
Federal Trade Commission
Privacy Impact Assessment

# Matter Management System 2 (MMS2)

**October 2019**

# Table of Contents

# 1 System Overview

## 1.1 Describe the project/system and its purpose.

The MMS2 is an electronic database system that the FTC uses to record, track, and report administrative and statistical information about FTC matters. Matters include investigations, litigation, rulemakings, studies, workshops, and other FTC law enforcement and regulatory projects. MMS2 allows Agency staff to monitor and share information regarding the conduct and progress of Agency matters. The system also allows staff to research FTC matters, both current and historic, and provides a historical record of actions and deliberations as they occur. Agency staff use information from MMS2 to develop and record plans for conducting matters and to identify the personnel resources used to conduct each matter.

The data in MMS2 about each matter varies slightly, depending on the nature of the particular matter being tracked and reported by the system. For example, for FTC investigations, the system database includes the matter name or title, alleged violations investigated, cross-references to related matters, and dates and descriptions of specific events or Agency actions that have occurred in the case or project (e.g., preliminary or full investigation opened, court complaint filed, decision appealed, case settled, etc.). For a rulemaking, the system database includes the title or subject matter of the rulemaking, relevant industry, project, or subject matter codes, and dates and descriptions or key events or Agency actions in the rulemaking proceeding (e.g., publication of notice of proposed rulemaking, closing of the public comment period, publication of final rulemaking notice). Each matter tracked by the system is designated with a unique matter number that is used for tracking and reference purposes.

The system database also contains certain information "in identifiable form" under the definition set forth in Office of Management & Budget (OMB) guidance (OMB Memorandum 03-22) implementing the PIA requirements of E-Gov. Specifically, for each agency matter, the system database contains the names, addresses, and certain other information on persons and organizations within and outside the FTC associated with that matter (e.g., FTC attorneys, economists, or other staff assigned to work on the matter, as well as defendants, opposing counsel, intervening parties, etc., who may be involved in the matter). The system does not maintain any content such as legal filings, correspondence, consumer complaints, or others documents compiled or generated in an Agency matter, but only records and tracks key historical, procedural, and statistical details about the conduct and progress of such matters. Metadata (username and organization) from public comments are also included in MMS2.

## 1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

The FTC Act and other laws enforced or administered by the FTC authorize the FTC to conduct investigations, perform rulemakings (including collecting and retaining public commentary), and carry out special projects (e.g., studies, workshops). The system allows staff and managers to research both current and historical matters, to develop and record plans for conducting the matters, to identify the personnel resources used to conduct those matters, and to provide a historical record of actions and deliberations as they occur. Contact information of respondents and counsel matters is collected for the purpose of serving these individuals with documents.

## 2 Data Type, Sources, and Use

**2.1 Specify in the table below what types of personally identifiable information (PII)[1] may be collected or maintained in the system/project. Check all that apply.**

| ***PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.*** | | |
|---|---|---|
| ☒ Full Name | ☐ Biometric Identifiers (e.g., fingerprint, voiceprint) | ☐ User ID |
| ☐ Date of Birth | ☐ Audio Recordings | ☐ Internet Cookie Containing PII |
| ☒ Home Address | ☐ Photographic Identifiers (e.g., image, x-ray, video) | ☒ Employment Status, History, or Information |
| ☒ Phone Number(s) | ☐ Certificates (e.g., birth, death, marriage, etc.) | ☐ Employee Identification Number (EIN) |
| ☐ Place of Birth | ☐ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.) | ☐ Salary |
| ☐ Age | ☐ Vehicle Identifiers (e.g., license plates) | ☐ Military Status/Records/ ID Number |
| ☐ Race/ethnicity | ☐ Financial Information (e.g., account number, PINs, passwords, credit report, etc.) | ☐ IP/MAC Address |
| ☐ Alias | ☐ Geolocation Information | ☒ Investigation Report or Database |
| ☐ Sex | ☐ Passport Number | ☐ Driver's License/State ID Number (or foreign country equivalent) |
| ☐ Email Address | | ☒ Other *(Please Specify)*:Organization name |
| ☒ Work Address | | |
| ☐ Taxpayer ID | | |
| ☐ Credit Card Number | | |
| ☒ Facsimile Number | | |
| ☐ Medical Information | | |
| ☐ Education Records | | |
| ☐ Social Security Number | | |
| ☐ Mother's Maiden Name | | |

For each Agency matter, the system collects some or all of the information in the chart above on non-FTC parties (e.g., persons who submit public comments, defendants, opposing counsel, intervening parties, etc.), if any, who are involved in or associated with the particular matter (e.g., subjects of investigations, witnesses, experts, respondents, defendants, outside counsel).

As noted in Section 1.1, MMS2 collects information in identifiable form about individuals who are or have been associated with FTC investigations, rulemakings, and special projects, such as workshops or studies. This information relates to FTC staff and to certain non-FTC parties.

Regarding individuals who submit public comments to the FTC, MMS2 retains only the names of these individuals and the company or association that they are connected to.

Regarding witnesses or experts or any other individuals who may be involved in FTC matters, MMS2 does not retain any information other than the name of the individual in event descriptions concerning witnesses or experts involved in FTC matters.

Data in the system about FTC staff (e.g., attorneys, economists, administrative law judges, other FTC officials or managers) involved in or associated with a particular matter include their names, titles, employee numbers, and FTC organizational codes.

[1] Per OMB Circular A-130, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

The system is not designed to, nor does it contain, Social Security or tax identification numbers, bank account numbers, driver's license numbers, passport numbers, other government identification numbers, or other more sensitive personal information about individuals within or outside of the FTC.

The system does not maintain any content such as public comments (except for name and organization of comment submitter), legal filings, correspondence, or other documents compiled or generated in an Agency matter, but only records and tracks key historical and statistical details about the conduct and progress of such matters.

**2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.**

As described more fully in Section 1.1, MMS2 contains other information necessary for tracking the progress of investigations and rulemakings, such as matter name and matter number.

**2.3 What is the purpose for collection of the information listed above?**

The system allows staff and managers to research both current and historical matters, to develop and record plans for conducting the matters, to identify the personnel resources used to conduct those matters, and to provide a historical record of actions and deliberations as they occur. Contact information of respondents and counsel matters is collected for the purpose of serving these individuals with documents.

Information in identifiable form about individuals inside and outside the FTC is used with other historical and statistical data in the system. This allows the progress of each matter to be tracked, reported, and analyzed. (e.g., matter profiles) along with analyses for use by Agency staff. The system provides a mechanism for staff to research current and historical matters, to develop and record plans for conducting matters, to identify the personnel resources used to conduct matters, and to provide a historical record of actions and deliberations as they occur.

Monthly and quarterly management reports containing information stored in MMS2 are distributed to managers throughout the Commission and are used to review past accomplishments, to plan future activities, and to help determine and evaluate employee workloads and performance on either an individual or aggregate basis. Daily reports are utilized by the Commissioners' offices in order to plan Agency activities and manage resources. In addition to those regularly distributed reports, MMS2 information is available through a variety of standard reports that each user can produce using Business Objects software.

**2.4 What are the sources of the information in the system/project? How is the information collected?**

| *Source of Data* | *Type of Data Provided & How It Is Collected* |
|---|---|
| Individuals who submit public comments to the FTC | Public comments are no longer uploaded to MMS2. However, MMS2 contains historical comments that contain Submitters name and organization. |
| Witnesses, experts, or any other individuals involved in FTC matters | This information is collected by other organization within FTC and passed to the RIM office. |

# 3 Data Access and Sharing

**3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.**

| *Data Will Be Accessed By and/or Provided To:* | *How and Why the Data Will Be Accessed/Shared* |
|---|---|
| FTC staff and contractors | The information primarily is used and disclosed within the FTC by Agency staff for internal administrative and reporting purposes.<br><br>Access to MMS2 is provided on a need-to-know basis to FTC staff using a role-based system. Different types of access are granted to different staff members and contractors:<br><br>• Read-Only access is granted to FTC staff and contractors located in the Records and Information Management Office and the Office of the Secretary to assist in investigatory, rulemaking, or other agency activities on a need-to-know basis. Access is approved by their Administrative Officer and the MMS2 Program Manager.<br><br>• Data-Entry access is granted to FTC staff and to contractors located in the Records and Information Management Office and the Office of the Secretary who require such access to carry out their official duties, including assisting in investigatory, rulemaking, or other Agency activities. Access is approved by their Administrative Officer and the MMS2 Program Manager.<br><br>• Administrative access is granted to FTC staff only on a need-to-know basis. Access is approved by the MMS2 Program Manager. |

| | |
|---|---|
| | All staff involved with maintaining and/or having access to the system are expected to adhere to written FTC policies regarding the nature and sensitivity of the information contained on the system pursuant to the non-disclosure agreement signed as a condition of employment. |
| Members of the public and other law enforcement agencies (via FOIA/Privacy Act procedures) | In accordance with the Privacy Act of 1974 (Privacy Act), system records also can be routinely used (disclosed) outside the FTC for certain authorized purposes (e.g., interagency law enforcement sharing). |

**3.2 Do contractors and/or third party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.**

Yes, onsite contractors have access to MMS2. Access to MMS2 is controlled using the least-privilege principle to assign read-only, data entry, and administration access as appropriate to the users' roles. All contractors are required to sign non-disclosure agreements (NDA) as part of the onboarding process.

☐ Not Applicable.

**3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third party service provider.**

☒ Not Applicable.

## 4 Notice and Consent

**4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.**

☒ Notice is provided via (*check all that apply*):
- ☐ Privacy Act Statement (☐ Written ☐ Oral)
- ☒ FTC Website Privacy Policy
- ☐ Privacy Notice (e.g., on Social Media platforms)
- ☐ Login banner
- ☐ Other (*explain*):_____

☐ Notice is not provided (explain): _____

### 4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

Since MMS2 does not directly collect information from individuals, the opportunity for individuals to decline to provide information to the FTC or to consent to particular uses of their information depends on the manner in which the FTC collects information from such individuals. For example, in a rulemaking or similar Agency proceeding where participation is purely voluntary, individuals decide whether to submit a public comment or otherwise provide or disclose personally identifiable information, which the Agency may then incorporate into the MMS2 system. By choosing to participate, individuals are consenting to the Agency's collection, maintenance, and use of the information they have submitted. This is described in the privacy policy posted on the FTC's website[2], notices published or provided under the Privacy Act, which the individual had the opportunity to review before submitting or disclosing their information to the FTC.

In contrast, when the Agency collects information about individuals in investigations or litigation for law enforcement purposes, whether from individuals directly or from other parties, these individuals may not have an opportunity to decline to provide the information. These individuals will not ordinarily have an opportunity to consent to the Agency's use of the information, which is determined by the FTC Act, the Privacy Act, as applicable, and other laws, regulations and policies governing the collection, maintenance, use, and disclosure of such information in the context of the law enforcement matter.

PIAs are not intended or legally required to address the collection or maintenance of identifiable information about the FTC employees or contractors in the system, which is considered a purely internal matter not affecting the public. MMS2 includes limited information about FTC employees or contractors (including names, titles, employee number, and FTC organizational codes), which would not normally be addressed in a PIA under E-Gov. Nonetheless, this document notes that an opportunity for such FTC individuals to decline to provide such information or to consent to particular uses would be inapplicable, since data in the system about such individuals are collected and pertain to their official duties and performance on behalf of the FTC, and are not about these individuals in their personal, private capacity.

### 4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

An individual may make a request under the Privacy Act for access to information maintained by the FTC about themselves in MMS2. The FTC's Privacy Policy provides links to the FTC's SORNs, as well as information about making Freedom of Information Act (FOIA) requests and the online FOIA request form. Individuals must follow the FTC's Privacy Act rules and procedures, published in the Code of Federal Regulations (C.F.R.) at 16 C.F.R. 4.13. Access to information under the Privacy Act is subject to certain exemptions.

[2] https://www.ftc.gov/site-information/privacy-policy

**4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.**

The FTC's Privacy Policy provides links to the FTC's SORNs, which include information about how to correct or amend records. See also 4.3 above.

## 5 Data Accuracy and Security

**5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?**

The RIM office runs a monthly and weekly report to verify the data in MMS2. These reports provide information on data accuracy, completeness, and other system details.

**5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.**

MMS2 has technical controls in place to assure the system is protected against unauthorized use. These controls include user access permissions, form validation, server STIGS, and database triggers.

Some administrative procedures and technical safeguards apply specifically to MMS2:

> If a user wants access to MMS2, a form must be completed and signed by the user's manager. The RIM office also determines whether the user should have the access being requested.

Other administrative procedures and technical safeguards apply not only to MMS2, but to many other applications at the FTC, as well:

> MMS2 is an application within the FTC network. In general, the FTC network is only accessible via multi-factor authentication using government-furnished equipment.
>
> All FTC positions are assigned a risk designation that has associated criteria for personnel screening. All potential FTC employees, contractors, and volunteers are subject to background investigations and suitability reviews in accordance with OPM guidance. Before any new employee, contractor, or volunteer can access FTC applications, that individual must first attend new employee orientation and successfully complete the 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. Categories of employees deemed to be higher

risk – such as interns and International Fellows – may have restricted access to network and physical space.

Supervisors and/or Contracting Officer's Representatives (CORs) must identify and approve employee requests to access network applications and specify the appropriate user role and level of access privileges. Auditing measures and technical safeguards are in place commensurate with the Moderate-Impact Baseline of the National Institute of Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems and Organizations Special Publication (SP) 800-53.

FTC staff is responsible for minimizing PII and disposing of it when the PII is no longer needed and in accordance with appropriate records disposition schedules. The FTC ensures that all staff and contractors annually electronically certify their acceptance of FTC privacy responsibilities and procedures by requiring comprehensive Information Security and Privacy Awareness training. Moreover, all staff must annually acknowledge procedures for handling PII – including minimizing PII – and attest that all PII maintained by the individual has been properly secured and accounted for as part of the FTC's annual privacy and security training.

**5.3 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?**

☒ Not Applicable

## 6 Data Retention and Disposal

**6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?**

MMS2 serves as the indexing tool to Documentum, the FTC case management system. The electronic data in the system is covered by the FTC NARA-approved records disposition schedule N1-122-09-1. However, along with the corresponding case data in Documentum, the MMS2 data is retained by the agency until no longer needed for agency business.

## 7 Website Privacy Evaluation

**7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.**

☒ Not Applicable

# 8 Privacy Risks and Evaluation

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

| *Risk* | *Mitigation Strategy* |
|---|---|
| Unnecessary collection of sensitive information | The system collects a limited amount of information in identifiable form about individuals involved in or associated with Agency matters. This information is sufficient for administrative matter tracking and reporting purposes. MMS2 does not incorporate sensitive information (e.g., Social Security or financial account numbers) that the FTC may collect and maintain in other Agency systems or files (e.g., investigational or case records compiled or generated by FTC attorneys with a need to maintain and use such information for law enforcement purposes). Thus, the omission of such sensitive information greatly minimizes the risk of financial or other harm, embarrassment, or loss in the event of any unauthorized access to the system. |
| Unauthorized access to MMS2 | The FTC also does not make user access to the application available to anyone other than authorized FTC employees and contractors on a need-to-know basis. The system is not accessible to outside parties (e.g., other law enforcement agencies). The Agency has appropriate rules and procedures in place for reviewing and determining when, and under what circumstances, the affirmative sharing or disclosure of such data outside the FTC may be authorized or required by law. For example see Commission Rule 4.11, 16 C.F.R. 4.11 (access to nonpublic records).<br><br>See also the safeguards discussed in Section 5.2 above. |

**8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.**

See the information on technical safeguards in 5.2 above.

**8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).**

Because the system allows users to retrieve information about an individual's involvement or association with an Agency matter from MMS2 by name or other personal identifier, the FTC treats MMS2 as a system of records subject to the Privacy Act of 1974, 5 U.S.C. 552a. The system is covered by an existing Privacy Act system of records notice. See https://www.ftc.gov/site-information/privacy-policy/privacy-act-systems (FTC-I-5). It should be noted that, due to the law enforcement nature of the system, records in the system about certain individuals (e.g., defendants) are exempt from mandatory access by such individuals. See 4 U.S.C. 4.13(m) (exemptions applicable to certain FTC Privacy Act system of records). The Privacy Act or other legal authorities may permit or require the disclosure of such records in certain cases.

**8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?**

The Privacy Office routinely collaborates with system/application owners as part of its Privacy Continuous Monitoring Strategy to ensure that the information in PIAs, including this one, is accurate and to mitigate any privacy risks, as needed. Members of the public with questions or comments on the FTC's privacy practices may contact the Chief Privacy Officer using the contact information at ftc.gov/privacy.