Federal Trade Commission
Privacy Impact Assessment

for the:
Electronic Document Management System
(Documentum)

Published: May 2011

1.0 System Overview

The Federal Trade Commission (FTC, Commission or the agency) is an independent federal government law enforcement and regulatory agency with authority to promote consumer protection and competition through prevention of unfair, deceptive and anticompetitive business practices; to enhance informed consumer choice and public understanding of the competitive process; and to accomplish these missions without unduly burdening legitimate business activity.

The FTC relies on an electronic document management system (EDMS) to support the agency's business. This system allows staff to track, search and access various types of agency documents, such as staff memoranda to the Commission; Commission approved reports; filings and orders in FTC adjudicative proceedings; and filings in federal court cases. Maintaining these documents in an EDMS also facilitates responses to Freedom of Information Act (FOIA) and other disclosure requests by providing search and access capability for responsive documents.

The FTC's electronic document management efforts date to the mid-1990s. At that time, the Commission began addressing the FTC's electronic document management needs by customizing and installing a Commercial-off-the-Shelf (COTS) system and placing it on the agency network. Called LANDOC (Local Area Network Documents) it was designed to serve as an electronic library of Commission documents and their related "metadata." Metadata are document index items designed to facilitate sorting and retrieval. They include such information as the document's submitter, title, number of the matter to which it pertains, type of document, format, the groups of users who have access to it, comments about it, and other internal document tracking information. LANDOC also provided document management functions, including the ability to restrict access to documents and their metadata to specified offices, and document version control.

Because LANDOC had limitations that did not meet increased agency needs, the Commission replaced LANDOC with Documentum in 2010, an EDMS that meets the

Department of Defense Directive 5015.2 standards, which the National Archives and Records Administration (NARA) has adopted for federal agencies to maintain federal records in electronic format. Documentum contains all of the documents that were in LANDOC (more than 300,000 documents in a variety of different text and image formats) and documents added to Documentum since LANDOC was decommissioned. One new feature in Documentum is a Brief Bank where staff in FTC's Bureaus, the Office of the General Counsel (OGC), the Regional Offices and certain other Offices can find briefs and other documents filed by FTC in federal court cases.

Documentum is "the system" referenced in this Privacy Impact Assessment (PIA). While many of the documents in the system are public, the system itself is non-public, with access limited to FTC staff and approved contractors.

2.0 Information Collected and Stored Within the System

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

The system stores numerous Commission documents that contain various items of PII, including names, addresses, telephone and fax numbers, e-mail addresses, financial information such as bank account information, credit information and Social Security numbers.

These documents include law enforcement related documents and other types of documents. Examples of law enforcement related documents in the system include compulsory process documents (e.g., subpoenas and civil investigatory demands); investigative hearing transcripts; transcripts of depositions in adjudicative proceedings[1], transcripts of adjudicative hearings and trials; briefs and other documents filed in adjudicative proceedings; orders entered in adjudicative proceedings; briefs and other

[1] Such proceedings may sometimes also be referred to as "administrative" proceedings to differentiate them from judicial (court) proceedings.

documents filed in federal court cases; federal court orders to pay consumer redress and financial statements from individuals ordered to pay redress; Federal Register Notices of proposed consents; petitions related to cease and desist orders and FTC responses; and attachments to filings made through the HSR (Hart-Scott-Rodino) Electronic Filing System.[2]

Examples of other documents in the system include staff memoranda to the Commission and other staff memoranda; Congressional correspondence; Federal Register notices of rulemakings; requests for formal and informal advisory opinions and FTC responses; news releases; and speeches given by FTC officials;

2.1(a) FTC Brief Bank

The FTC Brief Bank is located in Documentum's work product repository. The Brief Bank contains public versions of FTC briefs and other filings in federal court cases. These documents are contained in three folders—one for filings made by OGC, one for filings made by the Bureau of Consumer Protection (BCP) and by FTC's Regional Offices in consumer protection cases and one for filings by the Bureau of Competition (BC) and by FTC's Regional Offices in competition cases. Content is not being placed in the BC folder at this time, but BC is planning to do so.

Access to the Brief Bank is limited to staff in OGC, BC, BCP, the Bureau of Economics, the Office of International Affairs and the Office of Public Policy. Staff in these organizations have read-only access to all documents in the Brief Bank. Users will not be able to edit the documents in the Brief Bank (they are final versions) but can copy and paste to documents they create outside of Documentum. A limited number of users in OGC and BCP have additional rights to add content (documents and metadata) to and delete it from their organization's folder. A limited number of users in BC (and possibly a limited number of users in the Regional Offices) will also have these rights for the BC

[2] See Privacy Impact Assessment for www.hsr.gov and HSR Electronic Filing System, June 28, 2006, https://www.hsr.gov/privacyimpact.htm.

folder. See Section 3.2.1 for a discussion of access by the system administrator and a contractor in the Office of the Chief Information Officer (OCIO) and access during initial deployment by a limited number of staff and contractors in the Records and Filings Office (RFO).

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

Information in the system is obtained by FTC staff in connection with the agency's law enforcement and other activities. In some instances, this information is provided voluntarily, such as when individuals submit comments in rulemaking proceedings or send correspondence to Congress which is then forwarded to the FTC, and when investigatory targets agree to provide information to the Commission in lieu of compulsory process. FTC staff also obtain information in response to compulsory process, such as subpoenas and civil investigatory demands, or via discovery in administrative and federal court litigation. Information in the system may also be obtained from other sources, such as public resources on the Internet, nonpublic investigatory databases, other law enforcement agencies, and commercial databases such as Lexis/Nexis. In some instances, individuals – for example, third parties in investigations and witnesses in administrative and federal court matters--provide information about other individuals.

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

Information in the system is collected, used, disseminated and maintained in order for the Commission to perform its law enforcement functions and other activities. For example, FTC staff collects and uses the information to investigate anticompetitive practices and to enforce statutes protecting consumers from fraudulent, deceptive, and unfair practices in the marketplace. In addition, the information is used in a variety of other ways, such as to assist with consumer redress and respond to Congressional correspondence. As described in the System Overview, agency documents which contain the information are

maintained in the system so that staff can track, search, and access them as necessary, as well as to facilitate responses to FOIA and other disclosure requests by providing search and access capability for responsive documents.

2.4 How is the information collected?

See Section 2.2.

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

This system is a document management system that maintains agency documents already collected or generated in the course of agency business. Accordingly, these documents are placed into the system "as is" without verifying their accuracy or timeliness. The accuracy and timeliness of the information in such documents is verified, however, as necessary and appropriate at the time they are collected, generated or used by the agency (e.g., in law enforcement investigations or litigation).

2.6 Is the system using technologies in ways that the FTC has not previously employed (e.g., monitoring software, Smart Cards, etc.)?

Documentum uses an Oracle database and an application layer. Documentum uses an internal web interface for user interaction. The system does not use technologies in ways that the FTC has not previously employed with one exception. Documentum's work product repository implements the use of an audit feature within the repository that has not previously been employed. As noted, the Brief Bank is located in this repository. Any user with access to a document in the Brief Bank can click on "history" under the "properties" tab and see who added the document to the Brief Bank and when. Any user can also see if one of the limited number of users with add rights has checked a document out and checked it back in—for example to substitute a PDF version of the document for an MSWord version. The system administrator (an employee in OCIO) and an OCIO contractor who supports the system administrator can also run reports of who deleted a

document from the Brief Bank and when. As noted, all documents in the Brief Bank are public filings and most users have read-only access.

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

The FTC Act, the Commission's Rules of Practice, and other laws and regulations that the Commission enforces permit the collection of the information. For more information, see http://www.ftc.gov/ogc/stats.

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

The privacy risks that have been identified are unauthorized disclosure and misuse of the information. These risks have been addressed and mitigated as described in this section. A manager's written authorization is required before an agency employee receives access to Documentum. Only agency staff whose work assignments require access receive it. For contractors, a contracting officer's technical representative (COTR) or Administrative Officer at the request of the COTR, must provide written authorization before the contractor can gain access to the network and must specifically authorize access to Documentum and issuance of an Oracle password (needed to access Documentum) before the Documentum manager (an employee in OCIO who is also the system administrator) grants access to Documentum. Only contractors whose work assignments require access receive it.

In addition, agency staff and contractors are subject to security background checks, and access to the system is controlled by user ID and passphrase combination, a separate log in for Documentum with user ID and an Oracle password, and electronic or network controls (e.g. firewalls). Staff and contractors receive annual training on, and are required to adhere to, written FTC policies protecting sensitive PII and non-public information including that contained in the system.

Most documents in the system are also coded by type in order to limit access to particular classes of system users (e.g., Commissioners and their office staff; or Commission staff in a specific organization). Access to documents in the Brief Bank is controlled by the user groups assigned to the Brief Bank's folders. The system administrator and an OCIO contractor who supports the system administrator maintain the user groups. In addition, the FTC is addressing the risks of unauthorized disclosure and misuse of the information by developing a plan for disposing of the documents and metadata in the system when no longer needed. See Section 7.

3.0 Use and Access to Data in the system

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

3.1.1 Identify and list each use.

As discussed previously, the system provides staff and contractors with the ability to access copies of documents needed for law enforcement and other activities of the Commission. In addition, the system provides staff and contractors processing FOIA and other disclosure requests with the ability to access copies of potentially responsive documents.

3.1.2 If the system uses commercial or publicly available data please explain why and how it is used.

Some of the data in the system used for law enforcement and other Commission activities is commercial or publicly available. For example, commercial databases as well as publicly available sources (e.g. telephone and address directories) may be used to provide information on investigatory targets. The FTC is not engaged in data mining and the data is not used for this purpose.[3]

[3] See the Federal Agency Data Mining Reporting Act of 2007, Pub. L. No. 110-53, 121 Stat. 206, § 804(b)(1) for a definition/description of the term "data mining."

3.1.3 Confirm that all uses of the data are both relevant and necessary to the purpose for which it was collected.

All uses of the data are relevant and necessary to the purpose for which it was collected. The system does not collect any new information that is not already collected by the agency for its law enforcement programs and other activities.

3.1.4 Confirm that all users of the system have a level of access determined by their need-to-know, with the lowest level of access needed to perform their work.

All users of the system have a level of access determined by their need-to-know, with the lowest level of access needed to perform their work. See Section 2.8.

3.1.5 Describe privacy risks identified regarding the use of the information collected, and describe how these risks have been mitigated. For example, is it possible that the data could be used for multiple purposes?

See Section 2.8.

3.2 Which internal entities will have access to the information?

Agency staff and contractors who require information in support of FTC law enforcement and other activities, and in order to respond to FOIA and other disclosure requests, will have access to the information, subject to the access restrictions noted in Section 2.8.

3.2.1 Within the FTC, specify the categories of users who will have access to the system (include contractors).

All FTC staff and contractors with access to the system can do so at a read-only permission level. As noted previously, access to documents and their metadata is further restricted based on a need to know. See Section 2.8. The system administrator (an employee in OCIO) and an OCIO contractor who supports the system administrator, have full access rights to all documents and metadata in the system in order to assist with maintenance of and enhancements to the system and, in some instances, content management. In order to manage system content, a limited number of staff and contractors in RFO and the Office of the Secretary (OS) can add or delete documents and metadata in the system, with the exception of redress orders and the accompanying financial statements, attachments to premerger filings, speeches of agency officials, and OCIO task sections of the system. OS staff and contractors have no access to the Brief Bank. A limited number of RFO staff and contractors have the right to add content (documents and metadata) to and delete it from the Brief Bank during its initial deployment. A limited number of users in OGC and BCP have rights to add content (documents and metadata) to and delete it from their organization's folder in the Brief Bank. A limited number of users in BC (and possibly a limited number of users in Regional Offices) will also have these rights for the BC folder. In addition, OCIO contractors who are project managers, as well as OCIO staff can initiate project management workflows in Documentum and attach technical documents to these workflows. The initiators and a limited number of OCIO staff can create multiple versions of these documents and modify the documents' metadata as needed to manage the project.

3.2.2 If contractors will have access to the system, please describe the necessity of this access. Specify whether the contractors are involved with the design, development, or maintenance of the system. Specify whether confidentiality, Privacy Act, or other privacy-related contract clauses were inserted into their contracts.

To manage content, a limited number of contractors in RFO and OS can add or delete metadata and documents in the system (see Section 3.2.1). In addition, OCIO contractors who are project managers can initiate project management workflows in Documentum and attach technical documents to these workflows. These contractors can create multiple versions of these documents and modify the documents' metadata as needed to manage the project. An OCIO contractor who supports the system administrator has full access rights to all documents and metadata in the system. See Section 3.2.1. All FTC contractors sign Non-Disclosure Agreements.

3.3 Which external entities will have access to the information?

External entities do not have electronic access to the system. The FTC itself may share information in the system with other law enforcement agencies that have agreed, in writing, to treat the information confidentially. Individuals who file a FOIA request may be provided with information that FTC staff obtains from the system, unless the information is subject to a FOIA exemption. Likewise, individuals who file a Privacy Act request may be provided with information about themselves that is in the system subject to certain exemptions. See Section 4.4.

4.0 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?

Wherever possible, the FTC provides notice to individuals about its policies regarding the use and disclosure of information at the time the information is collected. For information that is collected pursuant to a request from the FTC, notice is provided as part of that request (e.g., in a letter request or in the document outlining the compulsory process request). For those occasions where the FTC cannot provide notice at the time the information is collected (e.g., when the information is collected by another law enforcement agency or another organization), the FTC provides notice via its privacy

policy, its Privacy Act system of records notices (SORNs), and its PIAs, including this one.[4] See also section 8.2.

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

The opportunity or right depends on how the information is collected. For example, those who provide information pursuant to compulsory process do not generally have a right to decline to provide the information. However, individuals who file public comments or requests for advisory opinions, or who send inquiries to members of Congress (which become part of the Congressional correspondence in the system) provide information about themselves voluntarily and could choose to decline to provide such information.

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

Individuals do not have the right to consent to particular uses of the information stored in the system.

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

An individual may make a request under the Privacy Act for access to information maintained about themselves in this system or other systems at the FTC. 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. Access to the information under the Privacy Act is subject to certain exemptions. In addition, there are many public documents in the

[4] See the FTC's Privacy Policy at http://www.ftc.gov/ftc/privacy.shtm, SORNs at http://www.ftc.gov/foia/listof paysystems.htm, and PIAs at http://www.ftc.gov/ftc/privacyimpactassessments.shtm.

system that also appear on the FTC's web site and are accessible to the public there or in paper format through the public reading room at Headquarters.

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

No privacy risks have been identified, because individuals do not have access to the system.

5.0 Web Site Privacy Issues

Not applicable. The system is not made available for access or disclosure through any public web site

6.0 Security of Information

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 contained in the system is appropriately secured.

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

The system is part of the FTC's Infrastructure General Support System (GSS), which has received a Certification and Accreditation (C&A) using NIST (National Institute of Standards and Measures) and Office of Management and Budget (OMB) guidance.[5]

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

6.3 Has a risk assessment been conducted on the system?

A risk assessment was completed on the Infrastructure GSS as part of the C&A. Appropriate security controls have been identified to protect against risk and such controls have been implemented.

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

As discussed earlier, the system does not use any technologies that the Commission has not previously employed with one exception. Documentum's work product repository implements the use of an audit feature within the repository that has not previously been employed. As noted, the Brief Bank is located in this repository. Any user with access to a document in the Brief Bank can click on "history" under the "properties" tab and see who added the document to the Brief Bank and when. Any user can also see if one of the limited number of users with add rights has checked a document out and checked it back in—for example to substitute a PDF version of the document for an MSWord version. The system administrator (an employee in OCIO) and an OCIO contractor who supports the system administrator can also run a report of who deleted a document from the Brief Bank and when. As noted, all documents in the Brief Bank are public filings and most users have read-only access. The technology employed in Documentum, including the audit feature, does not raise any special privacy concerns.

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

6.5.1 Describe generally the process by which an individual receives access to the system.

A manager's written authorization is required before an agency employee receives access to Documentum. Only agency staff whose work assignments require access receive it.

For contractors, a contracting officer's technical representative (COTR) or Administrative Officer at the request of the COTR, must provide written authorization before the contractor can gain access to the network and must specifically authorize access to Documentum and issuance of an Oracle password (needed to access Documentum) before the Documentum manager (an employee in OCIO who is also the system administrator) grants access to Documentum. Only contractors whose work assignments require access receive it.

6.5.2 Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Currently the permissions granted allow "read only" access for the majority of users, though a comparatively small number of users have rights to add and delete documents and metadata. The system administrator, an employee in OCIO, and an OCIO contractor who supports the system administrator have full access rights to all documents and metadata in the system in order to assist with maintenance of and enhancements to the system and, in some instances, content management. See Sections 3.2.1 and 3.2.2.

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

All FTC staff and all contractors with network access are required to complete computer security training and privacy awareness training annually.

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

The following auditing, testing, and technical safeguards are in place to prevent misuse of data:

- Access Enforcement – There is active monitoring and testing of access privileges.
- Least Privilege – Only the appropriate folder and file rights are assigned to a user to perform his/her function.
- Unsuccessful Login Attempts – The system automatically locks a user's account when the maximum number of unsuccessful attempts is exceeded.

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 complete their official duties.

Any questions regarding the security of the system should be directed to the FTC's Chief Information Security Officer.

7.0 Data Retention

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

Currently, most documents in the system are copies of paper records that are retained and destroyed in accordance with retention schedules approved by NARA. The FTC has submitted to NARA a new retention schedule authorizing the record copy of documents, structured databases, other types of electronic files, and metadata to be kept in electronic format in a document management system (such as Documentum) compliant with NARA standards. Once NARA has approved the new schedule, system records and data, including auxiliary information and data in the system, will be retained and destroyed in accordance with the new schedule. Pending NARA approval, the FTC will manage the data in a manner consistent with 44 U.S.C. Ch. 31, 44 U.S.C. 3506, 36 CFR Ch. XII, Subchapter B, Records Management, and Office of Management and Budget (OMB) Circular A-130, par. 8a1(j) and (k) and 8a4.

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

As discussed in Section 7.1, information in the system will be destroyed in accordance with the new retention schedule. All data will be deleted/destroyed in accordance with OMB, NARA and NIST regulations and guidelines.

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

Regarding privacy risks identified in data retention, see Section 2.8. Information in the system will be disposed of in a way that makes it impossible to recover.

8.0 Privacy Act

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

Yes. For example, the name of a party in an adjudicative proceeding or the name of an investigatory target may be used to retrieve relevant documents.

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

Yes, see FTC-VII-6, Document Management and Retrieval System—FTC. http://www.ftc.gov/foia/listofpaysystems.shtm.

9.0 Privacy Policy

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

Although the system does not disclose or make information available through any public web site, the collection, use, and disclosure of information in the system have been reviewed to ensure consistency with the FTC's privacy policy posted on the FTC's web site, www.ftc.gov.

10.0 Approval and Signature Page

Prepared for the Business Owners of the System by:

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

Review:

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

_____ Date: _____
Marc Groman
Chief Privacy Officer

_____ Date: _____
Margaret Mech
Chief Information Security Officer

Approved:

_____ Date: _____
Jeffrey Huskey
Chief Information Officer