



**Federal Trade Commission  
Privacy Impact Assessment**

**for the:**

**Hart Scott Rodino Act Electronic Filing System and HSR.gov**

**Updated: June 10, 2011**

## **1 System Overview**

The website [www.hsr.gov](http://www.hsr.gov) will provide online public access to information and electronic forms for merging parties filing notification of proposed acquisitions for review by the Bureau of Competition of the Federal Trade Commission (“FTC”) and the Antitrust Division of the Department of Justice (“DOJ”) under the “Hart-Scott-Rodino” provisions of the Clayton Act § 7A, 15 U.S.C. § 18a (“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” (FTC Form C4) and any necessary attachments (collectively referred to as a “filing”), which ordinarily contain confidential business information protected by the HSR Act. The system will also fulfill the requirements of the E-GOV Act and the Government Paperwork Elimination Act, which requires agencies, unless not practicable, to provide electronic filing, signature, disclosure and record keeping options for existing paperwork requirements.

The Bureau of Competition’s Premerger Notification Office, with contractor assistance, has designed and will principally manage and operate the components of the system used by the filing parties. The FTC also operates the internal components of the HSR database system that already exists behind the FTC’s firewall, with modifications to accommodate electronically filed data. Filers or their designated legal representatives will download PDF electronic filing form from the HSR.gov website, which the FTC will host on its servers. The filer will use Adobe Acrobat Reader (version 9) to open and complete the form electronically on their own computers, attach necessary documentation such as an affidavit, and then upload the filing electronically to the Agencies through secure means, as described further below. Once the form and attachments have been received by the Agencies’ own servers, the form will be decrypted, and the confidential data extracted from the form will be available to both Agencies electronically for the premerger review required by the statute.

## **2 Information Collected and Stored within the System**

Although FTC Form C4 is used to collect information from filing parties about their proposed corporate acquisitions, ePremerger system will collect only limited amounts of personally identifiable information incidental to the filing.

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

If a person downloads and submits the FTC Form C4, he or she will be asked to submit the same information that they would submit on the paper version of the forms. Since these forms are designed for corporations making acquisitions subject to antitrust review by the Agencies, the forms collect information relating to businesses, not individuals. Nonetheless, as part of that process, the form requires some miscellaneous information in identifiable form, *e.g.*: taxpayer identification number, which could be a Social Security number of an individual in some cases; names, titles, firms, business addresses, telephone

and fax numbers, and e-mail addresses of contact persons regarding the report and for purposes of receiving notice of requests by the Agencies for additional information from the filer; names of shareholders, who may be individuals in some cases; and the name, title, and, with the electronic form, the signature of the person submitting the form, and e-mail addresses, some of which may pertain to individuals.

Additionally, when a filer uploads the FTC Form C4, a submission form is attached to the FTC Form C4 and collects the name, firm, phone and email address of the person submitting the form. This information will be used to notify the individual of any problems with the filing process or the form.

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

The information is provided by individuals and/or companies required to file notification with the Agencies.

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

The Agencies are required to review proposed acquisitions of a certain transaction size, and FTC Form C4 are necessary in order to ensure that relevant information about the transaction is consistently identified and reviewed in a timely manner. Any personally identifying information that is incidentally collected on these forms is needed for contact, payment processing, debt collection, and reporting purposes. The filings are required by the HSR Act. Likewise, it is necessary to collect other identifying information, including taxpayer identification number required under 31 U.S.C. § 7701, in order to collect and report payments, since the collection of fees is mandated by appropriations law and funds the agency's work.

Log data is collected for system security purposes.

## **2.4 How is the information collected?**

With the exception of log data and submission form, the majority of the information is collected in the FTC Form C4.

Log data is generated by the system automatically.

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

Merging parties are responsible for submitting accurate information and for submitting corrective filings as appropriate. Additionally, contact information is requested at the time of filing in the event the Agencies need to contact the submitting party for any reason. The Agencies do not validate the accuracy of any contact information or other incidental PII attached to the filing, which is the responsibility of the filer.

**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. The system utilizes commercially available document formatting software (Adobe) and standard SSL and encryption technology that the agency has utilized for toerh agency programs and functions.

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

The HSR Act, Section 7A of the Clayton Act, 15 U.S.C 18a, requires parties of certain mergers and acquisitions to file a notification with the FTC and DOJ.

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

There is risk that information in the form or system will be viewed or altered by unauthorized parties. The form submission (PDF files) is encrypted during the transmission process across the Internet using HTTP/SSL. The form submission is encrypted and stored on a secure server before being transferred to the agencies internal systems.

**3 Use and Access to Data in the System**

The following questions are intended to clearly describe how the information in the system will be used, and who will use it.

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

The purpose of the ePremerger is to facilitate the submission of FTC Form C4 via electronic means. Once a filing is received and processed, it is accessible by the reviewing agencies through a shared database which. The agencies conduct an preliminary antitrust evaluation with the information provided in FTC Form C4.

**3.2 Which internal entities will have access to the information?**

Premerger Notification Office staff will have the ability to review submissions and notification information. Premerger Notification Office staff will not be able to edit any

forms or attachments. The HSR Act strictly prohibits the reviewing agencies from sharing or publicly disclosing this information, except as may be relevant in judicial or administrative proceedings. The law does not prevent disclosures to either house of Congress or any duly authorized Congressional committee or subcommittee. Thus, the information will normally be shared only between the two reviewing agencies, i.e., FTC and DOJ. The personally identifiable information that is incidentally collected with the filing may be shared with other agencies or contractors for payment processing, debt collection, and reporting purposes.

The system is maintained and operated by the FTC. The system administrator has full access rights to all documents in the system in order to assist with maintenance of and enhancement to support the system's operations.

### **3.3 Which external entities will have access to the information?**

Merging companies or their intermediaries will not have access to any information filed through this system. No external entities will have access to the FTC form C4 once submitted.

## **4 Notice and Access for Individuals**

The following questions are directed at how or whether the individual is notified of the scope of information collected. They also concern the individual's right to consent to uses of information, right to decline to provide information, ability to ensure the accuracy of the information collected, and right to access their information.

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

The website, [www.hsr.gov](http://www.hsr.gov) will provide detailed explanation and instructions on filling out FTC Form C4 and provide notice about what information is collected, and how it is used and disclosed.

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

While the HSR Act makes premerger filings mandatory for parties proposing acquisitions that fall within the scope of the Act's filing requirements, use of ePremerger is optional and voluntary.

**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 agencies, consistent with the HSR Act, cannot legally provide filers an opportunity to limit the collection or use of the information for purposes authorized by the Act. Likewise, because filers are required to pay filing fees, the agencies cannot provide an opportunity for filers to limit the collection or sharing of relevant information for payment processing, debt collection, or reporting purposes. In particular, we are required to collect taxpayer identifying numbers pursuant to 31 U.S.C. § 7701.

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

Once the parties have submitted a filing to the agencies, there are no procedures allowing them to access that information. On rare occasions, upon request, the FTC will provide a copy of a previously filed form when a party has lost the original form or changed law firms and has no access to the original filing.

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

Merging companies or their intermediaries will not have access to any information filed through this system.

**5 Web Site Privacy Issues**

Complete this section only if the new system or project creates or modifies an FTC Web site, page, or online form accessible through the Internet.

**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).**

The system does not use persistent or temporary cookies, web beacons, or other persistent tracking technology.

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

Not applicable.

**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.**

The form transmission via the Internet is encrypted via a secure connection (HTTPS/SSL).

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

Filers are provided with a Privacy Act statement, to the extent applicable, on forms used to collect the information. Additionally, Every page of the web site, [www.hsr.gov](http://www.hsr.gov) will contain a link the FTC Privacy Policy <http://www.ftc.gov/privacy>.

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

The form submission (PDF files) is encrypted during the transmission process across the Internet using HTTP/SSL. The form submission is encrypted and stored on a secure server before being transferred to the agencies internal systems. Because the system does collect confidential business information and small amounts of information in identifiable form, the system has access restrictions and other security measures to protect all system data.

**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).**

This system is not intended to collect information from children under 13. Therefore, COPPA does not apply.

## 6 Security of Information in the System

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

### **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 ePremerger is appropriately secured. ePremerger resides on the Infrastructure General Support System (GSS) which 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 been completed for the system or systems supporting the program?**

ePremerger resides on the FTC's Infrastructure GSS for which a Certification and Accreditation (C&A) has been performed.

### **6.3 Has a risk assessment been conducted on the system?**

A risk assessment was completed on the Infrastructure GSS as part of the C&A.

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

The system is used to submit forms that may contain sensitive information, but precautions have been taken to ensure the security of the forms during transmission through the use of HTTPS/SSL encryption.

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

Filers do not have access to the system other than to transmit a form. Once a form has been transmitted, a filer cannot access the form again.

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

All FTC staff receive privacy training on an annual basis. Staff in the FTC's Premerger Notification Office will receive specific training on the use of the ePremerger system.



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

Only authorized Premerger Notification Office staff and reviewing officials located at the FTC and DOJ can access form data. Access is allowed via authorized user ID and passwords must meet criteria established in the FTC password policy. The database and application servers are hardened per National Institute of Standards and Technology (NIST) guidance.

**6.8 Questions regarding the security of the system?**

The FTC's Information Assurance Manager shall be the point of contact for any security questions relating to this system.

**7 Data Retention**

This section addresses for how long data is maintained, and how and when it is disposed of.

**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 (NARA).

Information incorporated into FTC records is maintained in accordance with applicable schedules and procedures issued or approved by the National Archives and Records Administration (NARA).<sup>1</sup>

Information collected for the purpose of monitoring ePremerger usage, including access, system event, and device usage logs, is to be deleted or destroyed when the FTC determines it is no longer needed for audit purposes. The FTC has submitted to NARA a comprehensive records disposition schedule, SF-115 Request for Disposition Authority. Pending NARA approval, FTC will manage usage information in a manner consistent with 44 U.S.C. Ch. 31, 44 U.S.C. 3506, 36 C.F.R. 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?**

All forms submitted will be deleted/destroyed in accordance with OMB, NARA and NIST regulations and guidelines.

---

<sup>1</sup> For information about retention and disposal of this information, see SORN I-1, Nonpublic Investigational and Other Legal Records (<http://www.ftc.gov/foia/sysnot/i-1.pdf>).

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

Regarding privacy risks identified in data retention, see Section 2.8. No privacy risks have been identified in the disposal of the data.

**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?**

This information is also not routinely maintained or retrieved by the names of any individual who may be identified in filings but, rather, only by names or other data pertaining to corporate filing parties, whom the Privacy Act does not protect. Any information identifying specific individuals would ordinarily pertain to them in their business, rather than their individual, capacity, and would not be protected by the Privacy Act. Nonetheless, to the extent that the forms may collect SSNs or other information that may be retrieved and would pertain to individuals in any personal capacity for payment processing, debt collection, or reporting purposes, such information may, in such cases, be subject to the Privacy Act of 1974.

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

Forms received through the system are covered by FTC I-1.  
<http://www.ftc.gov/foia/sysnot/i-1.pdf>

**9 Privacy Policy**

This section confirms that the information handling practices of the system are consistent with the FTC's 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 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](http://www.ftc.gov).

**10 Approval and Signature Page**

Prepared for the Business Owners of the System by:

\_\_\_\_\_ Date: \_\_\_\_\_  
Holly R. Frost  
Deputy Assistant Director, Technology and Information Management  
Bureau of Competition

Review:

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

\_\_\_\_\_ Date: \_\_\_\_\_  
Marc Groman  
Chief Privacy Officer

\_\_\_\_\_ Date: \_\_\_\_\_  
Margaret Mech  
Chief Information Security Officer

\_\_\_\_\_ Date: \_\_\_\_\_  
Jeffrey Nakrin  
Director, Records and Filings Office

Approved:

\_\_\_\_\_ Date: \_\_\_\_\_  
Jeffrey Huskey  
Chief Information Officer

