Federal Trade Commission
Privacy Impact Assessment
for the: Bureau of Consumer Protection
Litigation Support System

March 2011

The Federal Trade Commission's (FTC) 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, BCP 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. BCP works to ensure that consumers have accurate information for purchasing decisions, and confidence in the traditional and electronic marketplaces. Increasingly, these activities involve electronically stored information (ESI) and the use of electronic discovery (e-discovery) tools and services, including computer forensics.

To support the this growing need for e-discovery tools and services, the BCP's Division of Planning and Information (DPI) has created a Litigation Support System (LSS). The services and tools provided by the LSS help attorneys, investigators, and other staff acquire, analyze, organize, and present large volumes of complex information and evidence.

1 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, acquiring, 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;
- process and prepare information for use in litigation support document management systems and other desktop-based review tools
- set up, create, load, and maintain databases;
- assist in the production of electronic data to opposing counsel, third parties, and courts;
- reviewing information, including searching, retrieving, coding / annotating, and organizing information; and
- preparation of ESI for courtroom 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[1] 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;
- 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").[4]

The LSS may collect, acquire, and store information that is obtained from various sources (see section 3.2 for a more detailed discussion). Typically, the LSS obtains information from targets of BCP's law enforcement activities and from individuals and entities with information that may be relevant to the BCP investigations. This information may be provided to the FTC voluntarily (e.g. 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 is managed by DPI with support from the FTC's Information Technology Management Office (ITMO).

---

[1] Write blockers are devices that allow acquisition of data on a drive (storage device) without damaging or corrupting the drive contents.
[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. Pursuant to this statute, the FTC may ask a court to issue an order providing the FTC with direct and immediate access to a target's premises and computing facilities so that the FTC can obtain documents, ESI, 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] http://www.justice.gov/civil/docs_forms/Mega%203%20Statement%20of%20Work.pdf

The LSS is primarily used by law enforcers (e.g. attorneys, forensic accountants, investigators, paralegals) and technologists in the BCP[5], 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 the Bureau of Economics (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 secure working environment tailored to meet the processing and security needs of the information being accessed and processed. Information that may pose heightened security risks[6] or that requires significant computing resources is processed by technologists in a secure network isolated from the FTC's production (computer) network and servers (GSS)[7] and that is dedicated to forensic and e-discovery processing. 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 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. Information in the production network is protected by the technical and procedural controls of the FTC's GSS. In addition, when needed, the LSS provides customized solutions to meet unique or unusual requirements.

---

[5] The BCP law enforcers include staff in the ten satellite locations, (two in Washington, D.C. and one in each of the eight FTC regional offices).

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

[7] 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). (We will link to GSS PIA when that is completed this Spring)

2 Information Collected and Stored within the System

2.1 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, including sensitive personally identifiable information (PII) of individuals other than FTC employees and contractors. 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 SHI 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. Sensitive PII may relate to specific defendants, individual targets of investigations, employees of corporate defendants or targets, witnesses, consumers, or victims of fraud.

2.2 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[8] 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 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, Dunn & Bradstreet, Westlaw, etc.,).

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

As described in the introduction and system overview (see section 1), the LSS may collect and store information as part of its law enforcement and other activities, including to investigate and enforce statutes and regulations protecting consumers against fraudulent, deceptive, or unfair practices in the marketplace; to locate victims; to assist

---

[8] See http://www.ftc.gov/os/2011/01/1101crss-pia.pdf for a copy of the CRSS PIA.
[9] See http://www.ftc.gov/ogc/brfovrvw.shtm for an overview of the Commission's investigative and law enforcement authority.
[10] See http://www.ftc.gov/os/2011/01/1101bcpinternetlab.pdf for a copy of the Internet Lab's PIA.
[11] See http://www.fincen.gov/foia/pia.html.

with redress; to investigate internal matters; and to defend against suits brought against the agency.

2.4 How is the information collected?

As described in the system overview (see section 1) and in 2.2, 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.

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 1 and 2.2), 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,[12] 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.

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

---

[12] See http://www.ftc.gov/os/2011/01/1101bcpinternetlab.pdf 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 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 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.

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?

No. The LSS uses advanced tools (software and hardware) for litigation support that enable users to acquire, analyze, organize, and present large volumes of digital evidence. These tools include typical desktop software applications as well as litigation support software applications such as Concordance, Summation, TrialDirector, CaseMap, Encase, and Forensic ToolKit. These tools do not employ new technologies not previously employed by the FTC, although the establishment of the LSS centralizes the data collection and e-discovery functions for efficiency. 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.[13]

Program managers for LSS are continuously evaluating new software and hardware to increase efficiency and respond to new technologies used by third parties. The upgrade of current software and applications or the acquisition of increased processing power does not constitute the use of new technologies that have not been previously employed at the FTC. New technologies are acquired in consultation with the Chief Privacy Officer and the LSS PIA will be updated as appropriate where new technologies may impact individual's privacy.

[13] 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."

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

The Federal Trade Commission Act, 15 U.S.C. §§ 41-58, authorizes the FTC to collect and store this information.

2.8 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 1), the LSS collects and stores large volumes of information, some of it sensitive that is obtained from various sources. Some matters involve multiple terabytes of information. 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, which if lost could result in financial, reputational, or other personal harm to individuals. The primary risks posed by the collection, processing, sharing, 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 1), the LSS provides users with computing resources and tools in an environment that is tailored to the processing needs and security risks 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 in the secure LSS, a network that is isolated from the FTC's production network and servers (GSS) and that is dedicated to forensic and e-discovery processing.

Physical access to DPI's server room and ligation support office spaces is restricted to authorized staff in BCP/DPI, and ITMO. Temporary/visitor access may be granted to other users on a case-by-case basis.

Once processed in 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. Other data may remain available for search and review by case teams within the LSS. Information in the production network portion of the LSS is protected by the technical and procedural controls of the FTC's GSS. Access is restricted to authorized users, including security monitoring, auditing, and remote access controls in both the LSS and FTC GSS networks.

For duplication or digitization of information from physical / paper format, the BCP/DPI 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 BCP/DPI 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.[14] 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.

3 Use and Access to Data in the System

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

As discussed in the introduction and system overview (see section 1), information in the system may be used to support the BCP's law enforcement and other activities, including to investigate and enforce statutes and regulations protecting consumers against fraudulent, deceptive, or unfair practices in the marketplace; to locate victims; to assist with redress; to investigate internal matters; and to defend against suits brought against the agency.

[14] See e.g., 16 CFR § 2.16 and 15 USCS §§ 57b-1 and 57b-2.

3.2 Which internal entities will have access to the information?

As discussed in the system overview (see section 1), the LSS may be accessed by law enforcers (e.g. attorneys, forensic accountants, investigators, paralegals) and technologists in BCP and by specific technologists in ITMO. The LSS may also be accessed by staff in other FTC offices – e.g. the OGC, OIG, the OIA, and BE on a case by case basis.

3.3 Which external entities will have access to the information?

As discussed in the system overview (see section 1), the LSS may be accessed by authorized contractors and law enforcement partners.[15] BCP 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.[16]

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 required, 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.[17] On those occasions where the FTC cannot provide notice at the time information is collected (e.g. information contained in systems maintained by other organizations), the FTC provides notice via its privacy policy, its Privacy Act system of records notices (SORNs), and its

---

[15] See e.g., 16 CFR § 4.11 (c), (d) and (j) for information regarding FTC rules for sharing information with law enforcement partners.
[16] See e.g., 16 CFR § 4.11. In addition, the FTC also has internal policies regarding the redaction of PII.
[17] 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.[18] 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.

4.2 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 such as via compulsory process.

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

Individuals generally do not have a right to consent to particular uses of the information stored in the system. An exception is in FTC administrative or court proceedings, where individuals may in some cases limit the agency's use or disclosure of their information that may be stored in the system (e.g., under a stipulated pre-trial protective order or other binding agreement in discovery).

4.4 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

---

[18] 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.

(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. 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 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).

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 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.

5 Web Site Privacy Issues

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

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 LSS follows all applicable Federal Information Security Management Act (FISMA) requirements to ensure that information collected is appropriately secured.

6.2 Has a Certification & Accreditation been completed for the system or supporting program?

The Litigation Support System Certification & Accreditation activities were completed in September 2010. Authorization of the system is pending.

6.3 Has a risk assessment been conducted on the system?

The Litigation Support System risk assessment was completed in September 2010.

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

The Litigation Support System does not employ technologies that raise privacy concerns not already addressed.

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

Access to the Litigation Support System (including physical access to the DPI server room and staff offices) is restricted to authorized staff in BCP/DPI and ITMO. Temporary/visitor access may be granted to other users on a case-by-case basis.

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.

6.6 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 and privacy awareness training annually. Interactive online training covers topics such as properly handling of 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. Litigation support services contractors who access the Litigation Support System are also required to complete computer security training and privacy awareness training annually.

In addition, BCP LSS staff complete security training and privacy awareness training twice a year.

6.7 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 DPI's server room, BCP shared spaces and staff offices, and the Litigation Support Lab. Once data is moved to the production network, FTC policies for handling and safeguarding sensitive PII apply.

In addition, DPI staff perform regular audits of the LSS network system event logs and keycard access logs.

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.

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 National Archives and Records Administration (NARA).[19]

Information collected for the purpose of monitoring LSS usage, including access, system event, and device usage logs, is to be deleted or destroyed when the FTC determines it is no longer needed for audit purposes. The FTC has submitted to NARA a comprehensive records disposition schedule, SF-115 Request for Disposition Authority. Pending NARA approval, FTC will manage usage information in a manner consistent with 44 U.S.C. Ch. 31, 44 U.S.C. 3506, 36 C.F.R. Ch. XII, Subchapter B, Records Management, and OMB Circular A-130, par. 8a1(j) and (k) and 8a4.

7.2 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.[20] 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.

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 LSS 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 LSS may be stored on external media, either in the form in which it

---

[19] For information about retention and disposal of this information, see SORN I-1, Nonpublic Investigational and Other Legal Records (http://www.ftc.gov/foia/sysnot/i-1.pdf).
[20] See NIST Special Publication 800-88, Guidelines for Media Sanitization.

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 7.2), and has not identified any additional risks associated with information disposal.

8 Privacy Act

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

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.

8.2 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.[21]

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.

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.

---

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

10 Approval and Signature Page

Prepared for the Business Owners of the System by:

_____ Date: _____

David M. Torok
Associate Director, BCP
Division of Planning Information

Review:

_____ Date: _____

Alexander C. Tang, Attorney
Office of the General Counsel

_____ Date: _____

Marc Groman
Chief Privacy Officer

_____ Date: _____

Margaret Mech
Chief Information Security Officer

_____ Date: _____

Jeff Nakrin
Director, Records and Fillings Office

Approved:

_____ Date: _____

Jeff Huskey
Chief Information Officer