Federal Trade Commission
Privacy Impact Assessment

For the:

Desktop Major Application

October 20, 2011

1 System Overview

a. The Federal Trade Commission

The Federal Trade Commission (FTC, Commission, or Agency) is an independent federal law enforcement and regulatory agency with authority to promote consumer protection and competition through the prevention of unfair, deceptive, and anti-competitive business practices. The FTC pursues vigorous and effective law enforcement; advances consumer interests by sharing its expertise with federal and state legislatures and U.S. and international government agencies; develops policy and research tools through hearings, workshops, and conferences; and creates educational programs for consumers and businesses in a global marketplace with constantly changing technologies. The Commission enforces and administers a wide variety of competition and consumer protection laws.[1]

The Agency staff of approximately 1,400 employees and contractors operates out of three offices in Washington, DC, and eight regional offices located in Atlanta, Georgia; Chicago, Illinois; Cleveland, Ohio; Dallas, Texas; Los Angeles, California; New York, New York; Seattle, Washington; and San Francisco, California. The mission-related work of the FTC primarily is conducted by professional staff in the Bureaus of Consumer Protection (BCP), Competition (BC), and Economics (BE). The Office of the Chief Information Officer (OCIO) operates and maintains the necessary Information Technology (IT) services to support the mission, including the Agency's network, servers, applications, databases, computers, and communication facilities.

b. Background About the Desktop Major Application

The FTC Desktop Major Application (Desktop MA) is part of the Data Center General Support System (Data Center GSS).[2] (The FTC is treating the Desktop MA as a separate system for the purpose of this PIA.) The Desktop MA comprises all workstations, laptops, desktop software, multi-function devices, printers, and fax machines in the FTC along with selected minor applications. The OCIO is the business owner for the Desktop MA. The Desktop MA functions as the input and output mechanism for all internal access to the FTC data.

Generally, the Desktop MA is not a data repository. The Desktop MA primarily is used to manipulate and extract the data stored in the Data Center GSS. Although storage is available for the FTC staff and contractors on laptop and workstation hard drives (local drives), as a general practice, nonpublic data is stored on the shared network space that resides on the Data Center GSS. Individual staff and managers are responsible for the proper storage, handling, and use of Agency data residing on their workstations or laptops (the Desktop MA). Significantly, as

[1] A list of the statutes enforced or administered by the FTC is available at http://www.ftc.gov/ogc/stats.shtm
[2] The Privacy Impact Assessment for the Data Center GSS is available at http://www.ftc.gov/os/2011/08/1108datacenter.pdf

discussed in more detail below, FTC policy prohibits the storage of Sensitive Personally Identifiable Information (Sensitive PII) on the Desktop MA.

2 Information Collected and Stored within the System

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

The Desktop MA utilizes applications that process and store information in support of the Agency's mission. This can involve large volumes of information of many types that includes both public and nonpublic PII. PII may relate to specific defendants, individual targets of investigations, employees of corporate defendants or targets, witnesses, consumers, victims of fraud, FTC employees, FTC contractors, law enforcement partners, and others. Typically, this will include information in various electronic formats, such as word processing files, spreadsheets, databases, emails, images, videos, and audio files. This information includes law enforcement related information such as consumer complaints, affidavits, correspondence, financial information, health information, and other types of documents produced for the FTC pursuant to compulsory process or in the course of discovery.

Other information may include investigative hearing transcripts; transcripts of depositions in adjudicative proceedings; transcripts of adjudicative hearings and trials; briefs and other documents filed in adjudicative proceedings; orders entered in adjudicative proceedings; and briefs and other documents filed in federal court cases. Information potentially stored in the Desktop MA also includes staff and Agency-level memoranda; Congressional correspondence; Federal Register notices of rule makings; requests for formal and informal advisory opinions and FTC responses; news releases; and speeches given by the FTC officials. This list is not exhaustive, but illustrates the general categories of data that may be processed or stored on the Desktop MA.

The Desktop MA is not intended to maintain or store Sensitive PII. The FTC policy, which is mandatory and binding on all FTC officials, employees, and relevant contractors, provides that electronic documents (including email) containing Sensitive PII may be stored only on individually assigned FTC network storage space or on a shared FTC network drive in a file folder to which access has been restricted to authorized individuals who need the information to do their work. This data thus resides on the FTC Data Center GSS. Subject to limited exceptions, sensitive PII may not be stored on local computer drives (i.e., Desktop MA).

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

Information processed by the Desktop MA is obtained or created by the FTC staff in connection with the Agency's law enforcement functions, rulemakings, and other activities. Sources of information on the Desktop MA will vary. In some instances, this information is provided

voluntarily, such as when individuals submit comments in rulemaking proceedings or send correspondence to Congress that is then forwarded to the FTC, or when investigatory targets agree to provide information to the Commission in lieu of the compulsory process. The FTC also obtains information in response to the compulsory process, such as subpoenas and civil investigatory demands, and via discovery in administrative and federal court litigation.[3] Information processed by the Desktop MA also may be obtained from other sources, such as public resources on the Internet, nonpublic investigatory databases, other law enforcement agencies, and commercial databases such as LexisNexis®. In some instances, individuals—for example, third parties in investigations or witnesses in administrative and federal court proceedings—may provide information about other individuals or entities.

Information processed by the Desktop MA is also obtained from the FTC systems hosted by external entities, such as the Consumer Response Systems and Services (CRSS)[4] program, which gathers, processes, and updates consumer information; the Redress Program,[5] which permits redress class members to receive monetary disbursement from defendant-funded settlements or litigated final orders; and the Federal Trade Staffing and Employment Express (FT-SEE),[6] which is an automated recruitment and staffing system that enables the electronic submission and evaluation of applications for positions at the FTC.

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

Information processed by the Desktop MA is collected, used, disseminated, and maintained for the Commission to perform its law enforcement functions and other activities (e.g., internal administration, acquisitions, property management). For example, the FTC staff collect and use the information to investigate anti-competitive practices and to enforce statutes protecting consumers from fraudulent, deceptive, and unfair practices in the marketplace. In addition, the information is used to assist with consumer redress and to respond to Congressional correspondence.

2.4 How is the information collected?

Information processed by the Desktop MA is obtained or created by FTC staff in connection with the Agency's law enforcement functions and other activities.

The Desktop MA utilizes the information that is obtained by the FTC from a variety of sources, including information provided to the FTC voluntarily, as well as information obtained via

[3] See http://www.ftc.gov/ogc/brfovrvw.shtm for an overview of the Commission's investigative and law enforcement authority.
[4] The CRSS PIA is located at http://www.ftc.gov/os/2011/01/1101crss-pia.pdf
[5] The Redress Program PIA is located at http://www.ftc.gov/os/2011/01/1101crss-pia.pdf
[6] The FT-SEE PIA is located at http://www.ftc.gov/os/2007/09/ftsee_pia_web.pdf

compulsory process, discovery, or other investigative sources. Typically, information is obtained directly from targets of FTC's law enforcement activities and from individuals and entities with information that may be relevant to an FTC investigation. Information is generally collected directly from whatever media is used to submit it. This may include copying information from paper-based sources or from removable media such as CDs, DVDs, and hard drives. It may also include copying information that is electronically submitted via FTC's Secure File Transfer System[7], email, or some other electronic submission mechanism (e.g. through a website collection mechanism).

Information may also be collected by the FTC, its contractors, and law enforcement partners by entering the premises where the information is stored and using specialized computer equipment and software to copy the information to removable media (typically hard drives). Finally, information may be obtained from other sources, such as directly from the Internet, from other law enforcement databases, or from commercial sources.

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

Information that is used by the FTC is reviewed for accuracy and timeliness as required by the particular activity. For example, staff performing an investigation based upon a "whistleblower" complaint may check the information that is obtained to ensure that it is timely and accurate, while the information obtained for use in an economic study may be checked against publicly available information or analyzed by other testing or evaluation methods.

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

The Desktop MA does not employ any technologies that are new to the FTC. The system generally relies on commercial off-the-shelf (COTS) equipment, software, etc. Although the Desktop MA does not use technologies new to the FTC, the FTC has considered how the use of such technologies may affect individuals' privacy, and how the FTC has mitigated such risks, as described elsewhere in this document.

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 the Commission administers or enforces permit the collection of the information. For more information, see http://www.ftc.gov/ogc/stats.shtm.

[7] The Secure File Transfer System PIA is located at http://www.ftc.gov/os/2011/06/1106securefiletransfer.pdf

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

- Malicious Code (viruses, trojans, worms, root kits, spyware, and dishonest adware). To address these risks, the FTC deployed a suite of anti-virus tools that remove and block these malicious threats. Such threats include malicious code that could be downloaded to a workstation or laptop via a CD, DVD, or other portable storage device. In addition, the FTC staff do not have administrative rights to download and install additional software or applications to their FTC workstations or laptops.

- Hackers (individuals who access a computer system by circumventing its security system). To address this risk, the FTC implemented a defense-in-depth strategy in the Data Center GSS to include the use of firewalls, routers, switches, intrusion prevention and detection systems, and internet filtering. Additionally, the FTC participates in the Office of Management and Budget (OMB) Managed Trusted Internet Protocol Service (MTIPS) initiative that created a secure gateway to protect the FTC's internal network from traffic to/from external networks. Furthermore, the FTC participates in the Department of Homeland Security (DHS) Einstein program, which facilitates identification and response to cyber threats and attacks and improves network security, among other things.

- Unauthorized Access to Data (Logical and physical access). To address these risks, access to information is based on the least privilege security model. The most restrictive set of privileges are applied to Agency network user IDs upon creation. All network activity is closely audited and monitored. Any unauthorized activity is referred to the appropriate official for action. The FTC enforces a password policy for all workstations and laptops consistent with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 3, *Recommended Security Controls for Federal Information Systems and Organizations*. All laptops and mobile devices are encrypted consistent with the Federal Information Processing Standards Publication (FIPS PUB) 140-2, *Security Requirements for Cryptographic Modules*. Finally, all FTC staff and contractors with network access are required to execute a System Access Acknowledgement Form that addresses key information security policies and procedures.

- Data Leakage/Breach (unintentional release of sensitive PII to an untrusted environment). Management controls to address this risk include policies, procedures, and training to guard against unauthorized access, use, loss, theft or other potential data breaches. Physical controls include continuous human and video surveillance within the FTC facilities and perimeters, cables, locks, burn bags, secured cabinets, and storage rooms, etc. Logical controls include access lists and automated logging of system and user events.

- Misconfigured Information Asset. To address this risk, the FTC has deployed a strict configuration management program to approve and document all configuration changes made to Data Center GSS IT assets. In addition, the FTC staff do not have administrative rights to download and install additional software or applications to their FTC workstations or laptops.

- Unapproved Sensitive PII Storage. To address this risk, FTC policy states that electronic documents (including emails) containing Sensitive PII may be stored only on individually assigned FTC network storage space or on a shared FTC network drive in a file folder to which access has been restricted to authorized individuals. This data resides on the Data Center GSS, not the Desktop MA. The network storage space on the Data Center GSS is scanned to ensure that Sensitive PII is not stored in an unauthorized file folder. All FTC officials, employees, and relevant contractors are required to sign an annual compliance form certifying that they have identified the Sensitive PII under their control and will comply with this policy.

- Information Loss Through IT Asset Decommissioning. To address this risk, all IT asset hard drives are sanitized before reuse or degaussed before destruction. As Multifunction Devices are replaced, the FTC has contractual provisions in place that require the removal of the hard drive by the vendor, which is then turned over to the FTC for degaussing and destruction.

- Personally Owned IT Equipment. To address this risk, no personally-owned mobile wireless devices (e.g., personal digital assistants, smart phones [iPhone, Blackberry, Droid]), laptops, tablets (e.g., iPad), printers, eBook readers (e.g., Kindle, Nook) and personal electronic storage devices (e.g., removable media such as Universal Serial Bus (USB) flash drives, memory cards, external hard drives, or other equipment with electronic storage or communications capability such as digital cameras, portable digital music players) are allowed to be connected to any IT asset within the Data Center GSS.

3 Use and Access to Data in the System

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

Information may be used to support FTC's law enforcement functions and other activities, to include: investigating potential or alleged violations of anti-competitive practices, investigating and enforcing statutes protecting consumers against fraudulent, deceptive, or unfair practices in the marketplace, resolving consumer complaints, or assisting with consumer redress. Information may also be used to support internal agency functions (e.g., administration, property and records management, acquisitions, security, information technology).

3.2 Which internal entities will have access to the information?

Agency staff and contractors who require information to support the FTC law enforcement and other activities including system administrative activities to respond to FOIA and other disclosure requests will have access to the information. The information also is used to carry out administrative functions related to human resources, security, financial management, and matter and resource management.

3.3 Which external entities will have access to the information?

No external access is allowed, except by authorized individuals (e.g., contractors). Individuals outside the FTC may access data about themselves in the system, if any, as described below.

4 Notice and Access for Individuals

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

Wherever possible, the FTC provides notice to individuals about its policies regarding the collection, 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.

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

The opportunity or right to decline to provide information depends on how the information is collected and the purpose for the collection. For example, those who provide information pursuant to compulsory process generally do not have a right to decline to provide the information. In contrast, individuals who, for example, file public comments or requests for advisory opinions, or send inquiries to members of Congress, provide information about themselves voluntarily and may choose not to submit such information. An analysis of all data collection activities by the Agency is beyond the scope of this PIA.

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

The opportunity or right to consent to particular uses of the information depends on how the information is collected and the purpose for the collection. For example, those who provide information pursuant to compulsory process generally do not generally have a right to consent to particular uses of the information. In contrast, individuals who, for example, file public comments or requests for advisory opinions, or who send inquiries to members of Congress, provide information about themselves voluntarily and, by submitting such information, are consenting to the FTC's use of that information, as described in its Privacy Policy. Moreover, the FTC may, in some cases, negotiate or offer submitters the right to determine how their information is used or disclosed (e.g., in camera or protective orders). An analysis of all data collection activities by the Agency is beyond the scope of this PIA.

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

Individuals may file an access request under the Privacy Act of 1974 (PA) or the Freedom of Information Act (FOIA), depending on how the information is maintained and retrieved. The Privacy Act provides a procedure for individuals to request their own information, if the agency maintains and retrieves that information by the individual's name or other personal identifier (e.g., Social Security number). FTC's Privacy Act procedures are published in 16 C.F.R. 4.13 and may be viewed online at http://ecfr.gpoaccess.gov/. The request must be made in writing and, if mailed, it must be addressed as follows:

Privacy Act Request
Office of the General Counsel
Federal Trade Commission
600 Pennsylvania Avenue, NW.
Washington, DC 20580.

Privacy Act requests may also be made electronically using FTC's online FOIA request form, https://www.ftc.gov/ftc/foia.htm.

Otherwise, if information about an individual is not maintained and retrieved by his or her name, Social Security number, or other personal identifier, the individual's request must be made under the FOIA, rather than the Privacy Act. The procedures for making a FOIA request are similar to that of making a Privacy Act request, and are published in 16 C.F.R. 4.11, which can also be viewed online at http://ecfr.gpoaccess.gov/. Individuals who use FTC's online FOIA request form to file a PA or FOIA request will also have their request treated as a FOIA request for any records that fall outside of the PA.

Requesters should note that some records may be legally withheld from individuals for investigatory or other reasons under the FOIA and/or the PA. *See* section 8 of this PIA for additional details.

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

N/A. As noted earlier, individuals outside of the FTC seeking records about themselves do not have access to the Desktop MA.

5 Web Site Privacy Issues

5.1 Describe any tracking technology used by the Web site and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, Web beacon). Currently, persistent tracking technology is not approved for use by the FTC (see 5.2).

N/A.

5.2 If a persistent tracking technology is used, ensure that the proper issues are addressed (issues outlined in the FTC's PIA guide).

N/A.

5.3 If personal information is collected through a Web site, page, or online form accessible through the Internet, is appropriate encryption used? If not, explain.

N/A.

5.4 Explain how the public will be notified of the Privacy Policy.

The FTC's Privacy Policy is available to the public via a hyperlink on every FTC website. The FTC Privacy Policy is machine-readable (i.e., P3P compliant) and handicap accessible pursuant to Section 508 of the Rehabilitation Act.

5.5 Considering any Web site or Internet issues, please describe any privacy risks identified and how they have been mitigated.

N/A.

5.6 If the Web site will collect personal information from children under 13, or be directed at such children, explain how it will comply with the Children's Online Privacy Protection Act (COPPA).

N/A.

6 Security of Information in the System

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

The FTC follows all applicable Federal Information Security Management Act (FISMA) requirements, ensuring the Desktop MA is appropriately secured. The Desktop MA is categorized as moderate using Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.

6.2 Has a Certification & Accreditation (Security Control Assessment and Authorization) been completed for the system or systems supporting the program?

Yes.

6.3 Has a risk assessment been conducted on the system?

Yes.

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

No.

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

All FTC positions are assigned a risk designation and associated personnel screening criteria.

All potential FTC employees, contractors, and volunteers are subject to background investigations and suitability reviews per OMB guidance.

Before any new employee, contractor, or volunteer can access any data in the Desktop MA, they must first attend new employee orientation and successfully complete FTC's Privacy and Security Awareness training. All employees are granted basic network access to include email services, the Internet, the Intranet, network shared drives, network-based applications, and are assigned their own home directory. There are procedures to address access restrictions for higher-risk employees such as interns and International Fellows.

Supervisors and/or Contracting Officer's Technical Representatives (COTRs) must identify and approve employee requests to access network applications and specify the appropriate access privileges. Network and application access is based on: (1) a valid access authorization, (2) intended system usage, and (3) other attributes based on the system's business function. All network and application access is based on least-privilege and need-to-know security models.

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

All FTC employees are required to complete computer security training and privacy awareness training annually. Interactive online training covers topics such as how to properly handle sensitive PII and other data, online threats, social engineering, and the physical security of documents. Individuals with significant security responsibilities are required to undergo additional, specialized training, tailored to their respective responsibilities.

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

Auditing measures and technical safeguards are in place commensurate with the NIST SP 800-53, Rev 3, *Recommended Security Controls for Federal Information Systems and Organizations*.

6.8 Questions regarding the security of the system.

Any questions regarding the security of the system should be directed to FTC's Information Assurance Manager.

7 Data Retention

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

Information is retained and destroyed in accordance with applicable schedules and procedures issued or approved by the National Archives and Records Administration. The applicable schedule depends on the type of information involved (e.g., investigational, rulemaking, acquisitions). Electronic formats used to create paper records, such as word processing files, spreadsheets, and emails, are to be deleted within 180 days after the recordkeeping copy has been produced, which may be at the close of a project, litigation case or other kind of matter. Information that must be maintained in an electronic format, such as an audio file, is to be transferred to portable electronic media and placed in locked storage for recordkeeping purposes, then deleted from the Desktop MA within 180 days. Information in the Desktop MA acquired by the FTC in a matter investigation, study, or project that does not become part of a matter record file is to be deleted within 30 days of the close of the matter. Before the FTC deletes information not needed for the record file, the Desktop MA may be used to supply the information that is returned to the submitter upon request.

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

Disposal of all information will be conducted in accordance with the Office of Management and Budget (OMB) and NIST guidelines[8]. For the destruction of removable media and hard drives, the FTC has retained a vendor whose methods meet or exceed applicable standards for media sanitization and destruction.

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

An overall discussion of the privacy risks associated with the Desktop MA and the steps that the FTC has taken to mitigate those risks is provided in section 2.8, above.

As to information disposal, the FTC follows applicable NIST and OMB standards for media sanitization (*see* section 7.2), and has not identified any additional risks associated with information disposal.

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

8 Privacy Act

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

Some information processed or used by the Desktop MA may be retrieved by one or more personal identifiers (e.g. name, physical address, e-mail address, telephone number, etc.) that would make such records subject to the Privacy Act.

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

Yes. The FTC currently maintains 40 SORNs covering its systems of nonpublic investigatory records, public records, and other internal program and administrative records about individuals that may be processed or used by the Desktop MA. As required by the Privacy Act, these SORNs describe how these records may be used and disclosed by the FTC, including other details about each system of records (e.g., location, purpose, categories of individuals covered). All of these SORNs can be viewed and downloaded at http://www.ftc.gov/foia/listofpaysystems.shtm

9 Privacy Policy

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

The collection, use, and disclosure of the information in the Desktop MA has been reviewed to ensure consistency with FTC's privacy policy posted on its main Web site.

10. Scope of Desktop MA PIA and Future Modifications

Consistent with the requirements of the E-Government Act of 2002, the PIA will be revised to reflect any significant changes to the Desktop MA that impact the collection, storage, maintenance, or dissemination of PII. The PIA will not be modified to reflect routine application changes and modifications, version upgrades, feature patching, ongoing maintenance, new instances of existing products, or routine hardware upgrades such as the procurement of additional workstations or printers or fax machines. Changes to the Desktop MA are closely managed by OCIO and the decision to update this PIA will be made on case-by-case basis in consultation with the CPO.

11 Approval and Signature Page

Prepared for the Business Owners of the System by:

_____ Date: _____
Jeffrey Smith, Information Security Analyst
Office of the Chief Information Officer

Review:

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

_____ Date: _____
Marc Groman
Chief Privacy Officer

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

_____ Date: _____
Margaret Mech
Chief Information Security Officer

Approved

_____ Date: _____
Jeff Huskey
Chief Information Officer