Federal Trade Commission
Privacy Impact Assessment
for the:
www.FTC.gov Web site

March 2012

1 System Overview

The Federal Trade Commission (FTC or Commission) is responsible for implementing and enforcing Federal laws and regulations to promote consumer protection and competition. The FTC's work is divided among the bureaus of Consumer Protection, Competition, and Economics. The Bureau of Consumer Protection (BCP) aims to protect and empower consumers by preventing fraud, deception, and unfair business practices. The Bureau of Competition (BC) promotes healthy competition by surveying the marketplace for anti-competitive behavior and enforcing antitrust laws. Finally, the Bureau of Economics provides economic expertise to BC and BCP, and also prepares economic analyses of government regulation and policy recommendations regarding consumer protection and competition that may be shared with Congress, the Executive Branch, and the public.

The agency's central point of public information online is the FTC Web site: www.FTC.gov. This Web site includes content about the FTC's customer-facing departments; links to publicly published cases, reports, events, and resources; downloadable audio and video education files; RSS feeds; links to the Commission's social media accounts; and much more.

To comply with the Privacy Act of 1974, the E-Government Act of 2002, guidance issued by the United States Office of Management & Budget (OMB) and the FTC's own Privacy Policy, the FTC collects only the minimum information necessary to respond to customer concerns, and conduct investigations and other program activities. This Privacy Impact Assessment (PIA) explains what Personally Identifiable Information (PII) the FTC collects about individuals throughout the various touch points on www.FTC.gov, how the agency collects it, who is allowed to use this information and for what purposes, and what steps the FTC has taken to identify, secure, and reduce any privacy risks to that information.

Collectively, the FTC currently manages multipleWeb sites/microsites and maintains a social media presence, including two of its own blogs and agency accounts on Facebook, Twitter, and YouTube. This PIA primarily covers www.FTC.gov, but also serves as a hub for all FTC Web sites, microsites, social media sites, and applications, and their corresponding PIAs where applicable.

FTC Web sites, microsites and other features

Much of www.FTC.gov is a static Web site and, unless otherwise noted, does not use tracking technologies or collect PII from visitors. The main Web site is hosted on the internal FTC data servers and administered by FTC staff members. The following are the primary points of information collection that are either located within www.FTC.gov or have an appearance consistent with the www.FTC.gov design, resulting in a seamless user experience. Some of these information collection points are hosted externally and/or are accessible from unique Web site addresses displayed as Internet domains other than FTC.gov.

1. **Bulk Order:** Visitors interested in ordering bulk education materials from the FTC can do so through this feature located on www.FTC.gov. Review the Bulk Order PIA for more information.

2. **CommentWorks®:** Visitors to the Commission's Web site may file public comments on FTC matters via a secure web-based form that uses the CommentWorks® software, currently hosted by an FTC contractor. This form is accessible from the relevant FTC rulemaking and workshop pages throughout www.FTC.gov. Comment periods are generally open for 30 or 60 days, unless otherwise noted. More information about the collection of public comments is available in the Collection of Public Comments Filed Electronically PIA.

3. **Complaint Assistant:** Visitors to www.FTC.gov/complaint seeking to file a complaint with our agency are redirected to the secure Complaint Assistant Web site. Review the Sentinel Network Services PIA for more information.

4. **E-mail This News Release Feature:** This feature, which does not collect any user data for the FTC, allows visitors to www.FTC.gov to forward a web page of interest to other email address(es). When a user clicks on this button accessible from certain pages on www.FTC.gov, it causes the e-mail program on the user's computer to open and create a draft e-mail that automatically contains a hyperlink to the FTC online press release. The draft e-mail allows the user to enter the e-mail address of the receiving party. This information is used only one time for the purposes of sending the email from the user's computer and is not transmitted to or stored by the FTC.

5. **Event Registration:** In support of its general law enforcement, rulemaking, and community education and outreach programs, the FTC conducts workshops, seminars, and events. The FTC web pages for these events sometimes include an FTC e-mail address for individuals to register voluntarily if they plan to attend the event. Individuals are asked to provide basic information, such as name, e-mail, and telephone number. This PII is used only by the event organizers for the purposes of event logistics, such as space management and name tag preparation.

6. **GovDelivery:** A secure connection e-mail management system that allows visitors to sign up for e-mail updates to blogs, e-newsletters, press releases and consumer and business education, and manage their subscription preferences using their e-mail address and a self-chosen password stored by the system. This feature appears on a number of www.FTC.gov pages and microsites (e.g., BCP Business Center blog). More information about the collection of email addresses and passwords for this purpose is available in the GovDelivery PIA.

7. **FOIA Request:** Visitors to www.FTC.gov are able to request access to nonpublic FTC records under the Freedom of Information Act (FOIA) via a secure automated FOIA Request Form hosted on FTC's servers. This information is logged into a database accessible to a small number of specified FTC professionals who need system access to

process and fulfill the FOIA requests. More information regarding this process can be found in the FOIAXpress PIA.

8. **Registered Identification Number (RN) Database:** This Oracle database contains registration information for manufacturers, retailers, and other companies subject to the label requirements of the Textile, Wool Products, and Fur Labeling Acts, The database is hosted on the FTC internal data server, and accessible through the RN program pages at www.FTC.gov. The FTC's RN pages contain online forms allowing a company to apply for an RN, which must be printed on the garment label to identify the company, or to update the company's information in the database. There is also a database search function allowing any user to enter a company name or other data (ZIP, State, Product Line, etc.) to determine the assigned RN(s) (or vice versa). All data collected, maintained, and made publicly available in this database pertain solely to registered companies. The online application form requires the filing company to name the company official who is certifying the application on the company's behalf, but that identifying information is not available to the public through the search engine. No other information about any individual in his or her business or personal capacity is collected, stored, retrieved, or retrievable from the database. (The FTC's RN pages also contain a link to the Canadian RN database, which is operated and maintained by Canada's Competition Bureau, and is not under the FTC's control.)

In addition to www.FTC.gov, the following Web sites, accessible from www.FTC.gov, are managed internally by FTC staff members on FTC servers and abide by the FTC's privacy policy:

9. **HSR.gov:** This FTC Web site allows visitors to electronically submit forms required to comply with the Hart-Scott-Rodino (HSR) Act. The HSR Electronic Filing System ("ePremerger") is intended to provide a secure electronic method for merging parties to submit a "Notification and Report Form for certain Mergers and Acquisitions" and any necessary attachments, which ordinarily contain confidential business information protected by the HSR Act. Note: At the time of this PIA, the FTC has a pending rulemaking that will significantly revise the HSR Form. The Premerger Office is in the process of creating a new electronic HSR form for e-filing. Consequently, use of the existing e-filing form has been discontinued. Review the HSR PIA for more information.

10. **Joint ID Theft Web site:** This Web site covers information about the President's Task Force on Identity Theft, established in May 2006. This site provides information about what the government is doing to combat ID theft. It does not collect any PII.

11. **We Don't Serve Teens:** We Don't Serve Teens is a national campaign to prevent underage drinking. The Web site provides information and resources for individuals, organizations, media, retailers, and law enforcement. The Web site allows visitors to download tools, such as campaign artwork, pre-written materials and templates, in support of the campaign on a local level. This Web site does not collect any PII.

12. **NCPW Web site:** National Consumer Protection Week (NCPW) is a coordinated campaign that encourages consumers nationwide to take full advantage of their consumer rights and make better-informed decisions.

13. **Admongo:** This FTC Web site is an online video game that educates children about advertising in a fun and engaging way. Review the Admongo PIA for more information.

14. **OnGuard Online** (and Alerta en Linea, the Spanish language version of OnGuard Online): This FTC Web site teaches consumers and businesses about information security, computer fraud, and online safety issues. It is available in English and in Spanish. Review the DCBE Web sites and Blogs – OnGuard Online, Alerta en Linea, and BCP Business Center PIA for more information.

15. **Business Center Web site and Blog:** A microsite and blog developed and managed by the Bureau of Consumer Protection that provides resources to individuals and businesses to help them comply with consumer protection laws the FTC enforces. Review the DCBE Web sites and Blogs – OnGuard Online, Alerta en Linea, and BCP Business Center PIA for more information.

The following FTC Web sites, microsites, and features are hosted externally on third-party servers, but are managed by FTC staff members. All of the following FTC-affiliated Web sites/microsites are hosted in the United States. Unless otherwise noted, each of the sites abides by the FTC's privacy policy. Please refer to the respective PIAs for specific information regarding each site, all of which are hyperlinked below:

16. **Consumer Sentinel Network:** This FTC Web site provides law enforcement members of the Consumer Sentinel Network with secure access to millions of consumer complaints. Review the Sentinel Network Services PIA for more information.

17. **Do Not Call Registry:** Individuals seeking to register their home or cell phone numbers on the National Do Not Call Registry can do so through this secure FTC Web site. BCP uses the DNC to protect consumers from unwanted telemarketing sales calls, to educate telemarketers on relevant laws, and to help law enforcement investigate violations. Review the Sentinel Network Services PIA for more information.

18. **Do Not Call Registry (Telemarketers):** Telemarketers, sellers, and other such entities use this Web site to help them comply with the Telemarketing Sales Rule's Do Not Call provisions – particularly to download the current list of telephone numbers. Review the Sentinel Network Services PIA for more information.

19. **E-Consumer Complaint Assistant:** Located on the FTC's www.econsumer.gov Web site, this complaint assistant gathers complaints related to cross-border e-commerce fraud and provides online complaint forms in English, Spanish, French, German, Polish, Japanese, and Korean. Review the Sentinel Network Services PIA for more information.

20. **E-Filing:** The FTC's E-Filing System is a web-based application that enables parties to use the Web site to submit public filings electronically in adjudicative proceedings under Part 3 of the FTC's Rules of Practice, 16 CFR Part 3, and reduce time, expense, and burden associated with filing for the FTC and other parties in Part 3 proceedings, while continuing to ensure the security, integrity and availability of such filings. Review the E-Filing PIA for more information.

21. The FTC sometimes uses Web sites that allow individuals to submit redress claims online and to review the status of their claims. These sites are hosted by FTC contractors in data centers that are authorized to process in accordance with all applicable Federal Information Security Management (FISMA) requirements. Review the BMC Group's ClaimTracker and Online Claim Submission Websites PIA and Rust Consulting Online Claims Submission Websites PIA for more information.

Social Media

A key feature of the www.FTC.gov Web site is the "Stay Connected" console located on the home page that allows visitors to connect with the Commission via several social media outlets. Each official account is managed by FTC staff members, but the sites themselves are third-party sites, and the FTC privacy policy discusses, but does not directly apply, to them.

When leaving www.FTC.gov via a "Stay Connected" link, where applicable, visitors encounter an exit script alerting the visitor that they are leaving the FTC Web site, that the FTC's privacy policy does not apply to the new destination, and that these sites may collect information about them. Conversely, each of the Commission's social media pages provides a "privacy notice" (as required by OMB Memorandum 10-23) that the official source of FTC information is www.FTC.gov, as well as a link to the FTC's privacy policy.

Finally, each of the agency's social media sites is covered in a separate PIA in order to flesh out how the FTC uses these sites to promote news, information, tips, resources, and more to visitors who may not be regular visitors to www.FTC.gov:

1. **Add This:** This feature is currently only used in conjunction with the Business Center (BC) Web site and Blog and the OnGuard Online Web site. Refer to the respective PIA for more information.

2. **Blogs:** The Commission maintains threeblogs.. Theier PIAs are referenced above.
    a. OnGuard Online Blog
    b. Alerta en Linea Blog
    c. Business Center Blog

3. **Facebook:** The FTC has three Facebook accounts:
    a. Federal Trade Commission
    b. OnGuardOnline
    c. Alerta En Linea

4. **Twitter:** The FTC maintains two Twitter accounts; one in English and one in Spanish:
    a. FTC
    b. LaFTC

5. **YouTube:** Refer to YouTube PIA for more information.

Unidirectional Social Media Applications, Communications, and Outreach

Unidirectional social media applications allow users to view relevant, real-time content from predetermined sources. Dynamic communication tools such as podcasts, audio, and video streams, and Really Simple Syndication (RSS) feeds broaden the FTCs ability to disseminate content and provide the public multiple channels to receive and view content.

In addition to the GovDelivery system and social media tools mentioned earlier in this PIA, the following is a list of unidirectional tools currently used by the FTC. This section will address the FTC's use of such applications, describe the PII, and the extremely limited circumstances that the FTC will have access to PII, how it will use the PII, what PII is retained and shared, and how individuals can gain access to their PII.

1. **Audio Public Service Announcements (PSAs) and Podcasts:** Users may listen to FTC PSAs via MP3 or WAV files throughout the www.FTC.gov Web site. In addition to standard audio files, some FTC Web sites such as the Business Center provide podcasts. Users may download or simply listen to FTC audio content. The FTC may provide direct links for users to share the content on other Web sites. The FTC does not collect, track or have access to PII of the users who download, listen to, or share these files.

2. **Really Simple Syndication (RSS) feeds:** Visitors to www.FTC.gov may subscribe to the agency's press releases via RSS feeds. This subscription feature relies on RSS software that the user clicks or otherwise activates on his or her own computer, Web browser, or mobile device when visiting the FTC's RSS page to check the FTC's news feed on a regular basis and to collect new press releases available for the user's review. The FTC does not have collect, track or have access to PII of the users who subscribe to its feeds.

3. **Videos:** The FTC provides the public access to multiple educational videos. Visitors to www.FTC.gov/video can watch pre-recorded FTC videos via MOV or WMV files. This content is also featured on the FTC's YouTube channel. The FTC does not collect, track or have access to PII information of the users who watch these videos on either site.

4. **Webcasts**: A webcast is audio and video material that is available live from www.FTC.gov at the same time an event is occurring. Visitors to the FTC's webcast page can also access previously recorded and archived events. The FTC has a contract with a third-party site to host and manage this content. This Web site does not use cookies, collect information from its visitors, or utilize tracking technologies such as web logs or

analytic software to collect PII. The overall FTC privacy policy governs the use of this Web site.

The FTC.gov Web site is maintained by FTC's Office of Chief Information Officer (OCIO) Web team, with FTC staff members administering various parts of the site.

2 Information Collected and Stored within the System

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

The FTC's data servers automatically collect the following standard web log parameters: IP address, date and time of visit, browser, visit history, hits history, entry page, exit page, operating system, and referral URL.

For each of the individual microsites, features, and social media sites discussed above that collect, disseminate, or utilize information through online forms, comment soliciting forms or otherwise, please refer to respective PIAs as referenced in Section 1.0, System Overview.

Additionally, session cookies found on microsites and features track information like user IDs and preferences only while the user is on the page to enable a particular functionality or provide a more streamlined experience for the user. This is discussed in more detail in Section 2.4.

None of the unidirectional social media applications the FTC utilizes collect, use or disseminate PII, with the exception of the FTC e-mail updates, which are covered by the GovDelivery PIA as described in Section 1.0.

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

All PII through the site (*see* Section 2.1) is obtained directly from visitors to the site.

The FTC's data servers hosting the Web site automatically collect information from those who visit the Web site as described in Section 2.1.

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

Standard web log files are collected to analyze traffic to the site and help create a better user experience for FTC customers.

PII is collected by the site through various online forms and comment soliciting features posted or linked on the site for a variety of reasons ranging from requiring it for bulk orders of FTC materials to allowing individuals to add PII in connection with the Do Not Call feature. Refer to the respective PIAs referenced in Section 1.0 for more information.

2.4 How is the information collected?

PII is collected by the site through various online forms or comment soliciting features posted or linked on the site.

The microsites and features listed below also use session cookies in a limited number of pages to collect information in connection with the online forms and comment soliciting features referenced in Section 1.0. Refer to their respective PIAs for more information.

- Bulk Order
- Do Not Call Registry
- Do Not Call Registry (Telemarketers)
- E-Consumer Complaint Assistant
- E-Filing
- BMC Group's ClaimTracker and Online Claim Submission Websites
- Rust Consulting Online Claim Submission Websites
- DCBE Web sites and Blogs -- OnGuard Online, Alerta en Linea, and BCP Business Center PIA

As explained elsewhere, there are no persistent cookies on the www.FTC.gov Web site. To learn more about cookies in general and how they are collected and used by the FTC, also refer to http://ftc.gov/ftc/cookies.shtm.

Web log files are collected automatically by the web hosting provider's services.

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

Individuals submitting PII by filling out online forms posted or linked through www.FTC.gov or by commenting on workshops and rulemaking are responsible for checking the accuracy and timeliness of their information. In some cases, the online forms are designed to inform the individual when certain necessary information is missing or in the wrong format (e.g., e-mail address for e-mail updates).

The FTC does not routinely evaluate the accuracy of the web log files maintained by the FTC's internal servers or third-party contractors operating sites for the FTC. Such logs may be reviewed, however, for security reasons. (System security of www.FTC.gov is discussed elsewhere in this PIA.)

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?

No.

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

The FTC Act authorizes the FTC to prevent unfair and deceptive acts and practices in interstate commerce and, in furtherance of this mission, to gather, compile, and make information available in the public interest.

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

At points of collection of information directly from individuals (e.g., online forms), the FTC uses the Hypertext Transfer Protocol (HTTPS) to provide encrypted communications to mitigate risks of unauthorized interception or access.

Online forms found on www.FTC.gov collect the minimum PII necessary for the respective purposes. Any privacy risks posed by the various online forms and comment soliciting features posted or linked through www.FTC.gov are discussed in their respective PIAs, referenced in Section 1.0.

To prevent spoofing of the FTC Web site by outside entities, which can result in consumers being redirected to malicious Web sites that collect their personal information, the FTC is using Domain Name System Security (DNSSEC) Extensions at the domain level. DNSSEC is used as a digital signature for domain name system lookup using public-key cryptography, thereby improving integrity and authenticity of information and decreasing the risks associated with DNS-based attacks. *See* Section 6.1 for more information.

The risk of unauthorized access is mitigated by having only a small number of FTC employees with access to the automatic web log information and by requiring users to change their password every 60 days. Furthermore, the FTC administrators have a minimal level of access necessary to perform the tasks of updating Web site content and obtaining web logs for analysis.

3 Use and Access to Data in the System

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

The web log files are received as raw data files and subsequently evaluated by FTC staff in an effort to improve traffic flow through the Web site, provide more relevant content to Web site visitors and to improve overall user experience on the Web site.

PII is collected by the site through various online forms and comment soliciting features posted or linked on the site, is used to support various FTC functions, campaigns, and outreach programs. The specific uses of information collected through these forms and features are discussed in their respective PIAs, referenced in Section 1.0.

3.2 Which internal entities will have access to the information?

A limited number of FTC staff who provide and/or review internal reports on visits to www.FTC.gov and related microsites, OCIO, BCP, and OGC, will have access to the web hosting provider's web log information.

With respect to the PII collected by the site through various online forms and comment soliciting features posted or linked on the site, the entities having access to that information differ, as discussed in their respective PIAs, referenced in Section 1.0.

3.3 Which external entities will have access to the information?

The website is currently hosted on the FTC internal data servers. As such, external entities do not have access to www.FTC.gov Web site or the web log information.

As discussed above (*see* Section 1.0), some of the web pages and microsites on or accessible from www.FTC.gov are hosted and managed externally by third-party contractors. All PII collected through these pages is subject to FTC's privacy policy. For more information about which entities have access to specific PII collected through these pages, refer to their respective PIAs, referenced in Section 1.0.

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?

The FTC privacy policy accessible from every web page informs Web site visitors about what information is collected and how it will be used. Some microsites accessible from www.FTC.gov contain their own privacy policies linked directly from those pages. For more detail about all of the microsites, refer to their respective PIAs (*see* Section 1.0).

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

All information provided by individuals to the FTC via various Web sites, microsites, and features of www.FTC.gov is voluntary, as described in the respective PIAs referenced in Section 1.0.

By using the Web site, all site visitors agree to the terms of use for the Web site regarding the automatic collection of weblog information, as described in the FTC privacy policy.

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

Visitors do not have a right to consent to or otherwise determine how the agency uses the web logs automatically captured by www.FTC.gov. Likewise, by voluntarily submitting any personal

information through online forms or other features on the Web site, the individual is consenting to the use of the information by the FTC stated in the FTC's privacy policy.

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 (PA) or the Freedom of Information Act (FOIA), depending on how the information is maintained and retrieved. The PA 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). The FTC's Privacy Act procedures are published at 16 C.F.R. 4.13, which 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.

PA Requests may also be made electronically using the FTC's online FOIA request form, https://www.ftc.gov/ftc/foia.htm.

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 making a Privacy Act request, and are published at 16 C.F.R. 4.11, which can also be viewed online at http://ecfr.gpoaccess.gov/. Individuals who use the 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 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.

The Web site is not configured to allow members of the public or other external entities to gain access to any nonpublic information gathered by the Web site about individuals, and any such requests for access to this information require a formal written FOIA/Privacy Act request, as noted in Section 4.4. See Section 6 for information regarding security measures. Thus, there are no privacy risks associated with allowing individuals themselves to obtain records from the system, since they are not allowed to do so.

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).

FTC does not use persistent cookies or other persistent technology for visitors.
The microsites and features listed below use session cookies in a limited number of pages to collect information in connection with the online forms and comment soliciting features referenced in Section 1.0. Refer to their respective PIAs for more information.

- Bulk Order
- Do Not Call Registry
- Do Not Call Registry (Telemarketers)
- E-Consumer Complaint Assistant
- E-Filing
  BMC Group's ClaimTracker and Online Claim Submission Websites
- Rust Consulting Online Claim Submission Websites
- DCBE Websites and Blogs – OnGuard Online, Alerta en Linea, and BCP Business Center PIA

To learn more about cookies in general and how they are collected and used by the FTC, also refer to http://ftc.gov/ftc/cookies.shtm.

5.2 If a persistent tracking technology is used, ensure that the proper issues are addressed.

FTC does not use persistent cookies or other persistent technology for visitors.

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.

Appropriate encryption (e.g., https) is used for all FTC Web forms posted or linked on the Web site.

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

The Web site includes a prominent link to its privacy policy in the top navigation bar, accessible from every page. As explained earlier, the FTC also provides links to its privacy policy on its social media pages.

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

See Section 2.8.

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).

The Web site is not intended to collect any information from children under 13 years of age.

The only FTC Web site that is directed at young consumers and is linked from www.FTC.gov is AdMongo. The Web site does not collect personal information.

For further information regarding FTC's compliance with COPPA, review the Sentinel Network Services PIA.

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 www.FTC.govWeb site is appropriately secured. The www.FTC.gov Web site is hosted in the Data Center GSS which is categorized as moderate using Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.

In addition, as mandated by *Office of Management and Budget (OMB) Memorandum M-08-23, Securing the Federal Government's Domain Name System (DNS) Infrastructure*, the FTC has deployed Domain Name System Security (DNSSEC). This provides cryptographic protections to DNS communication exchanges, removing threats of DNS-based attacks and improving integrity and authenticity of information processed over the Internet.

6.2 Has a Certification & Accreditation (security control assessment and authorization) been completed for the system or systems supporting the program?

The www.FTC.gov Web site is maintained as part of the Data Center General Support System (GSS), which is certified and accredited. \

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.

Yes, and the FTC has addressed risks and vulnerabilities as described elsewhere in this document. *See*, *e.g.*, Section 2.8.

As discussed in Section 1.0, online forms and comment soliciting features located on or linked to from www.FTC.gov, address relevant privacy concerns in their respective PIAs. Refer to Section 1.0 for more information.

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

The Web site is public and accessible via the internet. Documented procedures limit access to nonpublic portions (i.e., log, site administration, forms data, etc.) to authorized FTC and contractor personnel only.

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

All FTC employees and designated contractor personnel 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 National Institute of Standards and Technology (NIST) Recommended Security Controls for Federal Information Systems and Organizations Moderate-Impact Baseline Special Publication (SP) 800-53, Rev. 3.

6.8 To whom should questions regarding the security of the system be addressed?

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

7 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. Data not covered by the Federal Records Act, such as session cookies described in PIA section 2.4, is deleted/destroyed when no longer needed.

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.

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 2.8Destruction 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 Privacy Act

This section addresses the applicability of the Privacy Act of 1974 to the system, and whether or not the system is covered by a System of Records Notice (mandated for some systems by the Privacy Act of 1974).

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

Web log data is collected and maintained in raw form, is used only to analyze traffic patterns as opposed to individual activity, and is not maintained or routinely retrieved by personal identifier.

Data collected directly from individuals through online forms, e-mail addresses listed on the site, etc., may be maintained and/or incorporated into one or more agency record systems retrieved by personal identifier, as described in Section 8.2.

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

As noted above, data collected directly from individuals through the site may be maintained and/or incorporated into one or more agency records systems retrieved by personal identifier and, thus, subject to the Privacy Act.

For example, rulemaking and workshop comments collected through online ICF CommentWorks® forms linked to the Web site are eventually posted publicly on the Web site, subject to retrieval by commenter name. The FTC's SORN for public records covers these comments (FTC I-6).

Complaint data collected through the Complaint Assistant form are covered by the FTC's Consumer Information System SORN (FTC IV-1). This data may then be incorporated into

other FTC records systems, as appropriate, such as its nonpublic legal program records (FTC I-1).

FOIA Requests form data are covered by FTC IV-1 (and Privacy Act request data, if any, by FTC IV-2).

All of the FTC's SORNs are listed and can be downloaded from our public SORN page: 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 www.FTC.gov has been reviewed to ensure consistency with the FTC's privacy policy. Additionally, the FTC privacy policy explains what the FTC does with personal information that it may collect and maintain on individuals and is accessible from every page.

10 Approval and Signature Page

Prepared for the Business Owners of the System by:

_____ Date: _____
Barri Hutchins, Webmaster
Office of Chief Information Officer

Review:

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

_____ Date: _____
Peter Miller
Acting Chief Privacy Officer

_____ Date:
Jeff Nakrin
Director, Records and Filings Office

_____ Date: _____
Jeffrey Smith
Information Assurance Manager

Approved:

_____ Date: _____
Jeff Huskey
Chief Information Officer