



Privacy Impact Assessment
for the

Mapping Information Platform (MIP)

October 1, 2010

Contact Point

Mary Jo Mullen

FEMA

202-646-3227

Reviewing Official

Mary Ellen Callahan

Chief Privacy Officer

Department of Homeland Security

(703) 235-0780



Abstract

The Mapping Information Platform (MIP) is provided to support the National Flood Insurance Program (NFIP). This project provides an online method to reference and update the maps which define flood planes throughout the US and its territories. The collection of data which is used to support this effort causes the data in this application's repository to contain information about the names and addresses of mapping professionals which constitutes PII.

Overview

The National Flood Insurance Act of 1968, Public Law 90-448, as amended by the Flood Disaster Protection Act of 1973, Public Law 93-234, established that the NFIP will provide flood insurance in communities that voluntarily adopt and enforce floodplain management ordinances that meet minimum NFIP requirements. As part of the NFIP, FEMA assists communities by producing flood maps that indicate, among other things, which properties are located in Special Flood Hazard Areas (SFHA). This application maintains and administers the maps which define the statutory zones discussed above.

During the process of administering the flood maps it sometimes becomes necessary to amend those maps. The process for amending the maps requires that licensed professionals (Surveyors, engineers etc.) make changes to the maps after appropriate research and surveys have been performed to justify the amendment. To ensure that only proper changes to the maps are made, the application must collect information about the amending professional. This information, when taken in aggregate, is considered PII and must be protected. Records in the system are retained for 20 years after creation of the record in accordance with records schedule N1-311-86-1 2A2c.

The processes that collect PII are called the electronic Letter of Map Amendment (eLOMA) process, and the paper Amendments and Revisions Workflow. During the eLOMA process the certifying professionals provide data necessary to establish their competence to update flood maps. This is done by providing their licensed engineer certification number or their licensed surveyor certification number. This information when combined with their signature and their address is to be protected by the system. During the paper based amendments and revisions workflow simple ownership changes are not entered by certified professionals and hydrological/topological changes are only performed by licensed professionals. All paper based changes to the MIP are entered into the electronic system by FEMA employees/contractors. These changes all collect PII in the form of names and addresses. All PII is stored in a manner defined in the System Security Plan (SSP). The SSP is evaluated in a continuous process by staff personnel and at least every three years during recertification by external auditors.



Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The National Flood Insurance Act of 1968, Public Law 90-448, as amended by the Flood Disaster Protection Act of 1973, Public Law 93-234, established that the NFIP will provide flood insurance in communities that voluntarily adopt and enforce floodplain management ordinances that meet minimum NFIP requirements. As part of the NFIP, FEMA assists communities by producing flood maps that indicate, among other things, which properties are located in Special Flood Hazard Areas (SFHA). This application maintains and administers the maps which define the statutory zones discussed above.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

FEMA-2005-0042

1.3 Has a system security plan been completed for the information system(s) supporting the project?

A full authority to operate was granted on June 4, 2010 with a one-year lifetime.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes, the records retention policy in effect for the MIP is records schedule N1-311-86-1 2A2c.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

This application is not covered by the paperwork reduction act.



Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The DHS/FEMA – 002 NFIP Letter of Map Change System of Records contains personally identifiable information voluntarily provided by individuals or certifiers applying for NFIP MT-1 LOMCs, which include Letters of Map Amendment, Conditional Letters of Map Amendment, Letters of Map Revision based on Fill and Conditional Letters of Map Revision based on Fill, and MT-2 LOMCs, which include Letters of Map Revision and Conditional Letters of Map Revision.

An individual is any person financing or refinancing structures or parcels of land (hereinafter referred to as “property” or “properties”) with a federally-backed loan. Examples of individuals are homeowners, investors, and property developers.

A certifier is a Registered Professional Engineer or Licensed Land Surveyor who provides technical information, such as elevation, to FEMA. A certifier is a Registered Professional Engineer or Licensed Land Surveyor who provides technical information, such as elevation, to FEMA. A certifier may also be a community official with authority over a community’s flood plain management activities, who provides their concurrence for the issuance of a LOMC. The certifier may provide information either electronically or in hard copy on behalf of the individual.

The information collected includes the individual’s name, mailing address, signature, and signature date. The individual can voluntarily provide daytime telephone number, e-mail address, and fax number (which are not required) but enables FEMA to contact the individual should questions arise. In addition, the certifier is required to provide name, professional license number and expiration date (if applicable), company or community name (whichever is required), property address or legal description, e-mail address, and business telephone number. The certifier can voluntarily provide a fax number that enables FEMA to fax documents related to the NFIP MT-1 and/or MT-2 LOMC.

2.2 What are the sources of the information and how is the information collected for the project?

The source for the PII is the licensed professional that is completing the eLOMA online and for the paper based process, the general public will be providing PII.



2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No such data is used.

2.4 Discuss how accuracy of the data is ensured.

The individual that is providing the PII data confirms its accuracy. Errors can be addressed through the helpdesk if needed.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: The data elements that are collected are publicly available in all respects. Changes to the user record may affect the integrity of the public record.

Mitigation: All access to the record of the licensed professional is limited to administrators and the individual in question; changes are logged and can be removed at the certified request of the licensed professional.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

The information is used to correctly identify the licensed professional that is making changes to the NFIP reference maps. Only licensed professionals are allowed to modify the maps and this data serves to confirm the status of those that submit modifications to the NFIP maps.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No such use is contemplated for this data.

3.3 Are there other components with assigned roles and responsibilities within the system?

Other than FEMA and its contractors, no, there are no other components with assigned roles in the MIP system.



3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: PII for each user is stored within the system.

Mitigation: The annual awareness training for all administrative users includes a discussion about PII and the responsibilities that each admin user bears in protecting and using that data. End users are cautioned about appropriate use when the login banner is displayed for the system.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

A privacy act statement is posted through a web page during the registration process of a new licensed professional. The same privacy act statement is available from within the application at any time. For the paper based process the privacy act statement is included on the application forms.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

In order for a licensed professional to provide letters of map amendment to FEMA, they must register and provide PII to FEMA through the registration process. Failure to provide the required data will prevent the professional from gaining access to create LOMAs online. The process of registration is an opt-in process. Professionals that do not wish to use the electronic LOMA functions of the website are still permitted to provide paper LOMAs to FEMA and thus avoid the PII disclosure online.

For the paper based process, end users voluntarily provide their PII to be put into the system. This is an opt-in format and end users that wish to remain anonymous may do so but cannot submit LOMA/LOMRs.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: PII For each user is stored in the system

Mitigation: Multiple informational statements within the sign-up process and during each subsequent authentication sequence indicate the data retained and its private nature to the certifier. Only those documents that would normally be "sealed" with an engineer or licensed surveyor's stamp retain reference to the certifier's PII. That reference is required because it is the minimal necessary to establish the licensure status of the certifier.



During the paper based analog processes PII is used to communicate with the end users and is available only through privileged interfaces to the MIP which are not available to the general public. Role based authentication protects this data after it has been entered into the system. The paper records are kept in secured storage in accordance with the retention policy cited above.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

The information is maintained for 20 years according to the retention policy referenced above. This information is maintained to facilitate legal records of the classification of the flooding characteristics of specific parcels of land as they are and were previously categorized under the NFIP. Changes to those classifications affect the costs of insuring land under the NFIP which requires that the program have the ability to determine a flood plane classification at any point in the last 20 years to address potential disputes and provide data for forward-looking insurance decisions.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: PII for licensed professionals is maintained in the system.

Mitigation: Due to the legal nature of the records retained in the NFIP, it is required that the system retain PII for 20 years in accordance with the above referenced policy. The information which is to be retained has been reduced to the bare essentials possible to identify a user. All paper records are kept in secure storage and all electronic records are protected as described in the system security plan.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

There is exactly one external data sharing channel and it is with North Carolina's Flood Mapping Information Program. That interconnection is permitted to perform data extracts that are exactly what a public user could accomplish. There is no additional exposure of data through this channel.



6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Only publicly available data is transmitted over that interface. That interface is controlled by an ISA and each participant has agreed to defend the data as required by federal and state laws.

6.3 Does the project place limitations on re-dissemination?

There are no restrictions on re-dissemination of documents created by the MIP. These are matters of public record and cannot be restricted for re-dissemination.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

All disclosures of PII are logged in the log server for the MIP project. There are paper records of disclosures that occur on paper only transactions at the secure storage facility.



6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: PII for all users is retained in the system

Mitigation: The ability to access PII that is hosted in the system is restricted to administrative users for all records and to those with elevated privileges for a specific case. End users are not able to access PII from a case to which they are not a party. Role based user accounts prevent accessing this data online and policies that are taught during annual security awareness training are used to prevent release from the paper records.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

Changes to personal information of any kind (including PII) are accomplished through editing one's own account or requesting assistance from the help desk to make the change. A request with proof of the needed change (license document etc.) sent to the help desk will be acted on to remedy the error in a user record. In the case of paper records, all changes are accomplished by resubmitting the case papers.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Changes to personal information of any kind (including PII) are accomplished through editing one's own account or requesting assistance from the help desk to make the change. A request with proof of the needed change (license document etc.) sent to the help desk will be acted on to remedy the error in a user record. In the case of paper records, all changes are accomplished by resubmitting the case papers.

7.3 How does the project notify individuals about the procedures for correcting their information?

Change procedures are outlined in the user documentation for the application. All user documentation for this application is located online and accessible from the application home page. Additional help is available to users by calling the dedicated helpdesk.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: PII is maintained in the application

Mitigation: Some user account details can be edited by the users. If the data element that a user needs to edit is not changeable by them, a call to the helpdesk can get assistance in changing other aspects



of the account data. The change process for the online application includes confirmation by the end user that the data is now accurately reflected online.

Section 8.0 Auditing and Accountability

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

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

There are no celebrity users and there is no reason to focus effort on an audit regime that does not protect individuals. Audits of account modifications and security operations are monitored constantly. Modifying a record creates a security event that is logged. Logs are reviewed on a monthly basis. Additionally, there is an IDS/IPS in place that throws a warning when security operations fail repeatedly.

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

Users are required to complete annual security awareness training. That is performed by security staff at all work locations. Annual security awareness training includes training on privacy and protection of privacy.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

This is managed by LDAP accounts for each user. Each account has specific privileges based on roles. The roles are completely defined in the System Security Plan also on file with DHS/FEMA.



8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All proposed MOU's, ISA's, etc. are reviewed by project security and infrastructure staff and then forwarded to FEMA for final approval. There is only one ISA in existence for this project to date.

Responsible Officials

Mary Jo Mullens

MIP Operations Manager

Phone: 202-646-3227

E-mail: Maryjo.mullen@dhs.gov

Department of Homeland Security/Federal Emergency Management Agency

Approval Signature

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security