Federal Trade Commission
Privacy Impact Assessment

Secure Investigations Lab

(SIL)

April 2025

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The mission of the Federal Trade Commission (FTC or agency) is to enforce the Federal Trade Commission Act by preventing the use of unfair methods of competition and unfair or deceptive acts or practices; to enforce many other consumer protection and antitrust statues; and to enhance informed consumer choice and public understanding of the competitive process. In support of these activities, the FTC often receives data sets to conduct investigations and perform long-term studies. Some of these data sets may be designated for special handling because of the nature or the volume of the data, the analysis required, or other considerations. For example, a data set may contain significant volumes of personally identifiable information (PII) or it may require analysis of sensitive PII (SPII)[1] or Sensitive Health Information (SHI).[2]

The Office of the Chief Information Officer (OCIO) created the Secure Investigations Lab (SIL) to allow FTC staff to work with certain data sets while supporting the agency's investigations, litigation, and studies. The SIL is a secure computing environment—isolated from the FTC's production, development, and test lab networks—that is configured with statistical and analytic software and sufficient processing power to allow the efficient analysis of the extremely large and/or sensitive data sets that are collected to support the agency's mission and regulatory activities.

The SIL allows authorized FTC users to securely import, store, work with, and export data sets that are received by FTC staff in connection with investigations, litigation, and other authorized projects and that are designated for special handling. The SIL is maintained by authorized administrators. It cannot be accessed directly from the Internet, and it cannot be accessed by third parties; only authorized FTC users can access SIL.

The SIL is used to store and analyze data sets that have been designated for special handling because of the nature or volume of the data, the analysis required, or other consideration. The FTC obtains this information in connection with its law enforcement and other activities, and the SIL contains data in a variety of electronic formats, including Word files, spreadsheets, databases, emails, images, videos, and/or audio files.

---

[1] For purposes of this PIA, sensitive PII refers to the following information, whether in paper, in electronic form, or communicated orally:

(1) An individual's Social Security Number (SSN);
(2) Sensitive Health Information;
(3) a Biometric Identifier; or
(4) an individual's name or address or phone number in combination with one or more of the following: date of birth; driver's license number or other state identification number, or foreign country equivalent; military identification number; passport number; financial account number; or credit or debit card number.

[2] For purposes of this PIA, SHI includes medical records and other individually identifiable health information, whether on paper, in electronic form, or communicated orally. Sensitive Health Information relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

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

Several statutes authorize the FTC to collect and store the information that is maintained in SIL data sets, including the Federal Trade Commission Act, 15 U.S.C. §§ 41-58; the Privacy Act of 1974, 5 U.S.C. § 552a; 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.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[3] may be collected or maintained in the system/project. Check all that apply.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.

☒ Full Name	☒ Biometric Identifiers (e.g., fingerprint, voiceprint)	☒ User ID
☒ Date of Birth	☒ Audio Recordings	☒ Internet Cookie Containing PII
☒ Home Address	☒ Photographic Identifiers (e.g., image, x-ray, video)	☒ Employment Status, History, or Information
☒ Phone Number(s)	☒ Certificates (e.g., birth, death, marriage, etc.)	☒ Employee Identification Number (EIN)
☒ Place of Birth	☒ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☒ Salary
☒ Age	☒ Vehicle Identifiers (e.g., license plates)	☒ Military Status/Records/ ID Number
☒ Race/ethnicity	☒ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	☒ IP/MAC Address
☒ Alias	☒ Geolocation Information	☒ Investigation Report or Database
☒ Sex	☒ Passport Number	☒ Driver's License/State ID Number (or foreign country equivalent)
☒ Email Address		☐ Other *(Please Specify)*:_____
☒ Work Address		
☒ Taxpayer ID		
☒ Credit Card Number		
☒ Facsimile Number		
☒ Medical Information		
☒ Education Records		
☒ Social Security Number		
☒ Mother's Maiden Name		

Note: Personal information obtained by the FTC and stored in the SIL may, for any particular matter, include any of the data elements selected in the table above. Given the varied data sets that are stored in the SIL, the list above may not be exhaustive. This personal information is located in financial transaction data, loan files, credit reports, consumer complaints, affidavits, hospital and patient records (including health diagnosis and treatment

[3] 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.

details), and other similar records produced during litigation, investigations, and other matters.

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.

As noted above, any and all kinds of information may reside within the SIL. Personal information collected as part of the FTC's litigation matters and investigations are maintained as part of the FTC's law enforcement activities. Other non-PII data is stored in the SIL to supplement statistical analyses of SPII/SHI data such as data from the U.S. Census, the Center for Medicare and Medicaid Services (CMS), and the Bureau of Labor Statistics among other data sources.

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

The data sets stored in the SIL are collected, used, and maintained in connection with the FTC's law enforcement and other activities. Law enforcement activities include investigations of potential or alleged violations of anticompetitive practices as well as investigations and enforcement actions related to alleged violations of statutes protecting consumers against fraudulent, deceptive, or unfair practices in the marketplace. Other activities include studies, rulemakings, and economic analyses.

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

Source of Data	***Type of Data Provided & How It Is Collected***
Companies and/or Third Parties	Typically, the FTC obtains information from targets of its law enforcement activities via compulsory process or discovery, by purchasing the information from data vendors, or through other investigative sources. Information obtained via compulsory process includes data provided to the FTC pursuant to any of the mechanisms available to the agency for compelling an individual or entity to provide information, including Civil Investigatory Demand (CID), access orders, and subpoenas. Information obtained via discovery includes information provided to the FTC pursuant to any of the mechanisms available to parties litigating matters in the Federal Courts of the United States, including court orders, requests for admissions, sworn statements (e.g., declarations, affidavits, depositions, and interrogatories), and electronic and documentary evidence.

Source of Data	*Type of Data Provided & How It Is Collected*
	Information may be provided by companies filing under the Hart-Scott-Rodino (HSR) Act as part of a proposed merger. Other information may be filed voluntarily by private sector entities, including financial institutions, hospitals, and insurance companies, as well as local, state, federal, and foreign government agencies. Information required for FTC studies, such as economic analyses, may, in limited cases, be obtained from third parties. They can be obtained in a variety of ways, including via solicitations to relevant external parties or pursuant to Section 6(b) of the Federal Trade Commission Act.
Members of the Public/Consumers	Information may be collected directly from individuals or entities filing complaints with the FTC. Authorized FTC staff upload the data to the SIL.

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.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
FTC staff and contractors	FTC staff use the SIL when a secure network environment is necessary to work with data sets that have been designated for special handling because of the nature or volume of the data, the analysis required, or other considerations. For example, the Bureau of Economics (BE) conducts economic studies, supports antitrust and consumer protection investigations and litigation, analyzes existing and proposed consumer protection rules, and studies the competitive impact of regulations for the Commission. Certain BE data sets may contain, for example, significant volumes of sensitive PII or Sensitive Health Information (SHI); as a result, those data sets would be stored in the SIL, and BE would conduct its analyses in the SIL. Only authorized FTC users and authorized administrators have access to the SIL. In addition, access to matter-specific folders is granted on a need-to-know and least privilege access basis, and matter-specific folders are deleted at the end of the investigation or study unless they are needed for further research.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
External Entities/Third Parties	Although information in the SIL may be derived from external sources, and in some cases, may be used or incorporated into other confidential materials (e.g., *in camera* filings in litigation or discovery subject to protective orders), external entities do not have direct access to SIL. However, the FTC may transfer data from inside SIL to authorized third parties, such as expert witnesses, if needed to complete their job functions. Data that the FTC stores on the SIL may be shared with external entities only as permitted by statute, FTC rules of practice, and data use agreements, where applicable, or as required by court rules or court order.

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.

Authorized FTC contractors who have access to SIL are required to sign nondisclosure agreements, complete the Privacy and Security Awareness Training prior to obtaining access to any FTC systems, and annually thereafter to maintain access to those systems.

External entities and/or third-party service providers do not have direct access to SIL. However, the FTC may transfer data from inside SIL to authorized third parties, such as expert witnesses, if needed to complete their job functions. Data that the FTC stores on the SIL may be shared with external entities only as permitted by statute, FTC rules of practice, and data use agreements, where applicable, or as required by court rules or court order.

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.

FTC contractors with access rights to the SIL are subject to the same rules and policies as FTC staff, including adherence to the FTC Breach Notification Response Plan. The SIL is also subject to the FTC Incident Response Policy, which includes measures to prevent, detect, contain, eradicate, and recover from breaches that would include PII.

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.

☒ 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*): Individuals who provide the FTC with information pursuant to discovery or a related court order are provided with notice of what information is being collected, and may in some cases be provided by the FTC as to how information may or will be used or disclosed (e.g., *in camera* or protective orders). Generally, the use and disclosure of this information is controlled by applicable discovery rules and court orders. Similarly, if such information is provided voluntarily, the FTC may provide notice about collection, use, and disclosure at the time the information is collected or through other means (e.g., negotiated agreements).

☐ 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)?

Yes, in some instances (e.g., by asserting privilege in response to discovery or court orders or withholding the materials when the information has been requested by voluntary production). In such instances, the FTC has the right to pursue additional relief to compel provision of the information. In other instances, an individual does not have the opportunity and/or right to decline to provide information that is stored in the SIL. For example, if an individual provides sensitive PII to an entity that the FTC subsequently subpoenas, the FTC may receive that sensitive PII and store it in the SIL without the individual's knowledge or consent.

When information is provided voluntarily, the use of such information may also be governed by mutual agreement. If the individual has a right to consent to a particular use, this right will normally be exercised when determining whether to provide information to the FTC. Some uses of information are not subject to the consent of the individual providing the information (e.g., information provided pursuant to a court order or subpoena). In addition, uses of information may also be governed by specific laws (e.g., routine uses authorized under the Privacy Act of 1974.

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

Individuals may request access to their information, if any, that the FTC retrieves by a personal identifier and that the FTC is required to disclose in accordance with the Freedom of

Information Act (FOIA) and the Privacy Act of 1974. Requests can be submitted via the online FOIA/Privacy Act portal.

Because individuals seeking access to their own records cannot directly access the SIL, the primary risk is providing personal information to an unauthorized recipient upon request. In responding to such requests, the FOIA/Privacy Act Office has identity verification processes and procedures in place to reduce this risk.

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.

Individuals seeking records about themselves do not have direct access to the system. They may make a request under the FOIA and Privacy Act for access to information maintained about themselves in any FTC system. However, due to the law enforcement nature of the system, records in the system about certain individuals, such as 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 any information in the system, they may 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?

The data sets that are collected and stored in the SIL are not systematically checked for accuracy and timeliness. However, information that is used by the FTC as part of its law enforcement and other activities will be reviewed for accuracy and timeliness as appropriate to the particular FTC activity. For example, staff performing a merger or fraud investigation may confirm that the information in the SIL data set for that particular matter is timely and accurate, and FTC staff analyzing information from a SIL data set for use in an economic study may cross check their results in the aggregate against publicly available information.

The SIL, like other FTC network environments, is subject to appropriate security controls and OCIO policies and procedures. SIL procedures, controls, and Rules of Behavior help protect SIL data sets against undue risk of loss and ensure that the contents of evidentiary materials remain unchanged from the point in time they are included in the SIL.

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 following auditing measures and technical safeguards are applied to prevent the misuse of SIL data. These controls include:

- Authenticator/Password Management – Application and monitoring of initial distribution, composition, history, compromise, and change of default authenticators.
- Account Management – Application and monitoring of account establishment, activation, modification, disabling, removal (including unnecessary/defunct accounts) and review.
- Access Enforcement – Application and monitoring of access privileges.
- Least Privilege – Application for a user to perform his/her function.
- Separation of functions – SIL users cannot import or export SIL data but can only work with SIL data inside the SIL environment in matter-specific folders.
- Unsuccessful Login Attempts –Application automatically locks the account when the maximum number of unsuccessful attempts is exceeded.

Privacy risks associated with unauthorized disclosure of information are mitigated through implementation of technical and administrative controls that limit access to SIL data to those who must work with it. This need-to-know and least privilege access ensures that SIL users have no more privileges to data than required to carry out their official duties with regard to specific matters. In addition, deterrent controls in the form of warning banners, rules of behavior, and auditing are in place. Procedures are in place for designated individuals to properly dispose of or properly store SIL data at the end of each study or investigation.

5.3 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?

SIL information is retained and destroyed in accordance with applicable FTC policies and procedures, and with the National Archives and Records Administration's (NARA) General Records Schedule (GRS) 5.2 (Disposition Authority DAA-GRS-2022-0009-0002). The NARA GRS and FTC Rules of Practice 4.12 indicate that SIL data (working files) can be destroyed/deleted when no longer needed or returned to the submitter. In some cases, the time period of data retention and destruction may be governed by an applicable data use agreement.

SIL data is backed up on storage disks within the SIL environment. The backup data is maintained for two weeks before deletion. Additionally, the SIL's volumes are backed up to the cloud once per day. In addition, local snapshots with changes are taken daily.

Disposal of SIL information is conducted in accordance with FTC policies and procedures and in compliance with Office of Management and Budget (OMB), NARA, and NIST guidelines.[4]

Internal procedures are in place for the destruction of original digital media used to load data into the SIL. For the destruction of external drives, the FTC has retained a vendor whose methods meet or exceed applicable standards for media sanitation and destruction.

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. The SIL is a secure computing environment that is isolated from the FTC's production, development, and test lab networks. It is not connected to the internet and does not employ website technologies such as cookies or web beacons.

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?

Risk	***Mitigation Strategy***
Original digital media used to load data sets into SIL may be lost after initial receipt from external parties	The FTC has put into place a chain of custody for media and has established policies, procedures, and Rules of Behavior, all of which ensure that SIL data is properly copied, transported, and stored. Additionally, all original digital media, when not in use, is locked in a safe that is located in a secure, locked room.
Unauthorized access, modification, and/or personal information in SIL data sets by FTC personnel	SIL networking components and computing resources are physically accessible only to authorized administrators. Authorized FTC users can only connect to the SIL from their internal FTC workstations via a Secure Sockets Layer Virtual Private Network ("SSL VPN") using two-factor authentication. The SSL VPN technology is deployed on the FTC internal network and provides the only logical access to the segregated SIL network. Authorized SIL users cannot access the SIL directly from the Internet, and third parties do not have direct access to SIL. In addition, SIL users are granted access to data sets in matter-specific SIL folders on a need-to-know and least privilege access basis. SIL users

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

Risk	*Mitigation Strategy*
	cannot access SIL data sets for matters that they are not working on, and a Bureau of Economics representative requests that the SIL administrator remove the user's permissions from folders once the user no longer needs access to the folder. Matter-specific SIL folders are deleted when the data are no longer required for the investigation or for studies. Additionally, the FTC Personnel Security Office performs various types or levels of background investigations on every FTC employee. The SIL is accessible only by authorized administrators and authorized FTC users, all of whom have received a Minimum Background Investigation (MBI) and Criminal History and Credit Checks.
Digital copies of SIL data sets may be removed or lost	The FTC has put in place a chain of custody for digital copies of SIL data sets. All requests for digital copies of SIL data sets must be initiated by designated individuals, and movement of SIL data sets must be properly documented. Finally, all digital copies of SIL data sets are encrypted using FIPS 140-3 standards
Printed documents or reports containing information from SIL data sets may be lost	The FTC has deployed multiple media protection controls, including limiting physical access to the SIL printer, enforcing print logging (SIL users must save the cover sheet of every document printed in the SIL), providing secure hard copy disposal methods (shredder and burn bags), Rules of Behavior, and signs in the SIL printer room reminding SIL users of their responsibilities.
Software used in SIL may contain malware that could run in the SIL environment	Security scans are run on the software before it is used in the SIL.
Data sharing with third parties may result in third parties storing FTC data in an insecure fashion	Periodically the FTC is required to remove data from the SIL and transfer it to authorized third parties, such as expert witnesses, who must access this data outside of the FTC's network to complete their job functions. To address the risk of third parties storing FTC data in an ensure fashion, the FTC includes non-disclosure agreements and provisions in contracts (where appropriate) that mandate secure handling of the data the FTC stores in the SIL. Additionally, transfers to authorized third parties are made only by secure (e.g., encrypted) means.

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

The SIL uses established technologies and controls for securing data and addressing privacy risks, while avoiding technologies that could raise additional privacy concerns. For example, the SIL does not directly connect to the Internet or host a website that might result in additional threats or vulnerabilities to the security and privacy of SIL data.

The FTC has a verification process for reviewing requests by FTC users to access SIL and for granting authorized SIL users the right to access matter-specific SIL folders, based on need and least privilege access.

All FTC personnel, including those who use the SIL, are subject to FTC procedures for safeguarding PII, including Sensitive PII and SHI. All FTC personnel are required to complete Annual Privacy and Security Awareness Training. Additionally, SIL users receive SIL-specific training on receiving, handling, and securing SIL data, as well as other guidance in relation to safeguarding information.

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).

Data may be retrieved from the SIL using a variety of factors, including personal identifiers. Actual retrieval methods depend upon the content of the SIL data set, the nature of the matter, and the purpose for which the data set is used.

To the extent SIL data about an individual are retrieved from a system or records by name or other identifier assigned to the individual, the SIL is covered by SORN I-1, Nonpublic Investigational and Other Nonpublic Legal Program Records.[5]

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?

The collection, use, and disclosure of the information in SIL has been reviewed to ensure consistency with the FTC's Privacy Policy.

[5] All FTC SORNs are available online.