Federal Trade Commission
Privacy Impact Assessment

for the:
SharePoint 2010 Pilot

April 2012

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.

This Privacy Impact Assessment (PIA) discusses the Federal Trade Commission's (FTC) deployment of Microsoft SharePoint 2010. At this time, the Office of the Chief Information Officer (OCIO) and the Office of General Counsel (OGC) are conducting SharePoint pilot studies, with the goal of eventually offering SharePoint as an enterprise service available to the entire agency.

Microsoft SharePoint 2010 is a commercial off-the-shelf web-based application that integrates with Microsoft Office 2010 to provide enhanced communication and collaboration features. For example, through SharePoint, FTC staff can more easily share documents, engage in simultaneous editing of documents, and create document libraries and knowledge bases. Through the use of the system, agency staff will be able to more effectively and efficiently perform the agency's law enforcement and other activities. The system runs on the FTC's secured internal servers. All data stored on SharePoint is saved and stored on the Data Center General Support System, which has undergone its own PIA. FTC SharePoint sites are not accessible to anyone outside of the FTC.

SharePoint sites can be set-up and customized for individual FTC organizations, for specific team members within those organizations, and even for particular business processes undertaken by those teams. This Privacy Impact Assessment will address the general privacy risks involved in deploying SharePoint, how such risks have been mitigated in the context of the pilot study, and how the same risk mitigation strategies will be applied during the agency-wide deployment of the SharePoint service. As the

agency expands its use of SharePoint, it will need to consider whether new uses of the system warrant a review and update of this assessment.

2.0 Information Collected and Stored Within the System

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

Since SharePoint is a collaboration tool that will be used by FTC staff to perform the agency's law enforcement and other activities, the information maintained in the system will depend on the particular business processes for which a SharePoint site is set up. SharePoint is able to store 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 of individual defendants or respondents, witnesses, consumers or other non-FTC individuals. As also described below, SharePoint system data may include login IDs, passwords, audit logs, personnel-related materials, or other PII pertaining to FTC employees, contractors, or other FTC individuals.

Documents maintained or processed in SharePoint may include law enforcement documents and other types of documents that may contain PII. Examples of law enforcement documents in the system could 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 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 consent agreements; petitions

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

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 potential SharePoint documents 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; speeches given by FTC officials; and documents related to Freedom of Information Act (FOIA) requests and appeals.

In addition, SharePoint also stores information on the identity of system users (those FTC staff with access as explained in Section 3.2). SharePoint maintains records showing who has logical access to particular sites, document libraries, etc. and the activities of those users on SharePoint.

In the case of the OGC pilot, SharePoint is being used, among other things, to process FOIA appeals. The following documents may be found within the SharePoint site customized for the FOIA Appeals team:

Communications with Appellant: Communications (e.g., letters, e-mails and facsimiles) to and from the appellant, including the original request letter and the appeal letter. Personally identifiable information (PII) captured here can include but is not limited to names, addresses, telephone numbers, e-mail addresses, fax numbers, and other contact information of the appellant or the person appealing on behalf of the appellant. Documents (such as an original FOIA request) may also contain social security numbers ("SSNs").

Responsive Materials: During the processing of the original request, the FOIA paralegal assigned to the request retrieves copies of materials responsive to the request from other FTC offices. These documents consist of legal, investigatory, administrative, or similar

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

nonpublic agency records, some of which may contain PII about investigatory targets or other individuals (e.g., witnesses, complainants, FTC staff, other consumers, or the requester) depending on the type and nature of the record. For example, such PII can include names, addresses, telephone numbers, or other information about an individual (e.g., a complaint by a consumer or description of an alleged violation by the subject of the investigation). During the appeal process, the FOIA paralegal who processed the original request uploads these materials in PDF format to the SharePoint site so that the attorney assigned to the appeal can review the materials to determine whether the documents were properly released or withheld pursuant to the statutory standards.

Appeal Memo and Determination Letter: Once the attorney assigned to the appeal has reviewed the original request and determination, the responsive materials, and the appeal letter, the attorney drafts a memorandum of law and fact for the General Counsel recommending the approval or denial of the appeal as well as a proposed determination letter addressed to the appellant. These documents are saved to SharePoint for review by the managing attorney and the Assistant General Counsel for FOIA. Personally identifiable information (PII) captured here can include but is not limited to names, addresses, telephone numbers, e-mail addresses, fax numbers, and other contact information of the appellant or the person appealing on behalf of the appellant. (Some FOIA processing data is already maintained and managed by the FTC in its FOIAExpress System, which has its own PIA.)

The Office Of The Chief Information Officer (OCIO) will store technical documents used in the support and maintenance of the FTC's information technology (IT) systems. This includes government personnel contact lists, design documents, Statements of Work, policies, procedures, financial management documents, project management documents, access control lists, and Standard Operating Procedures..

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, and in the case of FOIA requests and appeals. 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.

For the OCIO, information is obtained internally within the department and from contractors performing work on IT systems.

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

Information placed 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, respond to Congressional correspondence, and to process FOIA requests and appeals. As described in the System Overview, agency documents which contain the information are maintained in the system so that staff can collaborate on them as necessary to perform the agency's law enforcement and other activities.

With respect to the OGC FOIA Appeal team's use of SharePoint, for example, the information collected in the system is used to respond to appeals under the FOIA or the Privacy Act, to track these appeals in order to maintain compliance with statutory response times, and to review documents responsive to the original request, in order to assess whether the documents were properly released or withheld during the original determination.

The OCIO needs to document the technical details of its IT systems to properly maintain them.

2.4 How is the information collected?

See Section 2.2.

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

Information that is collected and stored in SharePoint 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 and the laws and authorities, if any, applicable at the time the agency compiles the records (e.g., FTC Act, personnel laws, administrative or court evidentiary rules and procedures) that are relevant to the business process for which the SharePoint site is set up. For example, with respect to FOIA and Privacy Act appeals, information about appellants has been collected from the appellants themselves (i.e., their original request letters, appeal letters, and related communications). OGC staff checks the accuracy and timeliness of this information (e.g., contact information, precise scope of the request or appeal) as necessary to allow FTC staff to respond to or contact an appellant with respect to the original request and any subsequent appeal. However, the OGC staff does not check the accuracy or timeliness of responsive documents that are uploaded to SharePoint for attorney review, including any PII that may be contained in such documents. The FTC is required under the FOIA to grant or

deny access to responsive records "as is," without alteration. The accuracy and timeliness of the information (including any PII) contained in such records, would be governed by other laws and authorities, if any, applicable at the time the agency compiles those records (e.g., FTC Act, personnel laws, administrative or court evidentiary rules and procedures).

Documents for OCIO are normally reviewed at least once by a government employee in charge of a particular technical area.

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

SharePoint, as configured for the FTC, is not employing technologies in ways that the FTC has not previously employed. SharePoint does have certain features that would present new privacy risks if enabled, but these features will not be enabled for the FTC configuration. For example, SharePoint can be configured such that SharePoint sites and any documents saved to the sites can be accessed from any web browser as well as certain mobile devices. This feature will not be available to FTC users. In order to access SharePoint sites, FTC users will need to be within the FTC network, connecting to the system from within an FTC building or through the FTC's secure web-based connection, SAFE. Likewise, SharePoint can be configured to allow users to broadcast PowerPoint presentations on the web, publish Excel documents on the web or to extranet sites, and publish Access databases on the web or to extranet sites. However, these features will not be available to FTC users. FTC users will be restricted to publishing information within the intranet SharePoint sites to which they have been given access. Furthermore, the FTC SharePoint configuration allows the sharing of links to documents (e.g., through email), but the links can only be accessed from within the FTC network. As configured, SharePoint does not allow documents to be shared directly (e.g., as an email attachment).

There is a risk that individual users could set up unauthorized SharePoint sites, and that this could lead to information being maintained on these sites without proper oversight and auditing. In order to minimize this risk, for purposes of the pilot, SharePoint has been configured so that only certain users (known as "superusers") have the right to create SharePoint sites. All other users will need to work with these superusers in order to create new SharePoint sites.

Lastly, SharePoint users who communicate through SharePoint discussion forums or wikis rather than email or other traditional methods will be instructed to include these SharePoint sites in their searches when responding to FOIA and Privacy Act requests.

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. In addition, for OCIO documents, the Federal Information Security Management Act (FISMA) applies.

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

General privacy risks, such as disclosure of PII or other nonpublic information, are being mitigated (as detailed in 2.6) by hosting SharePoint on the FTC's secured internal servers, limiting access to SharePoint sites to within the FTC network, and disabling SharePoint features that would allow for the publishing or sharing of information outside of the FTC intranet.

In addition, SharePoint training will include a module regarding privacy and security that trains staff on how to use SharePoint's access controls to restrict access, on a group or user-level, to SharePoint sites, document libraries, and specific documents. By default,

case-specific sites on SharePoint are governed by the least privilegeprinciple, by which only the owner of the case-specific site has access to the documents within it unless the owner extends permission to other users. This principle is applied, for instance, to segregate and limit access to files that may by their nature likely contain sensitive PII, such as personnel-related litigation or ethics files, assigned only to selected attorneys or other authorized staff for handling, viewing, and sharing.

Specific privacy risks will depend upon the types of information collected and the sources of collection for the particular business process for which a SharePoint site is set-up.

With respect to FOIA appeals, the main privacy risk associated with the collection and maintenance of PII in the system about FOIA and Privacy Act appellants is that individual appellants may, when filing their access request or appeal, include sensitive personal information about themselves, or about other individuals in their request or appeal letter. Similar risks are presented by the uploading of responsive documents into SharePoint. This information could then be compromised by unauthorized access or disclosure. To mitigate this risk, the FTC has taken steps to minimize the amount of information that the agency collects and maintains about such individuals. For example, the FOIA Office only asks for the minimum amount of contact information from individual requestors necessary to communicate with them and respond to their requests and appeals as required by law. At the weblink to our online request form, we alert requesters not to provide sensitive PII unless necessary to authenticate a specific request. To avoid unauthorized access or disclosure, this information is logged into the FOIAXPRESS database, but system access is limited (by software licenses) to a small number of specified FTC professionals who need system access to do their jobs. Similarly, during the appeal process, only the information necessary to make a determination on the appeal (as detailed in 2.1) is saved to the SharePoint site, and only those FTC staff who are working on the appeal (the FOIA paralegal who processed the original request, the attorney assigned to the appeal, the managing attorney(s), the

Assistant General Counsel for FOIA, and the General Counsel or Acting General Counsel) have access to the information.

Likewise, the SharePoint site dedicated to OGC's ethics activities is restricted to those staff that work on the ethics team. During the agency-wide deployment, depending on the particular activity for which a SharePoint site is being set-up, and the sensitivity of the information being handled through the site, controls can be configured in a similar way such that only those staff with a business need have access to the information. However, other SharePoint sites that have a lower risk due to the nature of the information contained within them may have fewer access restrictions in order to better facilitate collaboration between staff.

For the OCIO, any PII stored in SharePoint is non-sensitive, so no significant risks, if any, have been identified.

Finally, to guard against unauthorized or inadvertent disclosure, FTC staff also follow special internal agency procedures for working with, storing, sharing, sending, transporting, and destroying sensitive personal information.

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.

How information in SharePoint will or may be used depends on the particular business process for which a SharePoint site is set up. In general, the underlying uses of the information will remain the same, but SharePoint will provide enhanced collaboration and communication tools that will allow FTC staff to more efficiently carry out the processes for which the information was collected. These tools include, for example, the

ability to create work flows, to simultaneously edit documents, and to facilitate group communication through discussion forums and wikis.

With respect to FOIA appeals, the information will be used to review the original determination and to make a determination on the appeal, and for tracking the status of the appeal and approving the appeal determination.

For the OCIO, the information will be used to maintain the FTC's IT systems.

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 and used for law enforcement and other Commission activities may be commercial or otherwise 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 planning to use SharePoint to conduct any data mining programs within the meaning of applicable Federal law.[3]

The OCIO pilot does not use commercially or publicly available data on individuals. OCIO documents may reflect other types of commercial or publicly available matters, such as commercial software and systems.

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] 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."

3.1.4 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 SharePoint.

Which entities will have access to the information on any particular SharePoint site will depend on the particular business process for which the SharePoint site is set-up.

With respect to the FOIA Appeals SharePoint site, the managing attorney will grant permissions to only persons working on a particular appeal, and to only those documents to which access is needed. For example, the FOIA paralegal that processed the original request will be provided with access in order to upload and save the original request and determination letters and the responsive documents to the site. However, the FOIA paralegal will not have access to the appeal memorandum of law and fact and the appeal determination letter. Access to these appeal documents will be limited to the attorney assigned to the matter, the managing attorney, the Assistant General Counsel for FOIA,

and the General Counsel or Acting General Counsel. Moreover, staff in other sections of OGC, and of the FTC generally, do not have access permission to the SharePoint site for FOIA appeals. Administrator rights are limited to the managing attorney and his administrative assistant, who will create new folders within the site as necessary and provide appropriate access permissions to those staff working on a particular appeal. FTC Office of the Chief Information Office professionals have access as necessary to administer and support FOIA appeal processing.

Similar access controls will be set-up for each SharePoint site, depending on the business process for which it is created and the sensitivity of the information stored within it.

For OCIO, access is limited to authorized OCIO employees and contractors.

3.3 Which external entities will have access to the information?

External entities do not have electronic access to the system; contractors have access as necessary for the proper functioning of 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.

As noted above, for OCIO, some external entities (contractors) may be authorized to have access to OCIO documents in the system.

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 may become part of the Congressional correspondence in the system), or file FOIA requests or appeals 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?

[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.

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 somepublic documents in the system 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 such 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 Data Center 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]

6.3 Has a risk assessment been conducted on the system?

A risk assessment was completed on the Data Center 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.

No, not in its FTC configuration. See section 2.6 above.

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

Which users may access any particular SharePoint site will depend on the business process for which the site is set-up. With respect to the FOIA and Privacy Act SharePoint site, as noted in 3.2, the managing attorney and his administrative assistant grants permissions to those users working on a particular appeal to the extent that access is needed.

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

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

Before gaining access to the system, agency staff must complete a SharePoint training. The training module regarding privacy and security trains staff on how to use SharePoint's access controls to restrict access, on a group or user-level, to SharePoint sites, document libraries, and specific documents. Depending on the business process for which it is created and the sensitivity of the information stored within it, default access controls can be set-up for each SharePoint site created.

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. In addition, there is a module regarding privacy and security within the SharePoint training, as discussed in section 6.5.

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

Access to nonpublic system records is restricted to FTC personnel or contractors whose responsibilities require access. Access to all electronic records within the Agency, including those maintained on SharePoint, is controlled by "user ID" and password combination and other electronic access or network controls (e.g., firewalls). SharePoint also keeps information on the identity of system users, including the sites and folders that they have accessed. We also have the capacity to employ additional audit trail procedures about system users and to track activity as necessary. FTC buildings are guarded and monitored by security personnel, cameras, ID checks, and other physical security measures. These and other information and physical security measures currently in place are subject to periodic reviews and audits by the Commission's Inspector General.

7.0 Data Retention

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

Records are retained and disposed of in accordance with the applicable schedules approved or issued by the National Archives and Records Administration (NARA). The FTC has submitted to NARA a new, comprehensive retention schedule that includes systems. Once NARA has approved the new schedule, information and data 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 OMB Circular A-130, par. 8a1(j) and (k) and 8a4.

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

Records are to be electronically purged and destroyed when appropriate under the NARA disposition schedules. All data will be deleted/destroyed in accordance with OMB, NARA, and NIST regulations and guidelines.A file deleted from Sharepoint remains in the recycle bin for ninety days. The recycle bin must be emptied to permanently remove the document from SharePoint prior to the ninety-day expiration date.

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

See Section 2.8. Destruction of records occurs within the application by authorized personnel and does not create any additional risk. In particular, system users cannot delete or alter user audit trails, which are accessible only to system administrator(s).

8.0 Privacy Act

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

Whether data on a SharePoint site will be retrieved by a personal identifier depends on the particular business process for which the SharePoint site is set up. Generally, information about system users of any SharePoint site could be accessed by the system administrator and retrieved by user name or other user identifier.

With respect to the FOIA and Privacy Act appeals site, folders within the site will be organized and retrieved by appellant name. Other SharePoint sites may be used in a similar manner.

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

Generally, records pertaining to SharePoint system users are covered by: VII-3 – Computer Systems User Identification and Access Records – FTC.

With respect to the FOIA and Privacy Act SharePoint site:

Records pertaining to FOIA and Privacy Act appellants are covered by:
V-1 – Freedom of Information Act Requests and Appeals – FTC, and V-2 – Privacy Act Requests and Appeals – FTC.

Records pertaining to individuals whose information may be retrieved from some responsive materials would be covered by I-1 – Nonpublic Investigational and Other Nonpublic Legal Program Records – FTC, I-6 – Public Records–FTC, or other applicable FTC SORNs.

Copies of all FTC SORNs can be viewed and downloaded at: 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: _____
Sarah Mathias, Assistant General Counsel
Office of the General Counsel

Review:

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

_____ Date: _____
Peter Miller
Chief Privacy Officer

_____ Date: _____
Jeffrey Smith
Information Assurance Manager

_____ Date: _____
Jeff Nakrin
Director, Records and Filings Office

Approved:

_____ Date: _____
Jeffrey Huskey
Chief Information Officer