



**Federal Trade Commission
Privacy Impact Assessment**

Electronic Discovery Support System

November 2013

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 law enforcement activities such as performing investigations and litigating cases. Increasingly, these activities involve electronically stored information and the use of electronic discovery (e-discovery) tools and services, including computer forensics.

In addition to the FTC's law enforcement activities, the agency performs internal investigations and defends itself in legal actions 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 an Electronic Discovery Support System (EDSS).

1.1 Law Enforcement Activities

The FTC's law enforcement activities are supported by its 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, promotes the interests of consumers, and supports unfettered markets to produce 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 and provides consumer and

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

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 rulemakings. In addition, BE provides BC and BCP with analysis regarding remedies, including appropriate monetary relief.

Other offices within the FTC also support 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 to international organizations. The Office of the General Counsel (OGC), is the FTC's chief legal officer and adviser, 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 EDSS uses various customized commercial off-the-shelf (COTS) hardware and software tools and resources to accomplish e-discovery tasks. These e-discovery tasks typically include the following:

- Capturing or obtaining information in a secure and forensically sound manner, including electronic and non-electronic (e.g., paper) information;
- Storing and maintaining information in a secure and forensically sound manner;
- Analyzing and processing information, including computer forensic analysis and data retrieval, as well as 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 EDSS also has resources to create customized solutions for unique e-discovery challenges that may arise. Resources available within the EDSS include:

- Forensic laptops and write-blocking devices that are used in conjunction with forensic software tools to capture information during immediate access actions² and that are used by authorized staff to review electronic information in a live computing environment without the risk of contamination;
- Computing and networking equipment to create temporary e-discovery workspaces and mobile e-discovery units to solve unique discovery and review issues (e.g., reviewing a large volume of voice recordings³), or to support the needs of trial teams;
- Tools and computer applications for performing data analysis;
- Encrypted hard drives for transferring data to and from the FTC; and
- Access to additional advanced litigation support services through the Department of Justice's (DOJ) Automated Litigation Support Contract ("Mega") to supplement available FTC and EDSS resources and capabilities.

The EDSS may collect and store information that the FTC obtains from a variety of 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. The FTC may obtain this information voluntarily (e.g., from companies that wish to merge, or from consumers who file complaints with the FTC), through compulsory process (e.g., pursuant to an FTC-issued Civil Investigative Demand (CID), subpoena, or other requests), or during formal discovery processes in federal or administrative proceedings. For internal matters, the FTC may obtain information directly from its computer systems and from the computers that are issued to the agency's employees and contractors. It may also obtain information from public sources such as the Internet.

The FTC's Office of the Chief Information Officer (OCIO), BCP's Division of Planning and Information (DPI), and BC's Technology and Information Management Office (TIM) work together to manage and maintain the EDSS.

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 collect and preserve key evidence, including documents, electronically stored information, and other relevant material.

³ For example, as part of an investigation into alleged telemarketing abuses, the FTC may obtain copies of voice recordings that a telemarketer made to verify that a customer agreed to a particular commercial transaction.

The EDSS is primarily used by law enforcement staff (e.g., attorneys, investigators, paralegals) in BC⁴ and BCP⁵; by technologists in BC/TIM, BCP/DPI, and OCIO; by OGC; and also by authorized FTC contractors and law enforcement partners. The EDSS may also be used by staff in other FTC offices, including OIG, OIA, and BE. In addition, the FTC may retain experts or contractors who may be given access to portions of the EDSS. These groups collectively are referred to in this PIA as “users.”

The EDSS provides users with computing resources, tools, and environments that are tailored to the FTC’s investigation, litigation, and presentation needs and that help reduce the privacy and data security risks associated with the information being accessed and processed. To protect the FTC production network⁶ all EDSS data is processed and loaded onto a secure portion of the EDSS called the Litigation Support Lab (LSL). The LSL isolates data that may pose heightened security or privacy risks,⁷ that may require significant or specialized computing resources, or that may include not only relevant but also irrelevant sensitive data. Access to the LSL is restricted to select authorized staff in BC/TIM, BCP/DPI, OGC, and OCIO. The LSL permits forensic and e-discovery processing to take place before data are placed onto the FTC production network. Alternatively, information may be obtained and processed offsite by the FTC’s law enforcement partners or by contractors retained by the FTC to work on specific matters (for example, under the Mega contract) before it is incorporated into the EDSS.

After BC/TIM, BCP/DPI, or OGC staff copy and process the information within the LSL portion of the EDSS, the resulting data are loaded into the EDSS Review System, which is a dedicated portion of the FTC production network. At this point, the data are still in the EDSS but are also available for use by authorized members of the case team. All information in the EDSS Review System is subject to and protected by the technical and procedural controls of the FTC Data Center GSS, including restricted access, security monitoring, and auditing and remote access controls.⁸ Access to EDSS data is limited to

⁴ The Bureau of Competition includes law enforcement staff in Headquarters and in three FTC regional offices.

⁵ The Bureau of Consumer Protection includes law enforcement staff in Headquarters and in all eight FTC regional offices.

⁶ The FTC 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 production network is part of the agency’s Data Center General Support System (Data Center GSS). For more information, see Data Center GSS PIA, <http://www.ftc.gov/os/2013/05/1305datacentepia.pdf>.

⁷ Information that may pose heightened security or privacy risks includes sensitive and proprietary business information, PII (for a detailed discussion of this type of information, see section 3.1), and electronically stored information, which may contain computer viruses, spyware, and other forms of malware.

⁸ See Data Center GSS PIA, <http://www.ftc.gov/os/2013/05/1305datacentepia.pdf>.

authorized staff from BC, BCP, BE and OGC who are assigned to the specific matter. Authorized staff must access data through the EDSS Review System, and EDSS data cannot be identified or accessed by searching or navigating other parts of the FTC production network.

Authorized BC/TIM and BCP/DPI staff can use the GSS Data Center virtual private network (VPN) to remotely process and copy data that has been loaded into the LSL, but the data can only be managed within the EDSS.

3 Information Collected and Stored within the System

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

The EDSS may collect, use, disseminate, and maintain 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, including:

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

Information collected and stored within the EDSS may include many types of sensitive information, although the focus of this Privacy Impact Assessment (PIA) is personally identifiable information (PII) within the EDSS. For example, during a merger case, 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, BCP may obtain large volumes of sensitive information, including health and financial information and other PII.

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

The EDSS contains information obtained directly from individuals and from third parties. The information is provided to the FTC voluntarily, via compulsory process, during discovery, or through other investigative means.

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 Sentinel Network Services (SNS) system.⁹ 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 CIDs, access orders, subpoenas, and other types of court orders.¹⁰

Information obtained via discovery includes information available to parties litigating matters in federal court or in administrative proceedings and typically includes information provided or received in response to 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, including information that is available to the public (e.g., on the Internet¹¹), as well as from sources that are not publicly available, such as investigative databases, other law enforcement agencies, and commercial sources (e.g., Lexis/Nexis).

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 FTC may collect and store information in the EDSS as part of its law enforcement and other activities, which may include investigating potential or alleged violations of anticompetitive practices; enforcing statutes that protect consumers against fraudulent, deceptive, or unfair practices in the marketplace; resolving consumer complaints; locating victims and potential witnesses; assisting with redress; investigating internal FTC matters; and defending the FTC in suits brought against the agency.

⁹ See SNS PIA, <http://www.ftc.gov/os/2013/01/130103sns pia.pdf>.

¹⁰ For an overview of the Commission's investigative and law enforcement authority, see <http://www.ftc.gov/ogc/brfovrw.shtm>.

¹¹ See BCP Internet Lab PIA, <http://www.ftc.gov/os/2011/01/1101bcpinternetlab.pdf>.

3.4 How is the information collected?

As described in the system overview (see section 2) and in 3.2, the EDSS 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 that is included in the EDSS 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. The information is generally incorporated into the EDSS directly from whatever media it is received on, including by copying information from paper-based sources or from removable media such as CDs, DVDs, and hard drives or transferring information that is electronically submitted via a secure file transfer 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, 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 obtain 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 information may also be required to certify the accuracy of the information (e.g., witness or financial statements in court cases).

¹² See SNS PIA, <http://www.ftc.gov/os/2013/01/130103sns pia.pdf>.

Information incorporated into the EDSS is subject to appropriate security and chain-of-custody controls. In addition to protecting against unauthorized access, alteration, or dissemination, these controls reduce the risk of loss and assure the integrity of the evidentiary materials from the point at which they are included in the EDSS.

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 EDSS does not employ technologies in ways not previously used by the FTC. The establishment of a single FTC-wide EDSS to coordinate investigation, discovery, litigation, and other enforcement support functions that were previously performed separately within BC, BCP, and OGC will help coordinate and standardize FTC forensic, data collection and e-discovery practices for efficiency and consistency, including with regard to privacy and data security. Information that is collected and stored in the EDSS is segregated into matter-specific folders that can only be accessed by staff who are authorized to work on a particular matter.

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

A number of statutes authorize the FTC to collect and store the information contained in the EDSS, 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 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 EDSS collects and stores large volumes of information, some of it sensitive, that is obtained from various sources. Information may include sensitive business information and other nonpublic information, which if lost could result in significant monetary injury. In addition, the presence of PII within the EDSS creates privacy risks. Lost or compromised PII could result in financial, reputational, or other personal harm to individuals. The primary risks posed by the collection and storage of information in the EDSS are associated with, and flow from, the potential loss of control of this information, including unauthorized access, alteration, or dissemination. To mitigate these risks, the FTC has implemented a number of safeguards, as discussed below.

As discussed in the system overview (see section 2), the EDSS 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. To protect

the FTC production network, all EDSS data is processed in the LSL solely by technologists from BC/TIM, BCP/DPI, and/or OGC. Physical access to the LSL is restricted to authorized staff, and temporary or visitor access may be granted to other users on a case-by-case basis.

Staff who handle data in the LSL portion of the EDSS receive specialized training in its use. All staff who use the general EDSS receive training on how to use and access it.

Once information is copied and processed in the LSL portion of the EDSS, or received by the FTC in processed form from its law enforcement partners or contractors, it is then loaded onto the production network portion of the EDSS in a case-specific folder that can be searched and reviewed by authorized members of a case team. Information in the production network portion of the EDSS is protected by the same technical and administrative controls that protect the FTC Data Center GSS, which include limiting access to authorized users, security monitoring, auditing, and specific controls governing remote access.¹³ Authorized BC, BCP, and OGC staff can only access EDSS data through the EDSS Review System and are unable to search or navigate the other parts of the FTC production network to access EDSS information.

When staff need to duplicate or digitize EDSS information that is originally in a hard copy format, FTC controls require, when possible, use of approved vendors whose security controls have previously been vetted. When approved vendors are not available, as can happen because of location, time pressure, or workload or other conflicts, staff must use alternative controls that are tailored to the risks associated with the information, such as use of appropriate confidentiality and non-disclosure agreements, 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 and appropriate disposal of duplicate hard and electronic copies of the data. Depending upon the sensitivity of the information, alternative controls may also include direct supervision of the vendor while the work is being performed.

Information obtained in hard copy format or electronically stored on removable media is subject to FTC policies for handling and safeguarding 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

¹³ See Data Center GSS PIA, <http://www.ftc.gov/os/2013/05/1305datacentepia.pdf>.

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

possible. When encryption is not feasible due to technical limitations or cost, or the information is provided in hard copy 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 nature, type, and volume of information being shipped, the time and mode of transport, and the recipient.

4 Use and Access to Data in the System

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

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 EDSS is available to authorized staff throughout the agency.¹⁵ The EDSS is primarily used by law enforcement staff (e.g., attorneys, investigators, paralegals) in BC, BCP, and OGC and by technologists in BC/TIM, BCP/DPI, OGC, and OCIO. The EDSS may also be used by staff in other FTC offices, including OIG, OIA, and BE.

4.3 Which external entities will have access to the information?

As discussed in the system overview (see section 2), the EDSS may be accessed directly by authorized contractors and experts. The FTC may also share information with courts, opposing counsel, defendants, expert witnesses, law enforcement¹⁶ or other individuals as otherwise authorized by law, although these entities and individuals do not have direct access to the EDSS. Access by external entities will typically be conditioned upon compliance with non-disclosure agreements, contract provisions regarding privacy and

¹⁵ See section 7.2 for a discussion of access controls for EDSS users.

¹⁶ See, e.g., 16 CFR § 4.11 (c), (d) and (j) for information regarding FTC rules for sharing information with law enforcement partners.

data security protections, court-approved protective orders, or similar data protection controls.¹⁷

Authorized contractors and experts accessing the EDSS directly receive training on its use. Information shared with other parties is done as a data export.

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 given at the point of collection.¹⁸ 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 PIAs, including this one.¹⁹ 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.

¹⁷ See, e.g., 16 CFR § 4.11. In addition, the FTC also has internal policies regarding the redaction of PII.

¹⁸ See, e.g., notices provided to consumers by the SNS, <https://www.ftccomplaintassistant.gov/>. See also FTC Privacy Policy, <http://www.ftc.gov/ftc/privacy.shtm>.

¹⁹ See FTC Privacy Policy, SORNS, and PIAs, <http://www.ftc.gov/ftc/privacy.shtm>, <http://www.ftc.gov/foia/listofpaysystems.shtm>, and <http://www.ftc.gov/ftc/privacyimpactassessment.shtm>.

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

Yes, individuals who provide the FTC with information on a voluntary basis may choose to decline to provide that 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, and refusal to provide the information may result in legal action by the FTC.

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

No. Data sources who submit their information in FTC law enforcement investigations and mark their submissions confidential, however, may be afforded prior notice and opportunity to object to further disclosure, to the extent provided under section 21 of the FTC Act and the FTC's Rules of Practice, see, e.g., 16 C.F.R. 4.10 & 4.11.

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

Individuals may make a request under the Freedom of Information Act and Privacy Act for access to information maintained about themselves in the EDSS 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, for requests from the EDSS.²⁰ 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>). 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,

²⁰ 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>.

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).

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 EDSS records about themselves do not have direct access to the EDSS, so no privacy risks are associated with the process of providing individuals with access to their own records through the system. Nonetheless, to prevent the risk that records that the agency would be legally required to withhold from public disclosure may be improperly released to an individual purporting to be the subject of such records, the FTC may require additional verification of a requester's identity when such information is reasonably necessary to assure that records are not improperly disclosed. See section 9 below (Privacy Act).

6 Web Site Privacy Issues

Not applicable. The EDSS is not a website and can only be accessed remotely through the Data Center GSS's virtual private network (VPN), and then only for limited purposes by authorized staff.

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 EDSS is appropriately secured.

7.2 Has a Certification & Accreditation been completed for the system?

Yes. The EDSS is covered by the existing C&A for the Data Center GSS.

7.3 Has a risk assessment been conducted on the system?

Yes. A risk assessment was completed as part of the C&A for the Data Center GSS, and risks were also discussed in conjunction with consolidating litigation support activities into, and implementing, the EDSS and developing this PIA.

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

All staff in the FTC can access the production network portion of the EDSS. However, access to case-specific EDSS data is restricted to individuals based on their organization and work assignments. In addition, sensitive EDSS information is further limited to authorized staff whose work requires such access. Once staff no longer need access, that privilege is removed.

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

7.5 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 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.

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

An electronic keycard system restricts physical access to the EDSS facilities, including BC offices, BCP shared spaces, and the Litigation Support Lab. FTC policies for handling and safeguarding PII apply to the EDSS. In addition, OCIO's Operations Assurance branch performs monthly audits of the EDSS.

Questions regarding the security of the EDSS should be directed to the FTC's Chief Information Security Officer.

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 FTC policies and procedures and with [FTC records retention schedule N1-122-09-1](#) approved by the National Archives and Records Administration (NARA).

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

Disposal of all information will be conducted in accordance with FTC policies and procedures and in compliance with Office of Management and Budget (OMB) and NIST guidelines.²¹ 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 EDSS 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 EDSS 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 or unauthorized access. To mitigate these risks, all EDSS 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 that 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?

Yes. Information contained in the EDSS 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.

²¹ See NIST Special Publication 800-88, Guidelines for Media Sanitization.

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

Yes. The FTC SORN applicable to the Litigation Support System is I-1, Nonpublic Investigational and Other Nonpublic Legal Records.²² As noted earlier, subject individuals may make a request under the FOIA and Privacy Act for access, although some records may be exempt from disclosure, 16 C.F.R. 4.13(m), and the agency may require additional verification of the requester's identity to avoid improper disclosure of records to the wrong individual. See 16 C.F.R. 4.13(d).

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 EDSS 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 EDSS has been reviewed to ensure consistency with the FTC's privacy policy posted on its main Web site.²³

[Remainder of this page intentionally left blank]

²² See <http://www.ftc.gov/foia/sysnot/i-1.pdf>.

²³ See <http://www.ftc.gov/ftc/privacy.shtm>.

Approval and Signature Page

Prepared for the Business Owners of the System by:

_____ Date: _____
Edwin Acajabon, Assistant Director
Division of Planning and Information
Bureau of Consumer Protection

Review:

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

_____ Date: _____
Peter B. Miller
Chief Privacy Officer

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

_____ Date: _____
Jeffrey Smith
Chief Information Security Officer

Approved:

_____ Date: _____
Bajinder Paul
Chief Information Officer