Privacy Impact Assessment
for the

Executive Office for U.S. Attorneys: Litigation Technology Service Center

Contact Point
Anthony J. Ciccone, Senior Counsel
Office of the Chief Information Officer, EOUSA
Department of Justice
(202) 616-6973

Reviewing Official
Vance Hitch
Chief Information Officer
Department of Justice
(202) 514-0507

Approving Official
Kirsten J. Moncada
Acting Chief Privacy and Civil Liberties Officer
Department of Justice
(202) 514-0208

Introduction

In FY 2007, the Executive Office for U.S. Attorneys (EOUSA) established an electronic discovery processing facility, known as the Litigation Technology Service Center (LTSC), to serve the needs of all 94 United States Attorneys Offices (USAOs) nationwide. LTSC services include digitizing paper documents into electronic format, as well as coding and loading electronic documents into databases for legal review, redaction, and production during the discovery process and related litigation, investigation, and administrative activities. This includes scanning, auto-coding, optical character recognition (OCR), Bates labeling, deduplication, and email threading. Deliverables are provided in a variety of formats including Concordance load files, CD/DVDs, and a secure intranet repository (iConect) within the Department of Justice (DOJ) firewall.

Section 1.0
The System and the Information Collected and Stored within the System.

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

The LTSC processes litigation, discovery, and investigatory materials regarding civil and criminal cases, as well as personnel and administrative records, for USAOs and EOUSA. No information is independently collected from the public by the LTSC. Rather, the LTSC merely processes records received from authorized project requesters so as to facilitate electronic search, retrieval, and utilization. Processed data is either returned via secure shipping methods, or hosted on a secure iConect intranet site for legal review, redaction, and production.

1.2 From whom is the information collected?

Information is provided to the LTSC by authorized USAO or EOUSA project requesters, and may include information collected from client agencies or other Departmental components in connection with official DOJ litigation, investigations, or administrative matters.

Section 2.0
The Purpose of the System and the Information Collected and Stored within the System.

The following questions are intended to delineate clearly the purpose for which information is collected in the system.

2.1 Why is the information being collected?

The LTSC accepts paper and/or electronic records from authorized USAO or EOUSA project requesters in order to facilitate electronic search, retrieval, and utilization (e.g., through scanning/OCR, Bates labeling, auto-coding, deduplication, and email threading).

2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

The information processed by the LTSC for authorized USAO and EOUSA project requesters is collected pursuant to the underlying legal authority of the involved USAO and EOUSA project requester, such as 5 U.S.C. § 301 (agency operations), 28 U.S.C. § 516 (conduct of litigation), and 28 U.S.C. § 547 (duties of United States Attorneys), as well as applicable System of Records Notices (SORNs) published under the Privacy Act of 1974 (5 U.S.C. §552a), including but not limited to JUSTICE/USA-001 ("Administrative Files"), JUSTICE/USA-005 ("Civil Case Files"), JUSTICE/USA-007 ("Criminal Case Files"), and JUSTICE/USA-015 ("Debt Collection Enforcement System") (see www.usdoj.gov/opcl/privacyact.html).

2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

The following potential privacy risks were identified in connection with LTSC data and have been mitigated as noted below.

(1) To guard against the possible loss or theft of data being sent to/from the LTSC, special United States Attorneys Procedures have been established to facilitate secure shipping through the use of dual-container configuration requirements, media encryption, tamper-evident DOJ labels and special carrier handling requirements.

(2) To guard against potential breaches of LTSC databases or access by unauthorized individuals, LTSC protocols require password protection of electronic data and/or encryption of removable media. For example, all users of LTSC computers, databases, and intranet (iConect)

facilities must establish that they currently have satisfactory security clearances or background investigations and are authenticated JCON-IIA users who have executed Departmental Rules of Behavior governing appropriate computer usage. In addition, special United States Attorneys Procedures have been established to ensure that all potential LTSC projects are pre-vetted to avoid potential conflicts-of-interest, to ensure compliance with Fed. Rule Crim. Procedure 6(e) in Grand Jury cases, and to handle Federal Tax Information (FTI) pursuant to applicable legal requirements.

(3) To guard against the potential loss or theft of computer equipment, the LTSC facility has extensive physical security and access controls, including locked inner/outer doors, 24-hour guard service, automated intrusion detection/prevention systems, and proximity to EOUSA's Security Fusion Center and Network Operations Center, which are co-located in the same building.

(4) To guard against the potential loss or theft of paper documents or portable media at the LTSC (e.g., CD/DVDs, external hard drives, flash drives, etc.), the LTSC has established chain-of-custody protocols and stores such materials in locked document control rooms with racks and filing cabinets accessible only to authorized personnel.

(5) To guard against unauthorized disclosure, all LTSC personnel sign a strict Confidentiality Agreement and are notified of potential Privacy Act and other penalties for unauthorized disclosure. Deterrent controls such as auditing, Warning Banners, and Rules of Behavior are also in place. Prior to being granted access to system data, LTSC personnel undergo background investigations and/or security clearances, coupled with access restrictions. Finally, exit procedures for departing personnel include the prompt disabling of accounts and access rights to all data.

(6) In addition, there are United States Attorney Procedures governing the prompt reporting of incidents involving any breach of the confidentiality, integrity, or availability of electronically stored information, so that responsible officials may contain and eradicate threats, assess damage, preserve any artifacts, and take other appropriate mitigation steps.

Section 3.0
Uses of the System and the Information.

The following questions are intended to clearly delineate the intended uses of the information in the system.

3.1 Describe all uses of the information.

The LTSC processes litigation, investigatory, discovery, and administrative records for authorized USAO or EOUSA project requesters so as to facilitate electronic search, retrieval, and utilization. Also see ¶1.1.

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

The LTSC processes data in a variety of ways depending on the requirements of each particular project. For example, some USAO or EOUSA project requesters may only need to have paper documents scanned, OCR'd, and electronically Bates-stamped for administrative convenience. Others project requesters may require more extensive data processing (such as auto-coding, deduplicating, and email threading) in order to permit more extensive legal review and document analysis in connection with litigation, discovery, or criminal investigations. The LTSC itself does not engage in data mining.

3.3 How will the information collected from individuals or derived from the system, including the system itself be checked for accuracy?

As noted above, the LTSC does not independently collect information from the public, but rather merely processes records for authorized USAO and EOUSA project requesters. As such, the only accuracy checks performed by the LTSC consist of quality control protocols to ensure, for example, that scanned images accurately correspond to the paper originals.

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

The data in LTSC systems is maintained for as long needed by the authorized USAO or EOUSA project requester. LTSC data is only an electronic copy of the original USAO/EOUSA records. The originals are not retained by the LTSC and are subject to whatever retention periods govern them, e.g., NARA General Records Schedules, agency SF-115s, and any applicable System of Records Notices (SORNs) published under the Privacy Act of 1974, 5 U.S.C. §552a (see www.usdoj.gov/opcl/privacyact.html). Procedures will be developed to ensure that

these electronic copies are not in practice retained beyond the retention period established for the original records.

3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

System data is maintained in accordance with DOJ Order 2640.2F, "Information Technology Security" and related authority, including OMB guidance on safeguarding personally identifiable information. FISMA-mandated continuous monitoring requirements (NIST SP 800-53/CA-7) provide assurances that privacy-applicable controls are consistent with Certification and Accreditation standards. Also, please refer to the controls described in ¶ 2.3 above.

Section 4.0
Internal Sharing and Disclosure of Information within the System.

The following questions are intended to define the scope of sharing both within the Department of Justice and with other recipients.

4.1 With which internal components of the Department is the information shared?

Access to LTSC project data is typically restricted to the particular USAO or EOUSA project requesters who authorized the project. However, if there is a justified need for intra-DOJ collaboration in a particular case, LTSC project data may be shared with other Departmental components as discussed below.

4.2 For each recipient component or office, what information is shared and for what purpose?

The information that may be shared within the particular USAO or EOUSA and with other Departmental components depends on the instructions provided to the LTSC by the authorized USAO or EOUSA project requesters. The project requester identifies the individuals within the USAO or EOUSA, and in some instances, in other Departmental components, who may have access to the information. For example, a USAO requester may instruct the LTSC to grant FBI agents access to certain data (via iConect) during the pre-indictment phases of a criminal investigation.

4.3 How is the information transmitted or disclosed?

LTSC project data may be shared with other Department components in one of two ways: (1) encrypted media may be provided to authorized users in another DOJ component via secure shipping; or (2) a firewall modification may be requested to allow authorized users in another DOJ component to access the LTSC's secure intranet (iConect). Access to iConect would be through EOUSA computer facilities and would only be given to users vetted and approved by EOUSA.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Same potential risks and mitigation steps as outlined in ¶2.3.

Section 5.0
External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DOJ which includes foreign, Federal, state and local government, and the private sector.

5.1 With which external (non-DOJ) recipient(s) is the information shared?

Access to LTSC project data is typically restricted to the particular USAO or EOUSA project requesters who authorized the project. However, if there is a justified need for collaboration with a client agency in a particular case (e.g., coordination with an agency's Office

of Inspector General), LTSC project data may be shared with authorized personnel in that agency as discussed below.

5.2 What information is shared and for what purpose?

The information that may be shared with users in client agencies depends on the instructions provided to the LTSC by the authorized USAO or EOUSA project requesters.

5.3 How is the information transmitted or disclosed?

LTSC project data may be shared with authorized personnel in external client agencies via encrypted media. Alternatively, client agency personnel may request a USAO to grant them access to USAO premises and authorization for on-site use of USAO computer facilities from which to access the LTSC's secure intranet (iConect) after appropriate clearance (e.g., by presenting satisfactory security credentials and executing USAO Rules of Behavior). In all cases, access is limited to individuals identified by the project requester.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

No.

5.5 What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

They must sign USAO Rules of Behavior before accessing USAO computer facilities, and they are provided iConect training if they have been authorized to access LTSC project data via iConect.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

System data is maintained in accordance with DOJ Order 2640.2F, "Information Technology Security" and related authority, including OMB guidance on safeguarding personally identifiable information. Also, FISMA-mandated continuous monitoring requirements (NIST SP 800-53/CA-7) provide assurances that privacy-applicable controls are consistent with Certification and Accreditation standards.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

Same potential risks and mitigation steps as outlined in ¶2.3.

Section 6.0
Notice

The following questions are directed at notice to the individual of the scope of information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information.

6.1 Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

The LTSC neither collects data from, nor has direct contact with, the subjects of the data, but only communicates with the USAO or EOUSA project requester (or authorized designees). Nevertheless, where applicable, notice is provided in connection with the original records through existing System of Records Notices published in the Federal Register.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Information is not collected from individuals by the LTSC.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

Information is not collected from individuals by the LTSC.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

Information is not collected from individuals by the LTSC.

Section 7.0
Individual Access and Redress

The following questions concern an individual's ability to ensure the accuracy of the information collected about him/her.

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

The LTSC does not collect information from, nor deal directly with, the record-subjects of data provided to the LTSC for processing by the authorized USAO or EOUSA requester. Requests for access to, or amendment or redress of, records processed by the LTSC would be handled by the originating office.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

Same as ¶7.1.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

No.

7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

To the extent such opportunities and procedures exist, they would be provided by the originating office.

Section 8.0
Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 Which user group(s) will have access to the system?

Access is limited to cleared and authorized users of LTSC data. This includes USAO or EOUSA project requesters; DOJ components or client agencies designated by the project requester; and LTSC personnel authorized to work on a given project (e.g., certain personnel may be denied access to certain data if so warranted by Grand Jury secrecy requirements, tax privacy laws, or to mitigate potential conflict-of-interest issues).

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

Yes, the LTSC is a GO/CO (i.e., Government Owned/Contractor Operated) facility operated by IEDiscovery, Inc. pursuant to Contract No. GS-25F-0004P, Order No. 7F-EOA02-0165, issued by the Executive Office for United States Attorneys, DOJ, on September 28, 2007. Contractor access to LTSC system data is subject to the Privacy Act, 5 U.S.C. § 552a(m) (www.law.cornell.edu/uscode/html/uscode05/usc_sec_05_00000552---a000-.html); accord Federal Acquisition Regulation (FAR), 48 C.F.R. §§ 52.224-1, 52.224-2 (www.arnet.gov/far/current/html/52_223_226.html#wp1168976).

8.3 Does the system use "roles" to assign privileges to users of the system?

A system user hierarchy has been defined and implemented for LTSC users. The hierarchy defines roles, based upon job function, to assign privileges to users of the system.

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

Levels of access are determined by each user's job function (e.g., USAO or EOUSA project requester; other authorized DOJ component user; designated client agency contact, etc.). Documented Entry On Duty/Exit Standard Operating Procedures are followed to ensure that each user has only the access necessary to perform his/her job.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Access to LTSC systems (including the iConect intranet document repository) is handled in accordance with applicable DOJ account management policies and procedures. Each user account is specific to a particular user.

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

(a) The primary auditing measures and technical safeguards for preventing the misuse of system data involve access/authentication controls derived from FISMA requirements, which are configured in compliance with DOJ Order 2640.2F. These controls include:

- Authenticator/Password management, i.e., application and monitoring of initial distribution, composition, history, compromise, and change of default authenticators (NIST SP 800-53/IA-5).
- Account Management, i.e., application and monitoring of account establishment, activation, modification, disabling, removal (including unnecessary/defunct accounts) and review, all of which support implementation of "need-to-know" (NIST SP 800-53/AC-2).
- Access Enforcement, i.e., application and monitoring of access privileges (NIST SP 800-53/AC-3).
- Least Privilege; i.e., provision of the minimum tools required for a user to perform his/her function (NIST SP 800-53/AC-6).
- Unsuccessful Login Attempts: i.e., General Support System (GSS) automatically locks the account until released by a System Administrator when the maximum number of unsuccessful attempt is exceeded (NIST SP 800-53/AC-7).
- System Use Notification, i.e., a user has to acknowledge Department policies regarding use before access is granted (NIST SP 800-53/AC-8).
- Session Lock, i.e., a user has to re-authenticate after a specified period of inactivity (NIST SP 800-53/AC-11).

- Remote access is controlled and monitored. Encryption is used to protect the confidentiality of remote access sessions through the use of secure remote access tokens (NIST SP 800-53/AC-11).
- Audit trails are generated to facilitate intrusion detection and identify data misuse. The system is configured to protect audit information and tools from unauthorized access, modification and deletion (NIST SP 800-53/AU Family).

(b) The potential risk for unauthorized disclosure of personal information from the system is mitigated by:

- limiting the number of authorized system users;
- performing background investigations on candidate users;
- providing initial and annual system security training;
- vetting Freedom of Information Act (FOIA) requests;
- limiting physical access to the system;
- utilizing least-privilege restrictions based on user role;
- robust malicious software management;
- timely installation of security patches;
- monitoring network activity with a continuously monitored Intrusion Prevention System;
- encrypting data during remote transmission;
- encrypting personal data during storage; and
- utilizing separation-of-duties to limit data access.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

All DOJ employees are required to complete online information systems security training as part of annual training for DOJ employees. A certificate of completion is logged for employees after successful completion of the training. Also, new employees receive training on the use of the system before they are granted access to the system. Users are reminded

periodically about DOJ policies in these areas and their requirements to comply with these policies.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

The information is secured in accordance with the DOJ schedule-driven implementation of FISMA requirements as recorded in the JMD Cyber Security Assessment and Management application ("CSAM" or, formerly, "Trusted Agent"). Information security complies with the management, operational, and technical controls delineated by NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems. The applied system category control set is **moderate** as defined by NIST Special Publication 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories.

The system will be certified and accredited for control compliance as well as adherence to industry security best practices and mitigation of risk due to technical vulnerabilities.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Same potential risks and mitigation steps as outlined in ¶2.3.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

With all acquisitions of new or upgraded hardware, software or other products, a cost-benefit analysis has been performed in accordance with DOJ requirements. IT investments are pursued in accordance with the relevant provisions of the DOJ Systems Development Life Cycle Guidance and Federal Acquisition Regulations.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

In conformance with DOJ ITSS Standard 2.6, EOUSA implements data integrity controls to protect data from accidental or malicious alteration or destruction and to ensure that the data is accurate and has not been altered. EOUSA employs an intrusion detection/prevention system to detect vulnerabilities, changes to the network, and traffic anomalies. EOUSA backs up data regularly and controls access to data stored on the GSS.

9.3 What design choices were made to enhance privacy?

EOUSA's security strategy includes protecting EOUSA assets from outside attackers as well as from internal security violations. To protect personally identifiable and proprietary information, EOUSA utilizes an incident response plan and a GSS computer security policy. EOUSA also requires users to sign General User Rules of Behavior, which address accountability by requiring users to protect any and all sensitive information stored or processed by EOUSA computer systems. EOUSA also employs auditing controls, an intrusion detection/prevention system, secure router configurations, inactivity logouts and firewalls. To enhance the security of data, EOUSA encrypts removable hard drives, flash media, and laptop hard drives with Pointsec security software. Pointsec complies with Evaluation Assurance Level 4 in Common Criteria quality certification (CC EAL4) and FIPS 140-2.

Conclusion

The concluding section should inform the reader, in summary fashion, how you constructed your system, program, rule, or technology based on privacy risks and mitigation strategies.

The LTSC is used to process, store, and transmit data that supports USAO and EOUSA litigation, discovery, investigatory, and administrative needs. Securing this information and assuring its proper use is critical to the success of the United States Attorneys' mission.

The LTSC system architecture comports with EOUSA's security mandate for a hardened infrastructure and secure office automation services. Management review, periodic enhancement, and FISMA-mandated continuous monitoring of the system's technical configuration and procedural controls are of the utmost importance in maintaining network infrastructure security and continuity of operations.

Responsible Officials

LTSC Project Manager/COTR:

1/16/09

Anthony J. Ciccone — Date
Senior Counsel, Office of the Chief Information Officer
Executive Office for United States Attorneys

EOUSA Information Security Systems Officer:

1/16/09

Ted Shelkey — Date
Assistant Director, Information Systems Security Staff
Executive Office for United States Attorneys

EOUSA Privacy Officer:

1/16/09

William G. Stewart, II — Date
Assistant Director, Freedom of Information & Privacy Staff
Executive Office for United States Attorneys

Approval Signature Page

1/22/09

Kirsten J. Moncada — Date
Acting Chief Privacy and Civil Liberties Officer
Department of Justice