Federal Trade Commission
Privacy Impact Assessment

for the:

Secure Investigations Lab

May 2009

1 System Overview

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. In many instances, these data sets contain personally identifiable information (PII).

The Information and Technology Management Office (ITMO) created the Secure Investigations Lab (SIL) to allow staff to work with certain data sets obtained to support the agency's investigations, litigation, and studies. The SIL is a discrete computing environment, separate from the FTC production, development, and test lab networks, configured with statistical and analytic software and sufficient processing power to allow the efficient manipulation of extremely large data sets that are routinely used to support the agency's mission and regulatory activities. The SIL will have two separate and segregated areas for data, one for data that contains PII and one for data that does not.

There is no access to the SIL from the Internet or via the FTC's remote access capability. No information is independently collected from the public by the SIL or SIL program manager. Rather, the SIL stores data and allows FTC staff to securely work with records received by FTC staff as part of investigations, litigation, or other authorized projects.

The agency's law enforcement and other mission-related activities are carried out primarily by the FTC's Bureau of Competition (BC), Bureau of Consumer Protection (BCP), and Bureau of Economics (BE). The FTC will deploy the SIL in three phases, one for each of these Bureaus The first phase will deploy computing resources in the SIL to support BE and deployment for BC and BCP to follow at a later date.

The Program Manager for the SIL is Michael Rivera, Assistant Chief Information Officer, Infrastructure Operations Branch.

2 Information Collected and Stored within the System

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

The SIL stores PII that the FTC obtains as part of its law enforcement and other activities. This will include PII in various electronic formats, including:

- word processing files
- spreadsheets
- databases

- emails
- images
- videos
- audio files

PII obtained by the FTC may include names, addresses, telephone numbers, e-mail addresses, birth dates, social security numbers / tax identification numbers, bank account numbers, and credit card numbers. PII may be found in such records as financial transaction data, loan files, credit reports, consumer complaints, affidavits, hospital and patient records, and other similar records produced during litigation, investigations, and other FTC matters.

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

The SIL will store PII from various sources. 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 enforcement and other activities. Sources may include consumers; local, state, federal, and foreign government agencies; and private sector entities, including financial institutions. Information may be provided to the FTC voluntarily (e.g. from companies that wish to merge, or from consumers who file complaints with the FTC), via compulsory process (e.g., subpoenas or civil investigatory demands), or through discovery in matters in litigation. Information for other activities, such as economic analyses, may, in limited cases, be obtained from data brokers.

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

PII stored in the SIL is 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 How is the information collected?

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

Voluntary submissions may include information provided to the FTC by consumers, private sector entities, law enforcement partners, and others. 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 include CIDs, access orders, and subpoenas.

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

Information required for FTC studies may 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.

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

Information that is collected and stored in the SIL will not generally be 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 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 and the information obtained for use in an economic study may be checked in the aggregate against publically available information.

While information may not be systematically checked for accuracy and timeliness, it will be subject to appropriate security and chain-of-custody controls. These controls will ensure that sensitive information is protected from any undue risk of loss, and that the contents of evidentiary materials remain unchanged from the point-in-time they are included in the SIL.

2.6 Is the system using technologies in ways that the FTC has not previously employed (e.g., monitoring software, Smart Cards, etc.)? If so, how does the use of this technology affect individuals' privacy?

The SIL uses technologies that have been deployed previously within the FTC production and test lab environments. The SIL employs firewalls, routers, switches, various operating systems and Commercial-Off-The-Shelf (COTS) software. All SIL users connect via a Secure Sockets Layer (SSL) Virtual Private Network (VPN) and are required to use two-factor authentication.

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

Several statutes authorize the FTC to collect and store the information that is maintained in the SIL, 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.

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

Below are identified risks associated with the PII that will be used and stored in the SIL during an investigation or study, as well as a discussion of the steps that have been or will be taken to mitigate those risks.

There is a risk that the original digital media may be lost after initial receipt from external parties. To address this risk, the FTC has put in place a chain of custody for media to ensure the data is properly copied, transported, and stored. Additionally, all original digital media, while not in use, shall be locked in a safe which is located in a locked room.

There is a risk of unauthorized access, modification, and/or misuse of SIL data by FTC personnel. To address this risk, SIL networking components and computing resources are physically accessible only by authorized system administrators. Authorized end users of the SIL can only connect to the SIL from their internal FTC desktops which connect via an 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. The SIL can only be reached by initiating a connection from the internal FTC production network; there is no web-based or remote access from outside the FTC production network.

Additionally, the FTC Personnel Security Officer performs various types or levels of background investigations on every FTC employee. The SIL is accessible by only select attorneys, economists, paralegals, investigators, and technology workers who have received a Minimum Background Investigation (MBI), and Criminal History and Credit Checks. Additionally, file and folder access rights are granted using the need-to-know and least privilege information security concepts. User rights are revoked at the end of the investigation or study**.**

There is a risk that digital copies made of SIL data sets may be lost. To address this risk, the FTC has put in place a chain of custody for digital copies of data requested from the SIL. All requests for digital copies of SIL data sets must be pre-approved and can only be made by pre-determined individuals. All digital copies of data from the SIL are encrypted using FIPS 140-2 standards.

There is a risk that printed documents or reports containing data which resides in the SIL may be lost. To address this risk, the FTC has deployed multiple media protection controls to include limiting physical access to the SIL printer, enforcing print logging (SIL users must log every document printed in the SIL), providing hard copy disposal

methods (shredder and burn bags), and signage posted in the SIL printer room reminding users of their responsibilities.

There is a risk that a tape backup may be lost during transport to or from our offsite storage facility. To address this risk, the FTC contracts with an information protection and storage vendor who transports encrypted tapes in customized, secure vehicles.

3 Use and Access to Data in the System

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

FTC staff will use the SIL when a secure network environment is necessary to work with particularly large data sets on projects that are sensitive in nature and/or involve working with PII. For example, 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. Any study or investigation conducted by BE that necessitates the need for data containing PII or proprietary information will be conducted in the SIL.

3.2 Which internal entities will have access to the information?

As discussed in section 2.8, only authorized attorneys, economists, paralegals, investigators, and technology workers will have access to SIL information. Additionally, file and folder access rights are granted using the need-to-know and least privilege information security concepts. User rights are revoked at the end of the investigation or study**.**

3.3 Which external entities will have access to the information?

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 will not be given access to such data through the SIL.

4 Notice and Access for Individuals

4.1 How will individuals be informed about what information is collected, and how this information is used and disclosed?

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 notice 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)

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

In some cases, yes (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).

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

In some cases, the uses of the information are not subject to the consent of the individual providing the information (e.g., information provided pursuant to a court order or subpoena). Sometimes, the uses of information are also governed by specific laws (e.g., routine uses authorized under the Privacy Act of 1974). 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 the use, this right will normally be exercised by him or her when determining whether to provide information to the FTC.

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

Individuals to whom SIL data pertain do not have user access rights to the SIL, which is limited to FTC personnel. Individuals seeking access to information that may be stored about them in SIL may seek access only to information, if any, that the FTC is required to disclose to them under the Freedom of Information Act (FOIA) and the Privacy Act of 1974. See Section 8.

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

Not applicable. See section 4.4.

5 Web Site Privacy Issues

The SIL does not operate a website. Therefore, no web site privacy issues were identified.

6 Security of Information in the System

6.1 Are all IT security requirements and procedures required by federal law being followed to ensure that information is appropriately secured?

The FTC follows all applicable Federal Information Security Management Act (FISMA) requirements to ensure the information residing in the SIL is appropriately secured. The SIL will be reported to OMB as a Major Application (MA) and will receive a Certification and Accreditation using NIST and OMB guidance.

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

The SIL resides within the FTC Infrastructure General Support System (GSS), which has received a Certificiation and Accreditation (C&A). An independent C&A is expected to be completed for the SIL MA in FY 2010.[1]

6.3 Has a risk assessment been conducted on the system?

A risk assessment has been completed in conjunction with Phase One of the deployment of the SIL.

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

The SIL uses proven, secure technologies for internal use only.

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

The FTC has a controlled user access request process that verifies the qualification for specific access to SIL data**.** Each user access request must be approved by the Bureau's Deputy Director or above, the FTC Chief Privacy Officer (CPO), and the FTC Chief Information Security Officer (CISO).

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

All FTC personnel, including those who use the SIL, are subject to FTC procedures for safeguarding sensitive PII. All FTC personnel receive annual computer-based privacy and security training, as well as other guidance explaining how to safeguard information.

---

[1]The Data Center GSS PIA is available here: http://www.ftc.gov/os/2011/08/1108datacenter.pdf

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

The following in-place auditing measures and technical safeguards are applied to prevent misuse of 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.
- Unsuccessful Login Attempts – System automatically locks the account when the maximum number of unsuccessful attempts is exceeded.
- Audit logs are reviewed weekly for identifying system misuse.
- Users are not allowed, via technical security controls, to download data from the SIL to the FTC production network.

Privacy risks associated with unauthorized disclosure of information are mitigated through implementation of technical controls associated with need-to-know and least privilege, ensuring that users have no more privileges to data than required to affect their official duties. In addition, deterrent controls in the form of warning banners, rules of behavior, confidentiality agreements and auditing are in place. Procedures are in place to disable user accounts at the end of each study or investigation.

6.8 Who is the point of contact for questions regarding the security of the system?

Any questions regarding the safeguarding of the SIL should be addressed to the FTC CISO.

7 Data Retention

7.1 For what period of time will data collected by this system be maintained?

There are no pre-determined periods of time that the data collected for an investigation or study shall be maintained within the SIL. Data will be stored in the SIL until the matter is fully resolved. All SIL data subject to disposal shall be archived or destroyed according to National Archives and Records Administration (NARA) policy.

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

All SIL data subject to disposal will be destroyed in accordance with Office of Management and Budget (OMB), National Archives and Records Administration (NARA), and National Institute of Standards and Technology (NIST) policies and procedures.

7.3 Describe any privacy risks identified in the data retention and disposal of the information, and describe how these risks have been mitigated.

Risks associated with data retention and disposal do not raise any special privacy concerns not already addressed**.**

8 Privacy Act

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

Data may be retrieved from the SIL using a variety of factors, including personal identifiers. This will vary from project to project.

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

The SIL is covered by SORN I-1, Nonpublic Investigational and Other Nonpublic Legal Program Records - FTC. http://www.ftc.gov/foia/listofpaysystems.shtm

9 Privacy Policy

9.1 Confirm that the collection, use, and disclosure of the information in this system has been reviewed to ensure consistency with the FTC's privacy policy.

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

10 Approval and Signature Page

Prepared for the Business Owners of the System by:

_____ Date: _____
Margaret Mech
Chief Information Security Officer

Review:

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

_____ Date: _____
Kellie Cosgrove Riley
Acting Chief Privacy Officer

_____ Date: _____
Margaret Mech
Chief Information Security Officer

Approved:

_____ Date:_____
Stanley Lowe
Chief Information Officer