MAY 24, 2012

Privacy Impact Assessment

Matters management system

Consumer Financial Protection Bureau

Contact Point:
Claire Stapleton
Chief Privacy Officer
1700 G Street, NW
Washington, DC 20552
202-435-7220
claire.stapleton@cfpb.gov

DOCUMENT PURPOSE

The Privacy Impact Assessment or "PIA" provides the public with information about the Consumer Financial Protection Bureau's ("CFPB" or "Bureau") collection and use of personally identifiable information ("PII"). PII is any information "that can be used to distinguish or trace an individual's identity"[1] like a name, address, Social Security number, or place and date of birth. The CFPB uses PIAs to document that the PII it collects is used, secured, and destroyed in a way that protects each individual's privacy. Each PIA is broken out into sections that reflect the CFPB's Privacy Principles. The CFPB's Privacy Principles are a set of nine rules the CFPB follows when it collects or uses PII.

OVERVIEW

PROJECT / SYSTEM NAME: Matters Management System

PROJECT/SYSTEM INCLUDES INFORMATION ABOUT:

- ☒ Federal Employees
- ☐ Contractors
- ☐ Consultants
- ☒ The Public

PROJECT/SYSTEM INCLUDES:

- ☒ Name and other biographic information (e.g. date of birth)
- ☒ Contact Information (address, zip code, telephone number, email address)
- ☐ Social Security number (SSN) or other identifier
- ☐ Financial Information
- ☐ User and Online Information
- ☒ Third Party Information
- ☐ Other Information (including biometric information and health or medical information)

The Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Act"), Public Law No. 111-203, Title X, established the CFPB. The CFPB administers, enforces, and implements federal consumer financial protection laws and, among other powers, has authority to protect consumers from unfair, deceptive, and abusive practices when obtaining consumer financial products or services.

In carrying out its responsibilities, the CFPB will be involved in numerous legal and regulatory issues (collectively referred to as "matters") including:

- Investigations

[1] Office of Management and Budget (OMB) Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007, (OMB M-07-16) defines PII as information which can be used to distinguish or trace an individual's identity, such as his or her name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

- Enforcement actions
- Supervision and related regulatory actions
- Litigation
- Rulemakings
- Other related law enforcement and regulatory projects

To effectively manage its matters, and the associated activities of each, the CFPB has developed the Matters Management System (the "MMS"). The MMS allows the Bureau to:

- Create a central searchable repository of information relating each matter;
- Organize and distribute information about each matter to those with a *bona-fide* need to know, including the progression of each matter;
- Track deadlines for each matter, including synchronization with an employee's electronic calendar;
- Report on administrative and statistical information about each matter, such as which CFPB employees are associated with each matter, the type of matter, etc.; and
- Develop and record plans for conducting matters, including identifying personnel resources necessary to conduct each matter.

The system only records and tracks key historical, procedural, and statistical details (as outlined above) about the conduct and progress of matters. The MMS is not a document management system – the system provides links to, but does not itself maintain copies of any of the files, documents or other content related to a particular matter, such as public comments, legal filings, correspondence, consumer complaints, whistleblower complaints and tips, or other documents compiled or generated in a matter.

The information in the MMS about each matter varies slightly, depending on the nature of the particular matter being tracked and reported by the system. A general list of data fields included in the system is provided below in Section 3. Each matter tracked by the system is designated with a unique matter number created by the system.

The CFPB will roll-out the MMS in a series of phases, including a pilot phase, with full deployment anticipated by the end of 2012. Users will be allowed to use the system for case management while simultaneously providing feedback to the LawBase vendor for customization and other needs in the full deployment phase. As part of the roll-out, users will conduct continuous testing of the system. The CFPB will update this PIA accordingly if substantial changes impacting the privacy of individuals are made as the result of user feedback during the roll-out.

The CFPB has also published two System of Records Notices ("SORNs") which give notice of the information maintained and processed in the MMS: CFPB.004 – Enforcement Database and CFPB.018 – Litigation Files.

SECTION 1.0 Purpose of Collection

The CFPB will state the purpose and legal authority for collecting PII.

1.1 Why is the information being collected?

The CFPB collects and maintains PII in the MMS to record, track, and report administrative and statistical information about matters.

1.2 What legal authority and/or agreements allow the information to be collected?

Public Law 111-203, Title X, Sections 1011, 1012, 1021, and 1054 codified at 12 U.S.C. 5491, 5492, 5511, and 5564 provide authority for the collection of information in this system.

1.3 Is the information searchable by a personal identifier – like a name or Social Security number? If so, what Privacy Act System of Records Notice(s) apply/applies to the information being collected?

Yes. Information in the MMS is searchable by PII, including, but not limited to:

- Individual name(s)
- Address or location information (e.g. zip code, city, state)
- Phone Numbers
- Filing, case, or matter number (including identifying numbers of formal actions)[2]

The MMS has a search capability that allows for retrieval by search term or by a string of search terms or by using a series of filters to search within specific fields.

In general, records within the MMS are organized by a matter name, generally related to an institution which is the subject of an investigation, a party in litigation, a project name, a rulemaking, or a whistleblower complainant. Most matters are retrieved by the matter name and not by individual PII.

The CFPB SORNs – CFPB.004 –Enforcement Database and CFPB.018 – Litigation Files – document the collection of information that populates this system.

[2] Records may also be retrieved by a combination of any of these fields. This list is not exhaustive.

1.4 Is there a records retention schedule that has been approved by the National Archives and Records Administration ("NARA") for the information system(s)? Explain how long and for what reason the information is retained.

The CFPB maintains computer and paper records indefinitely until NARA approves the CFPB's records disposition schedule. Records that fall under a general records schedule will be disposed of according to the applicable schedule.

1.5 Are there any forms or surveys that are associated with the collection of the information that would be covered by the Paperwork Reduction Act ("PRA")?

No. The MMS does not use a form subject to PRA requirements to collect information for the system.

1.6 Are there any privacy risks for this system that relate to the purpose of the collection? If so, how will the CFPB mitigate these risks?

There are no identifiable risks associated with the purpose of this system.

SECTION 2.0 Openness and Transparency

The CFPB will be open and transparent. We should tell individuals about the PII we collect and how we will protect it, use it, and share it. We will provide an easy way for individuals to learn about what is happening to their PII.

2.1 Will individuals be given notice prior to the collection of personal information about them? If not, please explain.

When the CFPB collects PII about individuals who are involved in CFPB matters, it may collect such information directly from those individuals or it may collect such information from an entity that is the subject of research, an investigation or an enforcement action, or from third parties, including existing federal databases and other agencies responsible for related regulatory functions. In these latter cases, individuals may not receive actual notice of information collection. However, this PIA and the associated SORNs, CFPB.004 –Enforcement Database and CFPB.018 – Litigation Files, provide constructive notice of the CFPB's information collection practices.

2.2 Will individuals be given notice prior to their information being shared? If not, please explain.

In most cases, the Bureau will not provide actual notice to individuals prior to sharing MMS information that pertains to them. However, the CFPB has provided constructive notice of how it will share information stored in the MMS in its SORNs, CFPB.004 – Enforcement Database, CFPB.018 – Litigation Files and through this PIA.

2.3 Are there any privacy risks for this system that relate to openness, and transparency? If so, how will the CFPB mitigate these risks?

No. There are no identifiable risks related to openness and transparency for this system.

SECTION 3.0 Data Minimization

The CFPB will limit the collection of PII to what is needed to accomplish the stated purpose for its collection. The CFPB should keep PII only as long as needed to fulfill that purpose.

3.1 Whose information is included in the system?

The MMS contains PII about those individuals who are or have been associated with CFPB investigations, enforcement actions, litigation in which the Bureau is or has been involved, related supervisory activities, rulemakings, and special projects.

This may include:

- CFPB staff such as, but not limited to:
  - Attorneys
  - Administrative law judges
  - Officials
  - Managers
  - Paralegals

- Non-CFPB individuals such as, but not limited to:
  - Defendants
  - Opposing counsel
  - Intervening parties
  - Consumers whose complaints are included as part of an investigation
  - Whistleblowers
  - Individuals who comment on rulemakings
  - Federal and state employees related to a CFPB matter

More information about the categories of individuals included in this system is available in the associated SORNs for the system.

3.2 What PII will the system include?

For each Bureau matter, the system collects some or all of the following information about non-CFPB parties who are involved in or associated with the particular matter:

- First and last name
- Title
- Organization, company or affiliation name

- Contact information (business or personal), including mailing address, phone number, fax number and email address

Additionally, for each Bureau matter, the system may collect information about CFPB employees (e.g. attorneys, administrative law judges, officials, managers, etc.) involved in or associated with a particular matter including:

- First and last name
- Title
- Information about an individual's relationship to a case, including scheduling, role, etc.

Source documents related to a matter are not stored in the MMS. However, cases within the system may be directly linked to a shared document repository for referential materials. Thus, the system does not contain large amounts of PII and very little, if any, sensitive PII.

3.3 Why is the collection and use of the PII necessary to the project or system?

Various laws and regulations require or permit the Bureau to conduct investigations, take enforcement actions, represent itself in litigation, perform rulemakings (including collecting and retaining public commentary), and carry out special projects. 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.

3.4 Will the system aggregate previously unavailable data about the individual or create new data about the individual? If so, how will this data be maintained and used?

The system does not aggregate data nor create new data about individuals.

3.5 What controls exist to protect the consolidated data and prevent unauthorized access?

The system does not consolidate or aggregate any data, nor create new data about individuals.

3.6 Will the system monitor the public?

The system does not monitor the public.

3.7 Will the system monitor CFPB employees or contractors?

The system will audit CFPB employees or contractors with regards to their actions (i.e. uploading information, modifying or deleting information) in the system, and in relation to their workflow associated with a particular matter. For example, the MMS has a function which allows individuals to schedule meetings and other events associated with a matter and tie that directly to the individual CFPB employee assigned to that particular matter. The system can

also produce reports about time spent by an employee on a particular matter or set of issues or matters.

3.8 What kinds of reports can be produced on individuals? Will the data included in the reports produced be made anonymous?

The CFPB may generate reports from the MMS that identify matters related to specific CFPB staff, the subject of the matter, or the matter type. Such reports include lists of names and contact information of individuals involved in a matter and CFPB employees. In addition, such reports may include sensitive non-identifying information about the status of a matter.

The Bureau distributes reports derived from MMS internally only to employees with a *bona fide* need for such reports to carry out their assigned job responsibilities.

Externally, the Bureau discloses reports on a limited basis, as required or necessary, to other state and federal government agency employees whose job functions allow them to review reports generated about a CFPB matter. Section 4.2 of this PIA and the related SORNs, outline the ways the CFPB may share information from this system with other federal and state agencies.

3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will the CFPB mitigate these risks?

There are no identifiable risks associated with data minimization for this system.

SECTION 4.0 Limits on Uses and Sharing of Information

The CFPB will publish a notice about how we plan to use and share the PII that we collect from you. We will only share your PII in ways that are compatible with the notice or as stated in the Privacy Act.

4.1 Is the information in the project limited to only the information that is needed to carry out the purpose of the collection?

Yes, information included in the MMS is limited to that which is necessary for:

- Managing and maintaining a record of current and historical matters;
- Developing and recording plans for working on various matters;
- Identifying the personnel resources used to work on those matters; and
- Providing a historical record of actions and deliberations as they occur.

4.2 Will the CFPB share any of the information with other individuals, Federal and/or state agencies, or private sector organizations? If so, how will the CFPB share the information?

While the MMS will not directly connect to or share information with systems outside of the CFPB, reports generated by the system about matters may be shared with other individuals within the CFPB and at other federal and state agencies, as well as non-CFPB individuals associated with a particular matter, if such sharing is warranted. Such sharing will only occur through secure channels, such as encrypted email.

The CFPB has outlined the ways in which information from the MMS may be shared under the "Routine Uses" section of the related SORNs, CFPB.004 – Enforcement Database and CFPB.018 – Litigation Files.

4.3 Is the information collected directly from the individual or is it taken from another source?

As discussed in Section 2.1, the CFPB collects data for the MMS from various sources, including individuals included in the system. However, most of the data is collected from entities that are the subject of a matter or from other third parties like state and federal agencies.

4.4 Will the project interact with other systems, whether within the CFPB or outside of the CFPB? If so, how?

As discussed in section 4.2, the MMS will not connect to or interact with other systems outside of the CFPB. Within the CFPB, the system will connect to the Bureau's shared network drive in order to access documents and other files associated with a particular matter. This connection exists because the MMS does not serve as a document repository or document management system for documents associated with matters in the system. The system will also connect to the Bureau's email server for the purposes of calendar and email synchronization, and to the Bureau's Staff Directory for managing CFPB staff contact information.

4.5 Are there any privacy risks for this project that relate to use limitation? If so, how will the CFPB mitigate these risks?

There are no risks associated with use limitation for this system.

SECTION 5.0 Data Quality and Integrity

The CFPB will make reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

5.1 How will the information collected be verified for accuracy and completeness?

Information collected in the system is verified for accuracy and completeness only to the extent necessary for accurately recording, tracking and reporting administrative and statistical information about CFPB matters. This includes confirming the name of internal and external individuals associated with each matter, confirming dates associated with each matter, and confirming actions associated with each matter. Supplemental information about each matter contained in source and supporting documentation is not verified for accuracy within this system as the system does not store these documents or the PII contained within them.

5.2 Are there any privacy risks for individuals whose information is collected or used by the project that relate to data quality and integrity? If so, how will the CFPB mitigate these risks?

There are no identifiable risks associated with data quality and integrity for this system.

SECTION 6.0 Security

The CFPB must protect PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

6.1 Who will have access to the data in the project? What is the authorization process for access to the project?

For general users of the system, the Bureau restricts access to the MMS to employees who have a *bona fide* need for such access to carry out their assigned job responsibilities – mainly Enforcement and General Counsel attorneys, their supervisors and assistants working on matters in the MMS. Limited members of the Office of Fair Lending and Supervision teams are also granted access with regards to matters which they are involved in. Access is driven by role-based permissions relevant to an employee's association with a matter and position within the CFPB, with users receiving the least minimum privilege needed. The system limits the ability of individual staff not assigned to a particular matter to see detailed information about that matter. Individuals granted access to a particular matter may also have permission to write to that particular matter.

Access is granted through a user request form and governed by policy and procedures for determining what, if any, level of access should be granted to an individual user. Users are required to complete mandatory privacy and security training (Bureau-wide) and additional training on use of the MMS before being granted access to the system. Users must also complete the user agreement outlining their roles and responsibilities in using the system and the information contained within it.

MMS is an application based on the LawBase Commercial Off-the-Shelf Product, is a client-based executable application, and is hosted in the Terremark environment. The MMS's placement within the Terremark environment provides an additional level of security. The CFPB grants access only to authorized personnel who have been issued non-transferrable

access codes and passwords, which are verified at login to the Bureau's Terremark hosted General Support System ("GSS"). The MMS application is installed locally only on the machines of individuals granted permission to the system and accounts are authenticated through Active Directory (AD) and managed by a system administrator.

Given that CFPB has a limited number of licenses, system administrators will control which users have a need to have the executable program installed on their workstations. This layer of control, in addition to credential authentication through AD, will limit the number of individuals that have access to the application.

System administrators are considered privileged users and as such will have access to all data in the system, including PII, for the purposes of controlling, monitoring, and other administrative functions.

6.2 Has the CFPB completed a system security plan for the information system(s) supporting the project?

The CFPB has completed a system security plan for the Terremark hosted GSS, which the MMS resides on. The system was issued an Authority to Operate ("ATO") at the Moderate level by CFPB. The ATO was signed on September 30, 2011. MMS has undergone a security review including a review of documentation provided by the vendor, and interviews with technical representatives.

6.3 How will the system be secured?

The CFPB issues authorized personnel non-transferrable access codes and passwords to approved users of the system. Users are required to complete training and complete the user agreement before being granted access to the system. MMS is a client-based executable application that needs to be installed on a user's workstation prior to gaining access to the system, and licenses are limited. The system stores login/authentication credentials but encrypts them. Section 6.1 has more information about how users are granted access to the system.

The MMS system inherits many security controls from the underlying GSS it resides on. A detailed security assessment was performed on the MMS in line with applicable federal mandates. Additionally, as part of the phased roll-out of the system, users will engage in testing of the system's functions, including user access controls.

6.4 Are there mechanisms in place to identify security breaches? If so, what are they?

The CFPB relies on the Treasury Department's directives related to security and privacy incidents. The CFPB is developing supplemental interim incident-reporting materials, and, upon moving onto its own network infrastructure, will issue new directives related to security and privacy incidents.

6.5 Are there any privacy risks for this system that relate to security? If so, how will the CFPB mitigate these risks?

There is a risk that unauthorized individuals may gain access to the information in the MMS. The CFPB has mitigated this risk by only granting access to the system to authorized users who, based on their need to know, will be restricted to the minimal amount of data required or appropriate to carry out their assigned job responsibilities. Access is terminated or reduced as necessary should the user no longer have a need to know the information, change job functions, is terminated or resigns.

Additionally, there is a risk that changes to data in the system may not be able to be audited at the individual user level. LawBase, the commercially available off-the-shelf product being used for the MMS provides auditing functionality at the system level, meaning that when changes are made to the data housed in the database on which the MMS is built (and which houses the data in the system), the database only tracks that a user made such changes, but does not account for which user made the change. The CFPB has mitigated this risk by limiting access to the system through the access controls outlined above and in Section 6.1 and 6.3.

Additionally, as stated earlier, the MMS does not serve as a document repository for the referential documents and other files about a matter (such as an investigation). Rather, these files, which may contain large amounts of PII and sensitive PII, are stored on the shared drive, rather than in the MMS. Changes to these documents and associated files can be audited independently of changes to data in the MMS.

SECTION 7.0 Individual Participation

The CFPB will give individuals, in most cases, the ability to access their PII, and allow them to correct or amend their PII if it is inaccurate.

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

In general, individuals do not have opportunities to opt out or decline to provide information to the MMS. Most of the data collected by the MMS related to employees or customers of companies which are the subject of a matter is provided by a company pursuant to applicable laws and regulations rather than directly from customers or employees. Additionally, data collected about CFPB employees is related to their access and use of the system and is collected through use of the system.

Other data, such as the data related to regulations or whistleblower complaints is collected directly from individuals who may choose to limit the amount of data they provide to the CFPB.

7.2 What procedures will allow individuals to access their information?

The CFPB offers a means through the Privacy Act for individuals to access, amend, or correct, their records at their request. Information about Privacy Act requests is available in the

associated SORNs for the system, and at www.consumerfinance.gov/foia. It is important to note that some information in the MMS may not be able to be accessed or changed if doing so would impact the CFPB's ability to enforce consumer financial law or if doing so would harm a pending investigation, enforcement action or similar matter in the system.

7.3 Can individuals amend information about themselves in the system? If so, how?

The CFPB provides a means through the Privacy Act of amending or correcting your information in the MMS, which is described above in Section 7.2.

7.4 Are there any privacy risks for this system that relate to individual participation? If so, how will the CFPB mitigate these risks?

There are no risks associated with individual participation for this system.

SECTION 8.0 Awareness and Training

The CFPB will train all personnel about the proper treatment of PII.

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

The CFPB offers privacy and security training to all employees of the CFPB, including contractors who handle PII on behalf of the CFPB.

Additionally, those with access to the MMS receive training for use of the system before they are granted access. Users are also required to sign a user agreement outlining their roles and responsibilities related to accessing the system and the information contained within.

8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will the CFPB mitigate these risks?

There are no risks associated with awareness and training for this system.

SECTION 9.0 Accountability and Auditing

The CFPB is accountable for complying with these principles. We will regularly check that we are meeting the requirements and take appropriate action if we are not doing so.

9.1 How does the system ensure that the information is used in accordance with the stated practices in this PIA?

The CFPB has limited access to the MMS to those Bureau employees with a clearly defined business need to know the information and has employed role-based access controls in the system. The CFPB provides all employees with appropriate privacy and security training to ensure information is used and secured appropriately. Employees granted access to the MMS

area provided additional training on proper use of the system and must sign a user agreement outlining their roles and responsibilities related to the accessing and using the system and the information within. The MMS does not connect to other information systems outside or inside of the CFPB, with the exception of connections to the Bureau's email client for calendaring and emailing functions, and to the Bureau's shared network drive, which serves as a document repository for the system. The system is limited in its capability to collect PII as fields are generally limited to non-identifying information about the progress (historical or current) or management of a matter of the Bureau. Supporting or source documents associated with a matter that contain PII are not stored within the system.

9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will the CFPB mitigate these risks?

There are no identifiable risks for the MMS related to accountability and auditing.