically sound manner;
- analyzing and processing information, including computer forensic analysis and processing, as well as analyzing, processing, formatting, and organizing information for easy search, retrieval, review, coding / annotation, and presentation;
- reviewing information, including searching, retrieving, reviewing, coding / annotating, and organizing information; and
- presenting information, including processing, formatting, and organizing information for presentation.

The LSS also provides resources for creating customized solutions to unique e-discovery challenges that may arise. The following are examples of some of the resources available within the LSS:

- the LSS maintains a number of forensic laptops and write blocking devices that are used in conjunction with forensic software tools to capture information during immediate access actions,[2] and which can be used by staff to review electronic information in a live computing environment without the risk of contamination;

[2] Section 13b of the FTC Act (15 USCS § 57b) provides the FTC with the authority to commence civil actions in U.S. District Courts or in State courts with competent jurisdiction. Pursuant to this statute, the FTC may ask a court to issue an order providing the FTC with direct and immediate

- the LSS maintains an inventory of computing and networking equipment for creating temporary e-discovery workspaces / mobile e-discovery units, which can be used to solve unique document review issues (e.g. the review of large volumes of voice recordings[3]), or to support the needs of trial teams;
- the LSS provides tools and computer applications for performing data analysis;
- the LSS maintains an inventory of encrypted hard drives for use in transferring data from the FTC to others; and
- the LSS has access to advanced litigation support services through the Department of Justice's (DOJ) Automated Litigation Support Contract ("Mega").

The LSS may collect and store information that is obtained from various sources (see section 3.2 for a more detailed discussion). Typically, the FTC obtains information from targets of its law enforcement activities and from individuals and entities with information that may be relevant to the FTC's investigations. This information may be provided to the FTC voluntarily (e.g. from companies that wish to merge, or from consumers who file complaints with the FTC), or information may be obtained via compulsory process (e.g. via a CID) or discovery. For internal matters, the FTC may obtain information directly from its computer systems or from the computers that are issued to the agency's employees and contractors. Information may also be obtained from public sources such as the Internet.

The LSS systems are managed by BCP's Division of Planning and Information (DPI), BC's Technology and Information Management Office (TIM), and the FTC's Office of Information Technology Management (OITM). DPI, TIM, and OITM staff work together to maintain the LSS.

The LSS is primarily used by law enforcers (e.g. attorneys, investigators, paralegals) in the FTC's Bureau of Competition and the FTC's Bureau of Consumer Protection[4], and by technologists in BC/TIM, BCP/DPI, and OITM, as well as by authorized contractors and law enforcement partners. The LSS may also be used by staff in other FTC offices – e.g. the FTC's Office of General Counsel (OGC), the Office of the Inspector General (OIG), the Office of International Affairs (OIA), and BE. In addition, the FTC may retain experts or contractors who may be given access to portions of the LSS. These various groups are referred to in this PIA as "users."

The LSS provides users with computing resources, tools, and environments that are tailored to the processing needs and security risks inherent in the information to be accessed and processed. Information that may pose heightened security risks[5] or that may require significant

---

access to a target's premises and computing facilities so that the FTC can obtain documents, electronically stored information, and other relevant information.

[3] For example, the FTC may obtain large volumes of voice recordings as part of an investigation of alleged telemarketing abuses. Typically, this would include copies of recordings a telemarketer made to verify that a customer agreed to a particular commercial transaction.
[4] The Bureau of Consumer Protection law enforcers include staff in the eight FTC regional offices.
[5] Information that may pose heightened security risks may include sensitive and proprietary business information or PII (for a detailed discussion of this type of information, see section 3.1).

computing resources is processed by technologists in BC/TIM, BCP/DPI, and/or OITM, in a secure portion of the LSS that is isolated from the FTC's production (computer) network and servers (GSS)[6] and that is dedicated to forensic and e-discovery processing (the Litigation Support Lab).[7] Alternatively, this information may be obtained and processed by law enforcement partners or contractors retained by the FTC to work on specific matters. Once processed in the Litigation Support Lab portion of the LSS, or by law enforcement partners and/or contractors, information that is appropriate to be placed on the GSS is copied to the FTC's production network and made available for search and review by case teams in the production network portion of the LSS. Information in the production network portion of the LSS is protected by the technical and procedural controls of the FTC's GSS, which restrict access to authorized users, and include security monitoring, and auditing and remote access controls. In addition, when needed, the LSS provides customized solutions to meet unique or unusual requirements.

3 Information Collected and Stored within the System

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

The LSS may collect and store any information that the FTC might obtain as part of its law enforcement and other activities. Typically, this will include information in various electronic and non-electronic formats, such as the following:

- word processing files
- spreadsheets
- databases
- emails
- images
- videos
- audio files
- boxes of paper documents

Information collected and stored within the LSS may include sensitive information of many types. (The main focus of this Privacy Impact Assessment (PIA) is on personally identifiable information (PII).) For example, during a merger case, the FTC/BC may obtain large volumes of sensitive and proprietary business information, including pricing information, planning information, financial reports, strategic plans, contracts, sales reports, securities filings, organization charts, emails, sales data, invoices, specific project information, and other company records, some of which may include sensitive information about individuals (e.g., employee information or detailed customer data).. As part of a consumer protection matter, the FTC/BCP also may obtain large volumes of

---

In addition, the FTC may obtain ESI that contains computer viruses, spyware, and other forms of malware.

[6] The FTC's production network is a wide area network (WAN), and is the networking "backbone" of the agency – connecting desktop computers, servers, printers, scanners, network storage devices, etc. together into a seamless computing environment. The FTC's production network is part of the agency's general support systems (GSS).

[7] Access to the Litigation Support Lab (LSL) is restricted to staff in BC/TIM, BCP/DPI, and OITM.

sensitive information, typically including sensitive health information and PII, but typically not sensitive business information. For example, during a consumer protection investigation, the FTC/BCP may obtain large volumes of consumer complaints, consumer transaction data, financial transaction data, banking records, credit reports, contracts, patient records, and employee records, all of which may include sensitive health information and other PII such as names, addresses, telephone numbers, E-mail addresses, birth dates, social security numbers / tax ID numbers, bank account numbers, and credit card numbers.

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

The LSS contains information obtained from a variety of sources, including information provided to the FTC voluntarily, obtained via compulsory process, obtained via discovery, or through other investigative sources.

Voluntary submissions may include information provided to the FTC by consumers, private sector entities, law enforcement partners, and others. Voluntary submissions from consumers are typically obtained from the FTC's Consumer Response Systems and Services (CRSS) system, as well as from the FTC's Spam Database.[8] Voluntary submissions from private sector entities and others are obtained through a variety of means (e.g. Hart-Scott-Rodino (HSR) filings, "whistleblowers", interest groups, etc.). Voluntary submissions from law enforcement partners are typically obtained in those cases where an FTC target is also the target of another law enforcement entity.

Information obtained via compulsory process includes information provided to the FTC pursuant to any one of the mechanisms available to the agency for compelling or forcing an individual or entity to provide information. These mechanisms typically include civil investigative demands (CIDs), access orders, subpoenas, and other types of court orders.[9]

Information obtained via discovery includes information provided to the FTC pursuant to any one of the mechanisms available to parties litigating matters in the Federal Courts of the United States. These mechanisms typically include requests for admissions, sworn statements (e.g. declarations, affidavits, depositions, and interrogatories), and electronic and documentary evidence.

The FTC may also obtain information from other investigative sources. Other investigative sources may include information that is available to the public (e.g. on the internet[10]), as well as sources that are not publicly available, such as from other investigative databases (e.g. the Financial Crimes Enforcement Network[11]), from other law enforcement agencies, and/or from commercial sources (e.g. Lexis / Nexis).

---

[8] See http://www.ftc.gov/os/2008/06/pia-crss.pdf for a copy of the CRSS PIA. See <INSERT LINK> for a copy of the Spam Database PIA.
[9] See http://www.ftc.gov/ogc/brfovrvw.shtm for an overview of the Commission's investigative and law enforcement authority.
[10] See <INSERT LINK> for a copy of the Internet Lab's PIA.
[11] See http://www.fincen.gov/foia/pia.html.

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

As described in the introduction and system overview (see sections 1 and 2), the LSS may collect and store information as part of its law enforcement and other activities, including to investigate potential or alleged violations of anticompetitive practices; to investigate and enforce statutes protecting consumers against fraudulent, deceptive, or unfair practices in the marketplace; to resolve consumer complaints; to locate victims; to assist with redress; to investigate internal matters; and to defend against suits brought against the agency.

3.4 How is the information collected?

As described in the system overview (see section 2) and in 3.2, the LSS may collect and store information that 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 email or some other electronic submission mechanism (e.g. through a website collection mechanism).[12]

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).

As discussed previously (see sections 2 and 3.2), 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,[13] from other law enforcement databases, or from commercial sources.

In addition, to support internal investigations and to defend against suits brought against the agency, the FTC may collect / copy information directly from its own systems.

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

Information that is used by the FTC as part of its law enforcement and other activities is reviewed for accuracy and timeliness as required by the particular activity. For example, staff performing an investigation based upon a "whistleblower" complaint may check the information that is obtained to ensure that it is timely and accurate. In other cases, the individual submitting the

---

[12] See e.g., http://www.ftc.gov/os/2008/06/pia-crss.pdf for a copy of the CRSS PIA

[13] See <INSERT LINK> for a copy of the Internet Lab's PIA, which includes a discussion of the tools available to staff for collecting information from the internet.

information may also be required to certify the accuracy of the information (e.g., witness or financial statements in court cases).

Information collected by the LSS is also subject to appropriate security and chain-of-custody controls. These controls 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 LSS. These controls provide the FTC with tools to verify that information stored within the LSS has not been changed.

3.6 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 LSS does not employ any new technologies, although the establishment of the LSS centralizes the data collection and e-discovery functions for efficiency. The LSS does not use technologies in ways that raise privacy concerns not otherwise discussed in this document. In addition, information that is collected and stored in the LSS is not combined and / or loaded in a single database. The FTC is not engaged in data mining and the data is not used for this purpose.[14]

3.7 What law or regulation permits the collection of this information?

Several statutes authorize the FTC to collect and store information in the LSS, including the Federal Trade Commission Act, 15 U.S.C. §§ 41-58, the Sherman Act 15, U.S.C. § 1–7, the Clayton Act, 15 U.S.C. § 12–27, 29 U.S.C. § 52–53, the Hart-Scott-Rodino Antitrust Improvements Act, 15 U.S.C. § 18a, and the Robinson-Patman Act, 15 U.S.C. § 13. These statutes not only authorize the collection of information, but they also have provisions that limit the disclosure of the data.

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

As discussed in the system overview (see section 2), the LSS collects and stores large volumes of information, some of it sensitive, that is obtained from various sources. Information may include sensitive business information, which if lost could result in significant monetary injury, but such business information poses no privacy risks. In contrast, privacy risks are raised by sensitive PII and sensitive health information, which if lost could result in financial, reputational, or other personal harm to individuals. The primary risks posed by the collection and storage of this information in the LSS are those associated with, and flowing from, the potential loss of control of this information. To mitigate the risks associated with collecting and storing this information, the FTC has implemented a number of safeguards, as discussed below.

As discussed in the system overview (see section 2), the LSS provides users with computing resources, tools, and environments that are tailored to the processing needs and security risks

---

[14] See the Federal Agency Data Mining Reporting Act of 2007, Pub. L. No. 110-53, 121 Stat. 266, §804(b)(1) for a definition/description of the term “data mining.”

inherent in the information to be accessed and processed. Information that may pose heightened security risks or that may require significant computing resources is processed by technologists in BC/TIM, BCP/DPI, and/or OITM, in a secure portion of the LSS that is isolated from the FTC's production network and servers (GSS) and that is dedicated to forensic and e-discovery processing (the Litigation Support Lab).[15] Access to the Litigation Support Lab is restricted to authorized staff in BC/TIM, BCP/DPI, and OITM. Temporary/visitor access may be granted to other users on a case-by-case basis.

Once processed in the Litigation Support Lab portion of the LSS, or by law enforcement partners and/or contractors, information that is appropriate to be placed on the GSS is copied to the FTC's production network and made available for search and review by case teams in the production network portion of the LSS. Information in the production network portion of the LSS is protected by the technical and procedural controls of the FTC's GSS, which restrict access to authorized users, and include security monitoring, and auditing and remote access controls.

For duplication or digitization of information from physical / paper format, the FTC has implemented controls that require, when possible, the use of approved vendors whose security controls have been vetted. When approved vendors are not available, due to a lack of presence in a specific locale, or because of workload, the FTC requires staff use alternative controls that are tailored to the risks associated with the information that is present in the document collection. Typically, alternative controls include the use of appropriate confidentiality and non-disclosure agreements, coupled with a review of the vendor's operation, and the receipt of sufficient assurances as to the procedures that will be used to assure the security and confidentiality of the information. Alternative controls may also include direct supervision of the vendor.

Information obtained in physical / paper format or electronically stored on removable media is subject to FTC polices for handling and safeguarding sensitive PII. In addition, the FTC has adopted and published detailed procedures for managing information that it receives.[16]These controls serve to mitigate the privacy risks associated with information once it is received by the FTC. To address the risks associated with transportation of electronic data to and from the FTC, the agency requires that data be encrypted with National Institute of Standards and Technology (NIST) certified cryptographic modules, when possible. When encryption is not feasible due to technical limitations or cost, or the information is provided in physical / paper format, the agency requires the use of alternative controls that are tailored to the risks associated with the data being transferred. Typically, alternative controls involve the use of couriers who are required to maintain possession of data as it is being transported. In addition, the FTC has implemented procedures that require management authorization prior to shipping sensitive information outside of the agency, as well as the creation of a log entry to record details about the information being shipped and its destination.

4 Use and Access to Data in the System

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

[15] Access to the Litigation Support Lab (LSL) is restricted to staff in BC/TIM, BCP/DPI, and OITM.
[16] See e.g., 16 CFR § 2.16 and 15 USCS §§ 57b-1 and 57b-2.

As discussed in the introduction and system overview (see sections 1 and 2), information in the system may be used to support the FTC's law enforcement and other activities, including to investigate potential or alleged violations of anticompetitive practices; to investigate and enforce statutes protecting consumers against fraudulent, deceptive, or unfair practices in the marketplace; to resolve consumer complaints; to locate victims; to assist with redress; to investigate internal matters; and to defend against suits brought against the agency.

4.2 Which internal entities will have access to the information?

As discussed in the system overview (see section 2), the LSS is accessible by staff throughout the agency.[17] The LSS is used by law enforcers (e.g. attorneys, investigators, paralegals) in the FTC's Bureau of Competition (BC) and the FTC's Bureau of Consumer Protection (BCP), and by technologists in BC/TIM, BCP/DPI, and OITM. The LSS may also be used by staff in other FTC offices – e.g. the FTC's Office of General Counsel (OGC), the Office of the Inspector General (OIG), the Office of International Affairs (OIA), and the Bureau of Economics (BE).

4.3 Which external entities will have access to the information?

As discussed in the system overview (see section 2), the LSS may be accessed by authorized contractors and law enforcement partners.[18] The FTC may also share information with courts, opposing counsel, defendants, expert witnesses, or other individuals as otherwise authorized by the law, although these entities and individuals do not have access to the LSS themselves.[19]

5 Notice and Access for Individuals

5.1 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 use and disclosure of information at the time information is collected. For information that is collected pursuant to a request from the FTC, notice is provided as part of the request (e.g. in a letter request, or in the document outlining the compulsory process request). For information that is collected via an FTC sponsored website or telephone call center, notice is also given at the point of collection.[20] On those occasions where the FTC cannot provide notice at the time information is collected (e.g. information contained in system maintained by other organizations), the FTC provides notice via its privacy policy, its Privacy Act system of records notices (SORNs), and its

---

[17] See section 7.2 for a discussion of LSS user access controls.
[18] See e.g., 16 CFR § 4.11 (c), (d) and (j) for information regarding FTC rules for sharing information with law enforcement partners.
[19] See e.g., 16 CFR § 4.11. In addition, the FTC also has internal policies regarding the redaction of PII.
[20] See e.g., notices provided to consumers by the CRSS system - https://www.ftccomplaintassistant.gov/. Also see the FTC's Privacy Policy - http://www.ftc.gov/ftc/privacy.shtm.

PIAs, including this one.[21] With regard to information collected from internal FTC systems for internal investigations or for the defense of suits brought against the agency, all staff are informed that the agency's computing systems are monitored, and that personal information may be collected. Notices are provided to staff at logon, and are also provided in administrative manuals, agency policy documents, and during employee training.

Individuals who provide the FTC with information pursuant to discovery or a related court order are not provided with specific notice by the FTC as to how information will be used or disclosed. Rather, the use and disclosure of this information is controlled by applicable discovery rules and court orders.

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

Individuals that provide the FTC with information on a voluntary basis may choose to decline to provide such information. However, individuals do not have a right to decline to provide information that is required by law or that is required to be provided via compulsory process.

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

Individuals do not have a right to consent to particular uses of the information stored in the system.

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

Individuals may make a request under the Privacy Act for access to information maintained about themselves in the LSS or other FTC record systems. See section 9 (Privacy Act) below. 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.[22] Privacy Act requests must be made in writing and submitted to the FTC's Office of General Counsel (see http://www.ftc.gov/foia/privactabout.shtm for more information). However, due to the law enforcement nature of the system, records in the system about certain individuals (e.g., defendants) may be exempt from mandatory access by such individuals. See 16 C.F.R. 4.13(m) (exemptions applicable to certain FTC Privacy Act systems of records).

Apart from the Privacy Act, once an FTC investigation is concluded, individuals (e.g., investigatory targets) who have provided information or materials under compulsory process (e.g., civil investigative demand) or voluntarily during the investigation may make a written request to FTC staff for the return of any such information or materials, excluding information or

---

[21] See the FTC's Privacy Policy - http://www.ftc.gov/ftc/privacy.shtm, and SORNs - http://www.ftc.gov/foia/listofpaysystems.shtm, and PIAs - http://www.ftc.gov/ftc/privacyimpactassessment.shtm.

[22] See http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=e561eb1eb77f7b01c1349a2690d8ceaa&rgn=div8&view=text&node=16:1.0.1.1.5.0.5.13&idno=16.

materials that the FTC is entitled or required by law to withhold or preserve See 15 U.S.C. 57b-2 (FTC Act), 16 C.F.R. 4.12 (FTC Rules of Practice).

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

Individuals seeking LSS records about themselves do not have access to the LSS, so no privacy risks associated with the process of providing individuals with access to their own records through the system were identified.

6 Web Site Privacy Issues

The LSS does not operate a website. Therefore, no website privacy issues were identified.

7 Security of Information in the System

7.1 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 to ensure that information collected through the LSS is appropriately secured.

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

All staff in the FTC are provided with access to the production network portion of the LSS. However, access to data is restricted to individuals based on their organization and work assignments. In addition, sensitive information is only available to staff whose work requires such access.

Access to the Litigation Support Lab portion of the LSS is restricted to authorized staff in BC/TIM, BCP/DPI, and OITM. Temporary/visitor access may be granted to other users on a case-by-case basis.

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

All FTC employees are required to complete computer security training and privacy awareness training annually. Interactive online training covers topics such as how to properly handle sensitive PII and other data, online threats, social engineering, and the physical security of documents. Individuals with significant security responsibilities are required to undergo additional, specialized training, tailored to their respective responsibilities.

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

An electronic keycard system restricts physical access to the LSS facilities, including BC offices, BCP shared spaces, and the Litigation Support Lab. Once data is moved to the production network, FTC policies for handling and safeguarding sensitive health information and PII apply.

In addition, ITM's Operations Assurance branch performs monthly audits of the FTC's production network.

Any questions regarding the security of the LSS should be directed to the FTC's Chief Information Security Officer, Margaret Mech, at (202) 326-2609.

8 Data Retention

8.1 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). In competition investigations, information is destroyed or returned to its owners one month after the conclusion of the matter.

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

Disposal of all information will be conducted in accordance Office of Management and Budget (OMB) and NIST guidelines.[23] For the destruction of removable media and hard drives, the FTC has retained a vendor whose methods meet or exceed applicable standards for media sanitization and destruction.

8.3 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 LSS and the steps that the FTC has taken to mitigate those risks is provided in section 3.8, above. In addition, data that is retained in the LSS 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 strict chain-of-custody controls and logging procedures. In addition, the FTC maintains a list of the information it has received, and performs periodic inventories and audits to ensure that the information is maintained in a safe and secure manner.

As to information disposal, the FTC follows applicable NIST and OMB standards for media sanitization (see section 8.2), and has not identified any additional risks associated with information disposal.

9 Privacy Act

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

[23] See NIST Special Publication 800-88, Guidelines for Media Sanitization.

Information contained in the LSS may be retrieved by one or more personal identifiers (e.g. name, physical address, e-mail address, telephone number, etc.), which makes such records subject to the Privacy Act.

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

The FTC SORN applicable to the Litigation Support System is I-1, Nonpublic Investigational and Other Nonpublic Legal Records.[24]

10 Privacy Policy

10.1 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.

Although the LSS does not operate any Web site that would require the posting of a privacy policy, the collection, use, and disclosure of the information in the LSS has been reviewed to ensure consistency with the FTC's privacy policy posted on its main Web site.

[24] See http://www.ftc.gov/foia/sysnot/i-1.pdf.

11. **Approval and Signature Page**

Prepared for the Business Owners of the System by:

_____ Date: _____

David Torok
Associate Director, BCP
Division of Planning Information

Review:

_____ Date: _____

Alexander C. Tang, Attorney
Office of the General Counsel

_____ Date: _____

Kellie Cosgrove Riley
Acting Chief Privacy Officer

_____ Date: _____

Margaret Mech
Chief Information Security Officer

Approved:

_____ Date:

Stanley Lowe
Chief Information Officer