



Federal Trade Commission
Privacy Impact Assessment

**Electronic Discovery Support System
(EDSS)**

Updated December 2016

Table of Contents

1	System Overview	1
2	Data Type, Sources, and Use	4
3	Data Access and Sharing	6
4	Notice and Consent	7
5	Data Accuracy and Security.....	9
6	Data Retention and Disposal.....	11
7	Website Privacy Evaluation.....	11
8	Privacy Risks and Evaluation	12
9	Approval and Signature Page.....	15

1 System Overview

1.1 Describe the project/system and its purpose.

The FTC works to prevent business practices that are anticompetitive, deceptive, or unfair to consumers and strives to enhance informed consumer choice and public understanding of the competitive process. The FTC engages in numerous activities that support this work, including law enforcement activities such as performing investigations and litigating cases. These activities often involve electronically stored information and the use of electronic discovery (e-discovery) tools and services, including computer forensics. 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

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, conducted primarily by the Office of the General Counsel (OGC), also require e-discovery tools and services similar to those used in the FTC's law enforcement work.

To support the agency's need for these services, the FTC has created an Electronic Discovery Support System (EDSS), which 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;
- Scanning non-electronic (e.g., paper) information into an electronic format;
- 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, software, write-blockers and other devices are used to capture information during immediate access actions², and 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;

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

² Pursuant to Section 13b of the FTC Act (15 U.S.C. § 57b), the FTC may seek a federal court order providing the FTC with immediate access to a defendant's business premises so that the FTC can collect and preserve evidence, including electronically stored information.

- Tools and computer applications for performing data analysis;
- Encrypted hard drives for transferring data to and from the FTC; and
- Access to additional litigation support services through the Department of Justice’s (DOJ) Mega4 Automated Litigation Support Contract to supplement available FTC and EDSS resources and capabilities. One such service – DOJ’s OMEGA Relativity Content Analytics (ORCA) application – is used by the FTC to process, store, and review information obtained through discovery and investigations.

The EDSS is primarily used by law enforcement staff (e.g., attorneys, investigators, paralegals) and technical specialists in BC,⁴ BCP,⁵ and OGC; by staff in the Office of the Chief Information Officer (OCIO); and by authorized FTC contractors, experts, and law enforcement partners. The EDSS may also be used by staff in other FTC offices, including OIG, OIA, and BE. 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. There are three distinct environments within the EDSS – the Litigation Support System, the EDSS Review System, and DOJ’s ORCA application.

To protect the FTC production network⁶, all EDSS data is first copied and processed onto a secure portion of the EDSS called the Litigation Support System (LSS).⁷ The LSS isolates data that may pose heightened security or privacy risks⁸ or that may require significant or specialized computing resources. Some data is stored in the LSS to permit specialized analysis of the data in a secure environment. Users must be inside the LSS to use the computers to manipulate the data; however they have the ability to read the stored data from outside the system. Users inside the LSS do not have access to the internet. Typically, the data undergoes forensic and e-discovery processing in the LSS before being placed into either the EDSS Review System or DOJ’s ORCA application. Access to the LSS is restricted to authorized staff and contractors in BC, BCP, OGC, and OCIO. These individuals can use the Data Center GSS virtual private network (VPN) to remotely process, copy, and analyze data that has been loaded into the LSS.

Occasionally, 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 DOJ’s Mega 4 contract) before it is incorporated into the EDSS. This data is copied to the LSS, potentially subject to further processing or analysis, and then incorporated into the EDSS Review System or DOJ’s ORCA application.

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.

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](#).

⁷ The Litigation Support System is also referred to as the Litigation Support Lab.

⁸ Information that may pose heightened security or privacy risks includes sensitive and proprietary business information, PII, and electronically stored information, which may contain computer viruses, spyware, and other forms of malware.

After information is copied and processed within the LSS portion of the EDSS, the resulting data is typically loaded into the EDSS Review System, which is a dedicated portion of the FTC production network. BC, BCP, and OGC technical specialists (and contractors performing similar duties) have access to the data in the EDSS Review System for the particular Bureau or Office with which they are working. Data in the EDSS Review System is also available for use by authorized members of the case team. Case team members have access to data only for the specific matters to which they are assigned. 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.⁹ Authorized staff must access data through the EDSS Review System; EDSS data cannot be identified or accessed by searching or navigating other parts of the FTC production network.

In some instances, after copying and processing the information in the LSS, the resulting data is loaded into the DOJ's ORCA application. The data is placed in case-specific databases, and access to the data is limited to authorized FTC staff, contractors, and law enforcement partners who are assigned to work on the specific matter. These individuals must access ORCA systems using two-factor authentication to access the application.

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

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.

⁹ See [Data Center GSS PIA](#).

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)¹⁰ may be collected or maintained in the system/project. Check all that apply.

<i>PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.</i>		
<input checked="" type="checkbox"/> Full Name	<input checked="" type="checkbox"/> Biometric Identifiers (e.g., fingerprint, voiceprint)	<input checked="" type="checkbox"/> User ID
<input checked="" type="checkbox"/> Date of Birth	<input checked="" type="checkbox"/> Audio Recordings	<input checked="" type="checkbox"/> Internet Cookie Containing PII
<input checked="" type="checkbox"/> Home Address	<input checked="" type="checkbox"/> Photographic Identifiers (e.g., image, x-ray, video)	<input checked="" type="checkbox"/> Employment Status, History, or Information
<input checked="" type="checkbox"/> Phone Number(s)	<input checked="" type="checkbox"/> Certificates (e.g., birth, death, marriage, etc.)	<input checked="" type="checkbox"/> Employee Identification Number (EIN)
<input checked="" type="checkbox"/> Place of Birth	<input checked="" type="checkbox"/> Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	<input checked="" type="checkbox"/> Salary
<input checked="" type="checkbox"/> Age	<input checked="" type="checkbox"/> Vehicle Identifiers (e.g., license plates)	<input checked="" type="checkbox"/> Military Status/Records/ ID Number
<input checked="" type="checkbox"/> Race/ethnicity	<input checked="" type="checkbox"/> Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	<input checked="" type="checkbox"/> IP/MAC Address
<input checked="" type="checkbox"/> Alias	<input checked="" type="checkbox"/> Geolocation Information	<input checked="" type="checkbox"/> Investigation Report or Database
<input checked="" type="checkbox"/> Sex	<input checked="" type="checkbox"/> Passport Number	<input checked="" type="checkbox"/> Driver's License/State ID Number (or foreign country equivalent)
<input checked="" type="checkbox"/> Email Address		<input type="checkbox"/> Other (<i>Please Specify</i>): _____
<input checked="" type="checkbox"/> Work Address		
<input checked="" type="checkbox"/> Taxpayer ID		
<input checked="" type="checkbox"/> Credit Card Number		
<input checked="" type="checkbox"/> Facsimile Number		
<input checked="" type="checkbox"/> Medical Information		
<input checked="" type="checkbox"/> Education Records		
<input checked="" type="checkbox"/> Social Security Number		
<input checked="" type="checkbox"/> Mother's Maiden Name		

Note: EDSS may collect, use, disseminate, and maintain any information that the FTC might obtain as part of its law enforcement and other activities. This may include any and all types of PII and sensitive information. To protect the FTC production network, all EDSS data is processed and loaded onto the LSS. Some data remains in the LSS to enable staff to conduct complex data analysis in a secure environment. Most data is processed in the LSS and then placed in the EDSS Review System, which is located on a portion of the FTC production network. Occasionally, data processed in the LSS is placed into DOJ's ORCA application.

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

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 includes information in various electronic formats, including: word processing files, spreadsheets, databases, emails, images, videos, audio files, etc. Information collected in non-electronic format (i.e., paper documents) are scanned into electronic form. Information collected and stored within EDSS may include many types of sensitive

¹⁰ Per OMB Circular A-130, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

information. 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 about individuals (e.g., employee information or detailed customer data). BCP also may obtain large volumes of sensitive and proprietary business information, such as planning information, sales data, and data security requirements.

2.3 What is the purpose for collection of the information listed above?

The FTC may collect and store information in EDSS as part of its law enforcement and other activities. These activities 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.

2.4 What are the sources of the information in the system/project? How is the information collected?

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. The FTC also may forensically acquire electronic information directly from a defendant's business premises pursuant to federal court order. If the FTC obtains paper documents, they are usually scanned into electronic form. 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 information is generally incorporated into the EDSS directly from whatever media it is received on, including by scanning information from paper-based sources or copying electronic information 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).

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

<i>Data Will Be Accessed By and/or Provided To:</i>	<i>How and Why the Data Will Be Accessed/Shared</i>
FTC Users	<p>Access is granted to the different environments within the EDSS depending on the user’s role. For the LSS, BC, BCP, OGC, and OCIO technical specialists (and authorized FTC contractors performing similar duties), have access to copy, process, and analyze data. Other BCP staff, such as data analysts, forensic accountants and investigators, are given access to specific folders within the LSS to conduct specialized data analysis. For the EDSS Review System, BC, BCP, and OGC technical specialists (and contractors performing similar duties) have access to the data for the particular Bureau or Office in which they are working. Data in the EDSS Review System is saved in case-specific databases, and FTC case teams (e.g., attorneys, investigators, and paralegals) are granted access to data for the specific cases to which they are assigned.</p> <p>For the DOJ’s ORCA application, all contractors who work with the application have DOJ security clearance, and those contractors who handle FTC data in the application have FTC security clearance through a reciprocal clearance process. Data in DOJ’s ORCA application is similarly saved in case-specific databases. FTC case teams and authorized contractors (typically expert witnesses) are granted access to data in DOJ’s ORCA application for the cases to which they are assigned.</p>
Non-FTC Users	<p>The FTC may share information in the different environments within EDSS with courts, opposing counsel, defendants, law enforcement or other individuals as otherwise authorized by law.¹¹ Except as discussed below, these entities and individuals do not have access to the LSS, the EDSS Review System, or DOJ’s ORCA application. Law enforcement agencies may obtain access to the LSS on a temporary, case-by-case basis. This access must take place in an FTC office. In addition, law enforcement entities may be provided with access to DOJ’s ORCA application for cases that the FTC and the law enforcement agency are co-prosecuting. When the FTC shares information with external entities, it typically does so pursuant to non-disclosure agreements, contract provisions regarding privacy and data security protections, court approved protective orders, or similar data protection controls.</p>

¹¹ See, e.g., 16 CFR § 4.11 (c), (d) and (j) for information regarding FTC rules for sharing information with law enforcement partners.

3.2 Do contractors and/or third party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

Yes, FTC contractors may have access to EDSS data. The level of access granted is commensurate with the contractor's duties. Contractors supporting the FTC's technical specialists will have access to the data for the particular organization or Bureau with which they are working. Contractors who are assigned to work on a specific case will be granted access only to data relating to the matter. All FTC contractors are required to complete computer security and privacy awareness training on an annual basis. Interactive online training provides guidelines for properly handling 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. Authorized contractors accessing EDSS directly receive training on its use.

Not Applicable.

3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third party service provider.

Authorized contractors who have access to EDSS are subject to the same rules of use and incident response policies as FTC employees. As stated above, contractors accessing EDSS are trained on its use and must adhere to strict guidelines.

Not Applicable.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

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.¹² 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

¹² 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>.

one.¹³ 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 governed by applicable discovery rules and court orders.

- Notice is provided via (*check all that apply*):
- Privacy Act Statement (Written Oral)
 - FTC Website Privacy Policy
 - Privacy Notice (e.g., on Social Media platforms)
 - Login banner
 - Other (*explain*): _____
- Notice is not provided (*explain*): _____

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

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.

Individuals do not typically have a right to consent to particular uses of their information. 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.

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

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. Individuals may make a request under the Freedom of Information Act (FOIA) and Privacy Act for access to information maintained about themselves in the EDSS or other FTC record systems. 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 for information from the

¹³ 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>.

EDSS. Privacy Act requests must be made in writing and submitted to the FTC's OGC. Requests can be made through the [FTC's website](#). 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). 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.

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

As stated above, individuals seeking EDSS records about themselves do not have direct access to EDSS. They may make a request under the FOIA and Privacy Act for access to information maintained about themselves in the EDSS or other FTC record systems. 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). If individuals have questions or concerns about the accuracy of any information in the EDSS system, they would raise those questions or concerns in the context of the FTC investigation or litigation in which they are involved.

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

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 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.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

The FTC's Office of the Chief Information Officer (OCIO), BCP's Division of Litigation Technology & Analysis (DLTA), and BC's Technology and Information Management Office (TIM) work together to manage and maintain the EDSS. An electronic key or keycard system restricts physical access to the EDSS facilities, including the BC and BCP intake rooms and the FTC Data Center. FTC policies for handling and safeguarding PII apply to the EDSS. In addition, OCIO's Operations Assurance branch performs monthly audits of the EDSS.

Only authorized staff are granted access to the LSS. Staff must create a password (separate from the FTC production network password), and staff members are locked out of the system after five failed attempts. The LSS resets after 15 minutes to allow users to attempt to log on again. The 15 minute reset is set up because the LSS does not have 24/7 help desk support and many users use the LSS after hours and on weekends. LSS administrators in OCIO and BCP have authority to reset passwords. Staff are given the least amount of access to data in the LSS as they need to perform their duties. For example, BCP's forensic accountants only have access to data within each matters' forensic accountant subfolder, and a case team may be granted permission to access one subfolder within the matter they are assigned.

For the EDSS Review System, BC, BCP, and OGC technical specialists (and contractors performing similar duties) have access to the data for the particular Bureau or Office in which they are working. FTC case teams and other authorized staff are given permission to access data relating to the cases to which they are assigned. These staff obtain access to the case specific folders in the EDSS Review System through a website that is accessible from the FTC's production network or through SAFE. That website authenticates users by IP address and using the same authentication methods employed on the FTC's production network.

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

With regard to the DOJ's ORCA system, data is secured in cipher or electronically locked rooms. These rooms are located in secure, guarded, and/or alarmed server rooms. All contractors who work in the DOJ's ORCA system have DOJ security clearance; those contractors who work with FTC data also have FTC clearance through a reciprocal clearance process. FTC staff, contractors, and law enforcement partners must be given access to the data in the ORCA system and are granted access only to data relating to the specific matter to which they are assigned. Users must utilize two-factor authentication to access all information in the ORCA system. Additionally, network security controls have been enforced and tailored based on best practices and Federal guidance to ensure a secure operating environment. Furthermore, ORCA backs up data regularly.

5.3 Has the system/project undergone the appropriate security risk assessment and received authority to operate?

Yes, each component of the EDSS (i.e., the LSS, the EDSS Review System, and DOJ's ORCA application) has undergone the appropriate security risk assessment and has received authority to operate. The LSS was given authorization to operate on August 24, 2014 for a period of three years. The EDSS Review System is

covered by the existing authorization for the Data Center GSS. 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 Review System. The ORCA application is subject to authorization by DOJ, which maintains ownership of the system; the FTC relies on the DOJ's authorization and a MOU with DOJ and CACI for its continued use of the application.

5.4 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

Not Applicable

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

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).

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.¹⁴ 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.

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

The information contained in the DOJ's ORCA application is deleted upon the termination of the litigation or investigation and close-out of the matter. Information contained on disaster recovery backup tapes are deleted within 90 days after request.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

Not Applicable.

¹⁴ See NIST Special Publication 800-88, Guidelines for Media Sanitization.

Authorized staff obtain access to the case specific folders in the EDSS Review System through a website that is accessible from the FTC's production network or through SAFE. That website authenticates users by IP address and using the same authentication methods employed on the FTC's production network. Authorized FTC staff and contractors access the DOJ's OMEGA application through a website that requires two factor authentication.

8 Privacy Risks and Evaluation

8.1 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 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.

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. All EDSS data is first copied to the LSS, a secure environment that is not connected to the Internet, where it is processed by BC, BCP, and OGC technical specialists (as well as FTC contractors performing similar duties) before it is loaded into the EDSS Review System. Some data is maintained in the LSS for staff who conduct complex data analysis in a secure environment. FTC staff, contractors, and law enforcement partners are given only the level of access to data in the LSS that their work requires. FTC staff and contractors who handle data in the LSS portion of the EDSS receive specialized training in its use. Once information is copied and processed in the LSS portion of the EDSS, or received by the FTC in processed form from its law enforcement partners or contractors, it is then loaded into case-specific folders in the EDSS Review System, which is located on the FTC production network. Authorized staff members must be given permission to access the case-specific data, according to their work assignments. 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.¹⁵ Authorized 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.

In some instances, data is loaded into a case-specific folder in DOJ's ORCA application. Authorized FTC staff and contractors and law enforcement partners must be granted access to the case folder in order to search and review the data. These users cannot search or access other case folders in the ORCA application.

¹⁵ See [Data Center GSS PIA](#).

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; 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 hardcopy 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 polices for handling and safeguarding 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 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.

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 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.

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

Only authorized FTC staff and contractors are granted access to the LSS within EDSS. These users must create a password (separate from the FTC production network password). Users are locked out of the system after five failed attempts. The system resets after 15 minutes to allow users to attempt to log on again. The 15 minute reset is set up because the LSS does not have 24/7 help desk support, and many users use the LSS after hours and on weekends. LSS administrators in OCIO and BCP have authority to reset passwords. Users are given the least amount of access to data in the LSS as they need to perform their duties. For example, forensic accountants only have access to data within each matters'

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

“forensic accountant” subfolder, and a case team may be granted permission to access one subfolder within the matter they are assigned. Law Enforcement partners may obtain access to the LSS on a temporary, case-by-case basis. This access takes place in an FTC office.

Authorized FTC staff and contractors must be granted access to data in case-specific folders in the EDSS Review System, based on the nature of their assignments. These users obtain access to the EDSS Review System through a website that is accessible from the FTC’s production network or through SAFE. That website authenticates users by IP address and using the same authentication methods employed on the FTC’s production network.

With regard to the DOJ’s ORCA system, authorized FTC staff and contractors, as well as law enforcement partners must be granted access to data in case-specific folders. These users access the ORCA application through a website that requires two factor authentication. ORCA administrators have authority to reset passwords or replace RSA tokens.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).

The FTC SORN applicable to the EDSS is I-1, Nonpublic Investigational and Other Nonpublic Legal Records.¹⁷ 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).

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

Although EDSS does not operate any website that would require the posting of a privacy policy, the collection, use, and disclosure of the information in EDSS has been reviewed to ensure consistence with the FTC’s privacy policy posted on its website (www.ftc.gov/privacy).

¹⁷ See <https://www.ftc.gov/sites/default/files/attachments/privacy-act-systems/i-1.pdf>.

9 Approval and Signature Page

Prepared By:

_____ Date: _____
Laura DeMartino
Associate Director, Division of Litigation, Technology & Analysis

Reviewed By:

_____ Date: _____
Katherine Race Brin
Chief Privacy Officer (CPO)

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

_____ Date: _____
Jeffrey M. Smith
Chief Information Security Officer (CISO)

_____ Date: _____
Jeffrey D. Nakrin
Director, Records and Filing Office

Approved By:

_____ Date: _____
Raghav Vajjhala
Chief Information Officer (CIO)