Privacy Impact Assessment

for

NFIP Map Service Center

February 12, 2007

Contact Point

Claire Drury, FEMA COTR
Mitigation Division MT-RA-DD
Federal Emergency Management Agency

Reviewing Official

Hugo Teufel, III
Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Abstract

The National Flood Insurance Program (NFIP) Map Service Center or MSC (formerly known as the NFIP Information Exchange) exists to provide immediate access to flood map information for any area in the United States to anyone needing map information. The NFIP Map Service Center is the Federal Emergency Management Agency's (FEMA) distribution center for the NFIP's 100,000 Flood Insurance Rate Maps, 12,000 flood studies, and other related material. A user may freely view the entire map online or purchase a paper map, purchase a digital version of the map on compact disc, or download the map from the website. It is the collection of personally identifiable information associated with the collection of customer information that is the reason for and subject of this privacy impact assessment (PIA).

Introduction

The National Flood Insurance Act established the National Flood Insurance Program (NFIP). FEMA is responsible for administering the National Flood Insurance Program. This program underwrites flood insurance for millions[1] of homeowners and businesses throughout the country. As part of administering this program, FEMA develops Flood Insurance Rate Maps (FIRMS) that assess flood risk. Use of these maps by insurance companies that write flood insurance policies[2] to determine rates and hazards is required by the Act.[3] In addition, the maps are used by community officials to develop ordinances and zoning determinations to help protect the public by reducing development in flood prone areas.

The NFIP Map Service Center or MSC (formerly known as the NFIP Information Exchange) exists to provide immediate access to flood map information for any area in the country to anyone needing this information. The NFIP Map Service Center is FEMA's distribution center for the NFIP's 100,000 Flood Insurance Rate Maps, 12,000 flood studies, and other related material. A user may purchase a paper map, privileges to freely view the entire map online, or a digital version of the map on compact disc. It is the collection of personally identifiable information associated with the collection of customer information that is the reason for and subject of this PIA.

Per the NFIP FEMA distributes paper and digital flood map products without charge to federal, state, and municipal governments and FEMA contractors. FEMA charges all other users to recover the reproduction and distribution costs for the NFIP flood map products. The Map Service Center operates a physical warehouse of paper products and an online web site for viewing and printing of flood maps and related products. The website also provides the ability to purchase the flood maps and related products. To carry out these functions, the website collects limited customer information.[4]

---

[1]http://bsa.nfipstat.com/reports/1011_200609.htm - September 30, 2006 - 5,363,981 flood insurance policies in-force.
[2]The Write Your Own (WYO) Program began in 1983 and is a cooperative undertaking of the insurance industry and FEMA. The WYO Program allows participating property and casualty insurance companies to write and service the Standard Flood Insurance Policy in their own names. These companies receive an expense allowance for policies written and claims processed while the Federal Government retains responsibility for underwriting losses. The WYO Programs operates as part of the NFIP, and is subject to its rules and regulations.
[3]Flood Insurance Act of 1968 as amended, 42 U.S.C. § 4100, *et seq*.
[4]http://msc.fema.gov

To describe a typical transaction, initially a user will choose to purchase a map through the map service center. Once the user determines he would like to purchase a map he is then required to register on the website if he has not already. The registration process collects name, email address, company name (optional), address, contact phone number, and business type.[5] Once registered with the site the user will be linked directly to the Department of Treasury's Pay.gov and will be prompted to enter a credit card number, credit card expiration date, credit card type, and billing address as well as shipping address, if applicable.[6] FEMA does not receive financial transaction information; rather, Pay.gov conducts all financial transactions for the Map Service Center.

Pay.gov then returns to the NFIP Map Service Center the payment approval or denial information, the last four digits of the credit card number, expiration date, and authorization code over an encrypted web connection (HTTPS) to the Financial Account Management Inventory System (FAMIS). See Figure 1, Data Flow. Order fulfillment is performed in FAMIS. The customer will then receive their map in the mail, permission to download from the website, or a CD containing their digital map.[7]

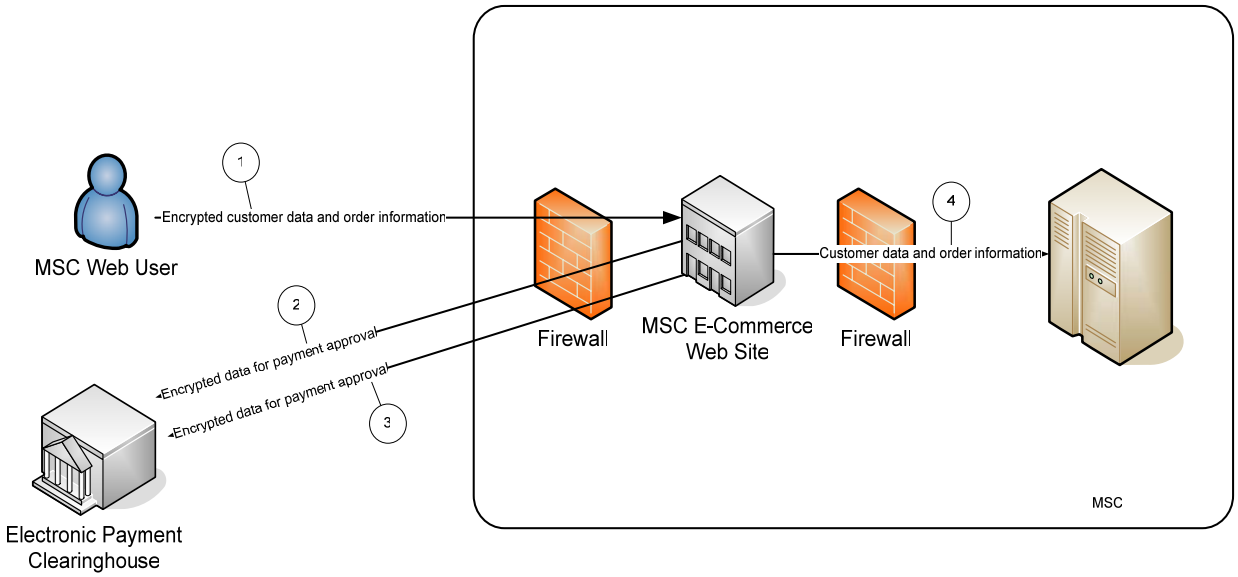
Primary NFIP Map Service Center operations are located in Elkridge, Maryland.

[5] "Business type" categories are FEMA, FEMA Contractor, Federal Government, State Government, Local Government, Appraiser, Insurance, Individual, Engineer, Lender, WYO, Real Estate, Builder/Developer, Surveyor, Flood Determination, Title Company, Law Firm/Settlement Company, Architectural Firm, Consulting Firm, Other.

[6] Pay.gov is the electronic payment clearinghouse approved by the Department of Treasury. Customers log on to the FEMA MSC Website at http://msc.fema.gov/ to purchase mapping products. During checkout customers provide credit card payment information directly to Pay.gov over a secure connection.

[7] The procedures for hard copy and electronic purchase differ slightly from electronic purchases. If a person calls or writes and requests a map and wishes to place an order, the customer service representative enters the same information directly into Pay.gov and converts the transaction into an electronic transaction. Paper orders are retained for three months and are filed by date and order type, not by personal identifier.

Figure 1 Logical Data Flow



1. Customer provides customer data and order information to MSC E-Commerce web site. Data is send via HTTPS providing authentication and encryption. Access to customer account is secured by customer user name and password combination.
2. MSC sends information to electronic payment clearinghouse for order payment approva. Data is send via HTTPS providing site-to-site authentication and encryption.
3. electronic payment clearinghouse returns payment approval information to MSC. Data is send via HTTPS providing site-to-site authentication and encryption.
4. Customer data and order information is sent to MSC ERP system for order fulfillment

Section 1 – Questions About The Data And Its Purposes

1.1 What information is to be collected (e.g., nature and source)?

The personally identifying information collected for ordering FEMA's Flood Insurance Rate Maps includes: customer name, company name (optional), address, personal e-mail address, and home phone number. Collected information is stored in FAMIS. Additional information is also stored, including NFIP Map Service Center account number, NFIP Map Service Center order number, the last four digits of credit card number, credit card authorization code, product requested, and appropriate transaction status such as approved and/or denied. Customers' full credit card information is not stored and is processed only by Pay.gov.

1.2 Why is the information being collected? Is it relevant and necessary to the purpose for which the system is being designed?

The information collected is relevant for the sole purpose of processing customer orders and requests for conventional paper NFIP Flood Maps and digital map products and services. The information collected is necessary for the purpose of receiving, filling, and shipping the orders received.

1.3 What is the intended use of the information?

The use of these records is for reference by the NFIP Map Service Center in processing customer orders and inquiries regarding our maps and to permit online processing of purchase transactions.

1.4 What are the sources of the information in the system? Where and how are you acquiring the information?

Personally identifiable information is provided directly by customers who purchase flood-related map products or whose requests have been forwarded to the NFIP Map Service Center.[8]

Customers provide the information via written, telephone and electronic (submitted on website) orders. This data is stored in the secure FAMIS system.

1.5 How will the information be checked for accuracy?

Customer provided information is assumed to be accurate for order fulfillment because it is provided to FEMA directly from the individual. Inaccurate home address information will result in orders returned by the mail, shipping carrier, or rejected credit card purchase. In this event, the customer is contacted via home telephone or personal email to obtain corrected information. Credit card information is assumed to be accurate as given to Pay.gov by the individual. If credit card information is inaccurate the transaction will be canceled or delayed. Overall, if accurate data is not provided, the order cannot be processed and is cancelled from the system.

[8] FEMA has several call centers that help coordinate communication and help information requests arrive in their proper destination. The call centers do not collect personally identifiable information for Map Service Center, but forward phone calls or emails regarding the purchase of maps to the Map Service Center.

1.6 Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

No. The system will not derive new data or create data about individuals through aggregation of information collected.

1.7 Will the newly derived data be placed on the individual's record?

No, not applicable.

1.8 Can the system make new determinations about an individual that would not be possible without the new data?

No, not applicable.

1.9 How will the newly derived data be verified for relevance and accuracy?

Not applicable.

1.10 Are the data elements described in detail and documented? If yes, what is the name of the document?

Yes. The data elements are described in detail and documented in the NFIP Map Service Center System Security Plan. Also, refer to Section 1, question 1 for the types of data that are being collected and the System of Records Notice (SORN, FEMA MIT-7, Flood Map Customer Records) which is attached as Appendix B.

Section 2 – Questions About Redress

2.1 What opportunities do individuals have to decline to provide information?

Purchasing of maps is purely voluntary and without giving personally identifying information a customer's order cannot be fulfilled.

2.2 What opportunities do individuals have to consent to particular uses of the information?

Under the FEMA NFIP Map Service Center Privacy Policy (Appendix A, and also at http://www.fema.gov/help/privacy_msc.shtm), individuals consent to the specific intended use of this information by the NFIP Map Service Center for the purpose of processing and filling their orders for NFIP map products and services by providing their names, home addresses, home phone numbers, personal e-mail addresses, and credit card information. Without this information, orders cannot be processed. The NFIP Map Service Center does not share any data or information with any

outside sources other than the limited information shared with pay.gov for processing. The collection of personally identifying information is used solely for the purpose of fulfilling orders.

2.3 How do individuals grant consent concerning how their information will be used or shared?

Customers voluntarily provide their personal data in order to purchase NFIP maps. Customers are informed of the voluntary consent for the NFIP Map Service Center's limited use of their customer information by the terms of the NFIP Map Service Center Privacy Policy**.**

2.4 What are the procedures for individuals to gain access to their own information?

Web users can view or update their personal data such as their home address or home phone number by logging into the website using their unique user ID and password combination which they established at registration. This procedure prevents unauthorized access to other customers data stored in the system. All non-web users can update their personally identifiable information by telephone to the NFIP Map Service Center Customer Service Center; again the customer must provide the Customer Service Center representative with their unique MSC account number.

A request for access to records in this system may also be made in writing to the System Manager, identified in Section 4.1(d) of this PIA, in conformance with 6 CFR part 5, subpart B and 44 CFR part 6, which provides the rules for requesting access to Privacy Act records.

2.5 What are the procedures for correcting erroneous information?

Once a profile is created, users can view or update their personal data such as their home address or home phone number by logging into the website using a unique user ID and password combination. This prevents unauthorized access to other customer's data stored in the system. If calling the NFIP Map Service Center Customer Service, the customer must provide the Customer Service Center representative with their unique MSC account number.

Also a request for correcting erroneous information may be made in writing to the System Manager, identified in Section 4 - 1. d. in conformance with 6 CFR part 5, subpart B and 44 CFR part 6, which provides the rules for requesting access to Privacy Act records.

Section 3 – Questions About Access To The Data

3.1 Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others) and is it documented?

All access to data is defined by each user's need and use of the data. All access to data is controlled by role based access controls defined by user profiles. All changes in the system including those made to personally identifiable information stored in the system are logged in the system and can be tracked to the specific user ID.

NFIP Map Service Center customers (private individuals ordering items from the web site) using a unique user ID and password combination, have access only to their own personally identifiable data for the sole purpose of updating or revising their own personal information.

Non-web customers have access to their data through NFIP Map Service Center Customer Service Representatives.

NFIP Map Service Center Customer Service Representatives have access to customer data as required for processing written, phone, or fax orders placed by customers and providing customer service on a need to know basis.

The NFIP Map Service Center IT staff (system administrators) has limited access to personally identifiable information data as required for the development, operation, and troubleshooting problems of NFIP Map Service Center computer systems and networks.

Access is controlled and documented in the NFIP Map Service Center System Security Plan.

3.2 How will access to the data by a user be determined?

The NFIP Map Service Center Program Manager authorizes all users' access roles only to the extent necessary for each individual to perform their official duties. The NFIP Map Service Center System Security Plan as well as job descriptions and duties determine which role will be assigned to an individual.

3.3 Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes, technical, operational, and management controls are in place per the NFIP Map Service Center System Security Plan, allowing authorized users access only to the data necessary based on user's roles and their required use of data.

3.4 Will users have role-based access to data on the system limiting them to some but not all of the data?

Yes. NFIP Map Service Center website customers are limited to the NFIP Map Service Center and the FEMA Map Store websites, and to only their own data. Customers access the FEMA Map Store site as a guest or as a registered user. In either case, access is limited to general information pages and

forms used to register or order maps. Registered users must login using a login ID and password. If a user forgets a password, then the system will generate a new one and e-mail it to the user's registered e-mail address after they correctly answer a challenge question. No one except the user can modify any registration data, including the password and the challenge question. The details of role-based access have already been addressed in Section 3, question 1.

Employee or contractor role based access is determined through the NFIP Map Service Center System Security Plan (see 3.2 and 3.3).

3.5 What controls are in place to prevent the misuse (e.g. browsing, expired privileges, etc.) of data by those having access?

Technical, operational, and management controls are in place and enforced in accordance with the NFIP Map Service Center System Security Plan allowing authorized users access only to the personal data necessary for each user's official role and their required use of data. NFIP Map Service Center Customer Service Representatives are allowed to modify data as specifically requested by the customer/user in order to perform their role in fulfilling customer orders. Systems Administrators are only allowed access to the data for system backup and to troubleshoot any system issues.

Operational Controls:

NFIP Map Service Center customers who place phone orders can obtain and request changes to their personal information via phone to an NFIP Map Service Center Customer Service Representative. The customer must provide his unique account ID as authentication for changes to their data. All changes in the system including those made to personally identifiable information stored in the system are logged in the system and can be tracked to the specific user ID.

Technical Controls:

All access to data is defined by the users need and use of the data. All access to data is controlled by role based access controls (RBAC) defined by user profiles.

Access to customer data by NFIP Map Service Center staff is controlled through use of a unique user ID and password combination. Strong passwords are required and ensured by system and application controls. User passwords must be changed on a regular basis.

Access to the NFIP Map Service Center facility is controlled via card key. All access to the NFIP Map Service Center facility is logged. Physical access to the systems containing the data is controlled by card key entry for authorized personnel. Logical access is password controlled based on each user's official role.

The computerized records and paper records are stored in secured areas that are accessible only to employees who require the information in performing their official duties. Paper documents are stored either in locked file cabinets within locked rooms or in otherwise secured areas. All personnel with access to records are screened, cleared, and trained on the use of these system safeguards.

Management Controls:

Regular reviews of NFIP Map Service Center security systems and procedures are preformed, ensuring that appropriate levels of security are maintained.

NFIP Map Service Center staff is required to take security classes and successfully demonstrate their understanding of security requirements, procedures and rules of behavior before access to NFIP Map Service Center systems is granted. Annual reviews and testing of security is also required for NFIP Map Service Center staff.

3.6 Do other systems share data or have access to data in this system? If yes, explain. Include a discussion of who will be responsible for protecting the privacy rights of individuals affected by the interface?

Release of any requested data would require the specific review and approval by the FEMA Office of Chief Counsel and the Systems Manager in accordance with the Routine Uses of the SORN, FEMA MIT-7, Flood Map Customer Records (Appendix B). FEMA does not collect credit card information; credit card information is sent directly to Pay.gov.

3.7 Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?

Yes, the U.S. Department of Treasury, for the very limited purpose of verifying the validity of credit cards used to pay for maps. As described in our response to question 3.6 above, purchasing transactions require that individual customer name, home address, credit card number, expiration date, and NFIP Map Service Center order number is transmitted to a credit card clearinghouse over an encrypted HTTPS Internet channel during the credit card payment process. The credit card clearinghouse is the electronic payments service provider sponsored by the U.S. Department of Treasury. The credit card clearinghouse provides real-time credit card authorization and accepts credit card collections on behalf of Federal agencies. The credit card clearinghouse does not have access to any data or records stored NFIP Map Service Center systems.

No other outside interface to the system exists and access to the system would not be permitted.

3.8 How will the data be used by these other agencies?

As already described in questions 3.6 and 3.7 above, individual customer name, home address, credit card number, expiration date, and NFIP Map Service Center order number is transmitted to a credit card clearinghouse over an encrypted web connection (HTTPS) during the credit card payment process for verifying credit card account information. This information is provided solely and specifically for real-time credit card authorization and credit card collections on behalf of the NFIP Map Service Center order processing.

3.9 Who is responsible for assuring proper use of the data by other agencies?

FEMA Office of General Counsel and the Systems Manager - Claire Drury, FEMA COTR - Mitigation Division -MT-RA-DD Federal Emergency Management Agency 202-646-2884

3.10 How will the system ensure that other agencies only get the information they are entitled to?

The transmission of data is only sent to the credit card clearinghouse solely and specifically for real-time credit card authorization and credit card collections on behalf of the NFIP Map Service Center order processing. The customers name, home address, credit card number, credit card expiration date, order amount, and NFIP Map Service Center order ID number are sent encrypted and authenticated to the clearinghouse. The credit card clearinghouse does not have access to any data or records stored in NFIP Map Service Center systems.

Section 4 – Questions About Maintenance Of Administrative Controls

4.1 Are the data secured consistent with agency requirements under the Federal Information Security Management Act? Specifically:

a. Affirm that the agency is following IT security requirements and procedures required by federal law and policy to ensure that information is appropriately secured;

Yes, the NFIP Map Service Center follows FISMA guidelines including documented Continuity Plans, mandatory Security Awareness Training for all users, incident detection, reporting and response, and annual review of system security with reporting to OMB. Security technologies comply with the following relevant DHS, National Institute of Standards and Technologies (NIST), Office of Management and Budget (OMB), and FEMA security guidance including:

- Public Law 107-296, Homeland Security Act of 2002, Title X, Federal Information Security Management Act (FISMA) of 2002, November 25, 2002.
- Homeland Security Presidential Directive 7 (HSPD-7), Directive on Critical Infrastructure Identification, Prioritization, and Protection, December 17,2003
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*.

- Public Law 104-106, Clinger-Cohen Act of 1996 [formerly, Information Technology Management Reform Act (ITMRA)], February 10, 1996.
- Privacy Act of 1974, as Amended. 5 United States Code (U.S.C.) § 552a, Public Law 93-579, Washington, DC, July 14, 1987.
- Executive Order (E.O.) 13231, Critical Infrastructure Protection in the Information Age, October 16, 2001.
- 5 Code of Federal Regulations (CFR) § 2635, Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch*.
- Department of State 12 Foreign Affairs Manual (FAM) 600, *Information Security Technology*, June 22, 2000.
- Federal Preparedness Circular (FPC) 65, *Federal Executive Branch Continuity of Operations*, July 1999.
- DHS Management Directive 4300A, Sensitive Systems Policy Publication.
- DHS Management Directive 4300A, Sensitive Systems Handbook for DHS.
- Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorizations of Federal Information and Information Systems, December 2003
- NIST SP 800-18, Guidelines for Developing Security Plans for Information Technology Systems, December 1998
- NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001.
- NIST SP 800-30, Risk Management Guide for Information Technology Systems, July 2002.
- NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.
- NIST SP 800-37, Guide for the Security Certifications and Accreditations of Federal Information Systems, May 2004.

b. Acknowledge that the agency has conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls;

FEMA has conducted a risk assessment and a documented System Security Plan. FEMA reviewed the NFIP Map Service Center security and policies and found them to be appropriate given the MSC level of acceptable risk. The NFIP Map Service Center received its first Certification and Accreditation (C&A) in June, 2003 with Authority to Operate (ATO) until August 2006. Map Service Center was recertified and accredited in 2006 with a new ATO issued on September 9, 2006.

c. Describe the monitoring/testing/evaluating on a regular basis to ensure that controls continue to work properly, safeguarding the information,

Monitoring/testing/evaluating is performed on a regular basis to include: Annual Self-Assessments are performed on system security per NIST SP 800-26 *Security Self-Assessment Guide for Information Technology Systems*, and System logs and Intrusion Detection Systems are reviewed daily by Systems Administrators.

d. Provide a point of contact for any additional questions from users.

Claire Drury, FEMA COTR
Mitigation Division -MT-RA-DD
Federal Emergency Management Agency

500 C Street SW
Washington, DC 20472
202-646-2884

4.2 If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

A secondary site is used for data replication for the purposes of the IT Contingency Plan. All physical and logical access to this site is equal to the primary site described above.

4.3 What are the retention periods of data in the system?

Consistent with our SORN, the personal information stored on paper is retained for three months after it is input into our electronic database. All personal information stored in the database is retained for six years and three months after the last log-in to the website occurs which is consistent with the National Archives and Records Administration's (NARA's) records retention schedule.

4.4 What are the procedures for expunging the data at the end of the retention period and are these procedures documented?

All records are disposed of consistent with NARA's records retention schedule and as documented in our SORN, after 6 years and three months.

4.5 Will the system provide the capability to monitor individuals or groups of individuals? If yes, explain.

No, the system does not provide the capability to monitor individuals or groups of individuals because the system is used solely for the purpose of maintaining order information of NFIP maps only.

4.6 What controls are in place to prevent unauthorized monitoring of individuals or groups of individuals?

The system is not a surveillance system and has no necessity to monitor individuals or groups of individuals. However, security controls are in place to prevent misuse of data or inappropriate access to data (see Section 3)

4.7 Under which Systems of Record Notice (SORN) does the system operate? Provide Number and Name.

The title of the system of records is Flood Map Customer Records, FEMA/MIT-7. The SORN was published in the Federal Register on June 8, 2001. (reference: *System of Records Notice (SORN) published on June 8, 2001 (Federal Register/Vol. 66, No. 111).* It is attached at Appendix B**.**

Section 5 – Decision Analysis

5.1 Did you evaluate competing technologies on their privacy handling capabilities? If yes, explain.

No. Industry standard protocols (HTTPS) were the only option available for a system open to the public for the purpose of ordering NFIP maps. The credit card clearinghouse was the only FEMA approved system for credit card processing and authorization during 2001 when the system was created.

5.2 Were any changes made to system architectures, hardware, software, or implementation plans as a result of doing a PIA? If yes, explain.

Yes, provisions for insuring the privacy of the individual's personally identifiable information provided by NFIP Map Service Center customers have been addressed from the inception of this project. However, we have found that this system review process in performing the Privacy Impact Assessment has been useful in identifying potential areas where we might improve the handling of personally identifiable information. As an example, we now only store the last four digits of the customer's credit card number rather than the entire number. Retaining the full account number was determined to be an unnecessary collection. Additionally, Pay.gov conducts transactions using the full credit card. Because Pay.gov is an authorized payment clearinghouse, MSC does not handle credit information, thereby eliminating a privacy risk.

Technical and operational controls protecting the customer data include data encryption, sender and receiver authentication, firewalls, and controlled physical access to all computer systems and networks. Management controls are also in place allowing authorized users access only to the data necessary based on user's roles and their required use of data. Figure 1 shows the logical flow of data.

Approval Signature Page

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

Appendix A

FEMA MSC Privacy Policy

Introduction

This World Wide Web (WWW) site is provided as a public service by the Federal Emergency Management Agency Map Service Center, (FEMA MSC).

Information presented on this WWW site is considered public information and may be distributed or copied. Use of appropriate byline/photo/image credits is requested.

Information collected and stored automatically

The information we learn about you from your visit to our website depends upon what functions you perform when visiting our site.

For site management, information is collected for statistical purposes. This government computer system uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.

If you do nothing during your visit but browse through the website, read pages, or download information, we will gather and store certain information about your visit automatically. This information does not identify you personally. We automatically collect and store the following information about your visit:

- The Internet domain (for example, "xcompany.com" if you use a private Internet access account, or "yourschool.edu" if you connect from a university's domain) and IP address (an IP address is a number that is automatically assigned to your computer whenever you are surfing the Web) from which you access our website
- The type of browser and operating system used to access our site
- The date and time you access our site
- The pages you visit
- The geographic location (country) visited from
- If you linked to the MSC website from another website, the address of that website

We use this information to help us make our site more useful to visitors -- to learn about the number of visitors to our site and the types of technology our visitors use. We do not track or record information about individuals and their visits unless you register on the MSC web site.

In addition, if you register and create a user account on the MSC web site, we will gather and store certain personal information provided by you. The following required information is collected:

- A unique login user name
- Your email address
- First and last name
- Address
- Daytime phone number
- Type of business
- Purchasing products from the MSC site may require specific credit card information

We reveal and store only the last four digits of your credit card numbers when confirming an order. We encrypt and transmit the entire credit card number to the Pay.Gov, a service provided by the United States Department of Treasury during order processing.

We work to protect the security of your information during transmission by using Secure Sockets Layer (SSL) software, which encrypts information you input.

Personal information provided by you while on the MSC web site will be used only for transacting business between you and the FEMA Map Service Center. Your personal information will not be sold.

Cookies

The MSC uses cookies on its websites solely to allow complex, software user-driven applications to function correctly. For example, MSC's online ordering services publications allow users to shop through online catalogs. The MSC server sends a "cookie" back to the user's computer containing only a "session id" whenever you access the site. This information may be retained by your browser until your session expires or your browser is closed. MSC's use of cookie technology is not otherwise designed, intended or used to collect, store, or analyze information pertaining to Internet users.

Security and Intrusion Detection

Unauthorized attempts to defeat or circumvent security features, to use the system for other than intended purposes, to deny service to authorized users, to access, obtain, alter, damage or destroy information, or otherwise to interfere with the system or its operation is prohibited. Evidence of such acts may be disclosed to law enforcement authorities and result in criminal prosecution under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act of 1996 (Pub. L. 104-294), (18 U.S.C. 1030), or other applicable criminal laws.

For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor host and network traffic to identify unauthorized attempts to upload or change information or otherwise cause damage.

Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with National Archives and Records Administration guidelines.

Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act.

Appendix B

MSC System of Records Notice

Privacy Act of 1974: Flood Map Customer Records

AGENCY: Federal Emergency Management Agency (FEMA)

ACTION: Notice of a new system of records

SUMMARY: In accordance with the Privacy Act of 1974 (5 U.S.C. 552a), we (FEMA) give notice that we are establishing a new system of records under the authority of the Flood Insurance Act of 1968 as amended, 42 U.S.C. § 4100, *et seq*. That Act established the National Flood Insurance Program (NFIP), a critical component of which is the identification and mapping of the nation's floodplains to provide the data necessary for community floodplain management programs and to actuarially rate flood insurance. Pursuant to statute, we distribute conventional and digital flood map products without charge to federal, state and municipal governments. We charge all other users for our products and services. This system of records will enable us, through the NFIP Flood Map Store, to fill written, telephonic and electronic orders from these users for the various map products; to cumulate and retrieve their order information; and to disseminate new product information to them.

FOR FURTHER INFORMATION CONTACT: Eileen Leshan, FOIA/Privacy Act Specialist, Federal Emergency Management Agency, Room 840, 500 C Street, SW,
Washington, DC 20472, (telephone) (202)-646-4115, (telefax) (202)-646-4536, or (email)Eileen.Leshan@fema.gov.

SUPPLEMENTARY INFORMATION:

We published a notice of Fee Schedule for Processing Requests for Map Changes, for Flood Insurance Study Backup Data, and for National Flood Insurance Program Map and Insurance Products on May 3, 2000, 65 Fed. Reg. 25726.

The new systems of records report, required by 5 U.S.C. 552a(r), is being simultaneously submitted to the Committee on Government Operations of the House of Representatives, the Committee on Governmental Affairs of the Senate, and the Office of Management and Budget, pursuant to Appendix 1 to OMB Circular A-130.

Accordingly, we add FEMA/MIT-7 of the FEMA Privacy Act systems of records to read as follows:

SYSTEM NAME: FEMA/MIT-7, Flood Map Customer Records

SECURITY CLASSIFICATION: Unclassified

SYSTEM LOCATION: Offices of the map sales servicing agent under contract with the Federal Emergency Management Agency, Washington, DC 20472.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who purchase flood-related map products or whose requests have been forwarded to the map sales servicing contractor. The system also contains records concerning individuals in their entrepreneurial capacity, corporations and other business entities whose records are not subject to the Privacy Act.

CATEGORIES OF RECORDS IN THE SYSTEM:

Electronic database contains name, address, phone number, credit card number and expiration date, account number, order number, product requested and appropriate accounting entries. Information from paper orders is entered into database and paper orders are destroyed after three months.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The National Flood Insurance Act of 1968, as amended, and the Flood Disaster Protection Act of 1973, as amended, 42 U.S.C. § 4001 *et seq.*, 5 U.S.C § 301, Reorganization Plan No. 3 of 1978 and E.O. 12127.

PURPOSE:

The primary use of the records is for reference by the map sales servicing contractor in processing customer inquiries, orders and complaints. The contractor must comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. § 552a.

ROUTINE USE OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to use of the records by a contractor engaged to assist the Agency in performing a contract service related to this system of records and who requires access to the records in order to perform the activity, disclosure of records outside FEMA or the map sales contractor may be made to:

(1) The U.S. Department of Justice or a court or adjudicative body when (a) the United States, FEMA, a component of FEMA, the map sales servicing contractor or, when represented by the Government, an employee of FEMA is a party to litigation or anticipated litigation or has an interest in such litigation, and (b) FEMA determines that the disclosure is relevant or necessary to the litigation and is compatible with the purpose for which the records were compiled;

(2) An appropriate Federal, State, local or foreign agency responsible for investigating, prosecuting, enforcing, or implementing a statute, regulation, rule or order, where FEMA becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation;

(3) A Congressional office when disclosure from the record of an individual is necessary to respond to an inquiry the individual has made to the Congressional office;

(4) To the National Archives and Records Administration for the purpose of conducting records management studies under the authority of 44 U.S.C. 2904 and 2906.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Disclosures under 5 U.S.C. §552a(b)(12): Disclosures may be made from this system to a "consumer reporting agency" as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f)) or the Federal Claims Collection Act of 1966 (31 U.S.C. 3701(a)(3)).

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

Storage

Records in this system are temporarily stored in a database (i.e., on computer hard drives and computer disks) and subsequently archived in magnetic media. Paper printouts of these data may be made as necessary. Paper copies of customer orders are stored in manual files and destroyed after three months.

Retrievability

Retrievable by name of organization, individual, account number, or order number.

Safeguards

Records are maintained by the FEMA map sales servicing contractor in areas occupied by contractor personnel during working hours with the building locked and secured by alarm during off hours. In addition, the risk of unauthorized access to or disclosure of personal data in the proposed system is minimized through the use of passwords and security profiles and permissions to enter the computer system in which data are maintained. The computerized records and paper records are stored in secured areas that are accessible only to employees who require the information in performing their official duties. Paper documents are stored either in lockable file cabinets within locked rooms or in otherwise secured areas. All personnel with access to records are screened, cleared, and trained.

Retention and Disposal

Records are retained and disposed of in accordance with the retention and disposition schedules set forth in FEMA Manual 5400 (August 1989), "Records Management: Disposition, Retention and Files Plan." Means of disposal are appropriate to the storage medium (e.g., erasure of disks, shredding of paper records, etc.).

SYSTEM MANAGER AND ADDRESS:

Project Officer, Map Service Center, Technical Services Division, Mitigation Directorate, Federal Emergency Management Agency, Washington, DC 20472.

NOTIFICATION AND RECORDS ACCESS PROCEDURES:

Inquires should be addressed to the System Manager following procedures set forth at 44 C.F.R. Part 6, Subpart C.

CONTESTING RECORDS PROCEDURE:

A petition for amendment should be addressed to the System Manager and must meet the content requirements set forth at 44 C.F.R. Part 6, Subpart D.

RECORD SOURCE CATEGORIES:

Customers on whom record(s) are maintained.

SYSTEM EXEMPTIONS FROM CERTAIN PROVISIONS OF THE ACT.

None.