Privacy Impact Assessment for the

Web-IFMIS (Integrated Financial Management Information System)

DHS/FEMA/PIA-020(a)

August 16, 2013

Contact Point
Michael Thaggard
Office of Chief Financial Officer
Federal Emergency Management Agency
(202) 212-8192

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The U.S. Department of Homeland Security (DHS) Federal Emergency Management Agency's (FEMA) Office of the Chief Financial Officer (OCFO) owns and operates the Web Integrated Financial Management Information System (Web-IFMIS). Web-IFMIS is FEMA's official accounting and financial management system that pulls all of FEMA's financial data from other FEMA, DHS, and Government-wide systems (subsystems), and is the source of data for both internal and external financial reporting. The system records and tracks all financial transactions. FEMA is conducting this PIA because Web-IFMIS collects, uses, maintains, retrieves, and disseminates personally identifiable information (PII) from the subsystems. This PIA replaces the previously published DHS/FEMA/PIA-020 Integrated Financial Management Information System Merger (IFMIS - Merger).

Overview

Web-IFMIS[1] is FEMA's official accounting and financial management system that tracks all of FEMA's financial transactions. Web-IFMIS does not collect information directly from individuals; the information contained in the system is pulled from other systems. Web-IFMIS provides FEMA's financial managers a global view of all FEMA's financial systems. Web-IFMIS uses information provided through these various subsystems in order to make payments to entitled groups (grantees), FEMA employees for payroll and travel reimbursement, and contractors and other vendors for payment of services. Web-IFMIS is also used to account for the expenditure of public funds as mandated under various statutes, Executive Orders, Office of Management and Budget (OMB) guidance, regulations, and DHS and FEMA policies.

To facilitate the processing of accounting and financial information, Web-IFMIS is comprised of various modules (see section 5.1 for a listing of modules). Web-IFMIS collects information on grantees, payrollers, employee travelers, contractors, and vendors. To account for expenditures, Web-IFMIS generates report invoices, payment receipts, cash receipts, commitments, obligations, receiving reports, expenditures, and advanced charges.

Web-IFMIS carries out the budgeting, management of vendor accounts, payment approval, and accounting for FEMA's finances. The process begins when Congress appropriates and OMB approves FEMA's funding. Next, FEMA's OCFO establishes accounts within Web-IFMIS to correspond with the funding appropriated by Congress and approved by OMB. FEMA program offices then request allocation of funds, via Web-IFMIS' subsystems, as part of FEMA's annual and ongoing budgeting, financial, and accounting processes.

FEMA's OCFO receives funding requests from the various program offices and processes these requests by first reviewing the request and determining whether funds are available for the transaction. If funds are available then FEMA commits the funds in Web-IFMIS to prevent those funds from being used for any other purpose. FEMA's OCFO also reviews the requests to make sure that vendor accounts are established for each individual, entitled group, or entity identified on the requests. FEMA establishes vendor accounts using PII, including name and a unique identifier (e.g., social security number, employer

[1] On May 15, 2003, IFMIS-Merger underwent a change in servers/platform and a system name change to reflect the new server/platform change. IFMIS-Merger is now known as Web-IFMIS, due to the system moving to a new web-accessible platform.

identification number). Once funding is appropriated and committed and the proper vendor accounts are established, FEMA is able to process payments or provide reimbursements to those individuals, entitled groups, or entities referenced on the initial requests.

As program offices receive invoices, they review and send payment approval to FEMA finance analysts. FEMA finance analysts approve payments within Web-IFMIS and transmit an electronic and encrypted file to the Department of the Treasury (Treasury) on a daily basis. Treasury is then responsible for collecting the electronic files, processing payments, and returning a control number for each batch file to FEMA. FEMA finance analysts verify payments by reconciling Treasury control numbers with the payment requests and Web-IFMIS deducts the paid funds from the appropriate accounts.

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 authority for this system is based on the Joint Financial Management Improvement Program, other statutes, Executive Orders, OMB and Treasury guidance, regulations, and DHS and FEMA policies:

- Debt Collection Improvement Act of 1996, 31 U.S.C. § 7701(c);
- Federal Claims Collection Act, 31 U.S.C. § 3711, et. seq.;
- 31 C.F.R. part 370;
- 42 U.S.C. §§ 5170a, 5170b, 5170c, 5172, 5173, 5174, 5177, 5177a, 5179, 5183, 5184, 5187m, 5189, 5189d, and 5192 (2013);
- 6 U.S.C. § 313 (2007);
- Federal Managers' Financial Integrity Act of 1982, 31 U.S.C. § 1352;
- Chief Financial Officers Act of 1990, 31 U.S.C. §§ 901-903; Federal Financial Management Improvement Act of 1996, 31 U.S.C. § 3512;
- Exec. Order No. 9397, as amended by Exec. Order No. 13478;
- OMB Circular A-130;
- OMB Circular A-127; and
- The Internal Revenue Code, 26 U.S.C. § 6011 (b) and § 6109.

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

The information in the system is covered by the following FEMA, DHS, and Government-wide SORNs:

- DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS), 77 FR 70,792 (Nov. 27, 2012);
- DHS/ALL-007 Accounts Payable System of Records, 73 FR 61,880 (Oct. 17, 2008);
- DHS/ALL-008 Accounts Receivable System of Records, 73 FR 61,885 (Oct. 17, 2008);
- DHS/ALL-019 Payroll, Personnel, Time, and Attendance Records, 73 FR 63,172 (Oct. 23, 2008);
- DHS/FEMA-004 Grant Management Information Files (GMIF), 74 FR 39,705 (Aug. 7, 2009);

- DHS/FEMA-008 Disaster Recovery Assistance Files System of Records (DRA), 78 FR 25,282 (April 30, 2013),
- DHS/FEMA-009 - Hazard Mitigation Assistance Grant Programs (HMA), 77 FR 17,783 (July 23, 2012); and
- General Services Administration (GSA)/GOVT-4 - Contracted Travel Services Program, 41 FR 26,700 (June 3, 2009).

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

A System Security Plan (SSP) has been completed for Web-IFMIS. Web-IFMIS is operational and was granted an Authority to Proceed (ATP) on May 7, 2013, for 60 days. Web-IFMIS has a "high" categorization in accordance with FIPS 199. The Web-IFMIS SSP complies with DHS Directive 4300A.

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

Web-IFMIS uses the standards for accounting record as stated in General Records Schedule 5 and General Records Schedule 7.

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.

Web-IFMIS is not subject to the requirements of the Paperwork Reduction Act (PRA) because a specific form completed by the public is not used to populate the information in Web-IFMIS. Information is populated from various subsystems.

Section 2.0 Characterization of the Information

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

Categories of records in this system include:

For Grantees:

- Employers Identification Number (EIN);
- Name (first, last);
- Address (personal, business);
- Phone Number (personal, business);
- Email Address (personal, business);
- Contract/Grant/Payment Amount;
- Bank Account, Routing Number, Bank Information (bank name, address, phone); and
- Grant Number.

For Payrollers:

- Total Payroll Expenditures by Fund Code;
- Total Payroll Expenditures by Project Code;
- Amount;
- Appropriation;
- Fiscal Year; and
- Schedule Number.

For Employee Travel Payments:

- Name (first, last);
- Address (personal, business);
- Phone Number (business);
- Social Security Number;
- Travel Payment;
- Voucher Number;
- Government Credit Card Number; and
- Bank Account, Routing Number, Bank Information (bank name, address, phone).

For Vendor Payments:

- Name (business);
- Address (business);
- Amount;
- Phone Number (business); and
- Bank Account, Routing Number, Bank Information (bank name, address, phone).

For Payment Verification:

- Control Number.

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

Web-IFMIS does not collect information directly from individuals; the information within the system is collected from various interfaces, batch processes, and data feeds from other systems. Each system is outlined below with a description and supporting privacy compliance documentation.

IAC: Individual Assistance Module provides requisite information before, during, and after a disaster. The following is a list of privacy compliance documents supporting this system:

PIA: DHS/FEMA/PIA-027 – National Emergency Management Information System-Individual Assistance (NEMIS-IA) Web-based and Client-based Modules, June 29, 2012.

SORN: DHS/FEMA–008- Disaster Recovery Assistance Files, 78 FR 25,282 (April 30, 2013).

ISAAC: Integrated Security and Access Control provides communication with other FEMA applications that send user name and password validation;

PIA: Forthcoming Authentication and Provisioning Service (APS) PIA.

SORN: DHS/ALL-004 - GITAARS, 77 FR 70,793 (Nov. 27, 2012).

EMMIE/PA: Emergency Management Mission Integrated Environment/Public Assistance Module provides automated information on grants related to public assistance and disaster mitigation. The following is a list of privacy compliance documents supporting this system;

PIA: DHS/FEMA/PIA-013- Grant Management Program, July 14, 2009.

SORN: DHS/FEMA-004-Grant Management Information Files, 74 FR 39,705 (Aug. 7, 2009).

PARS: Payment and Reporting System Web Server enables grant recipients to submit requests for grant payments and submit financial status reports online. The following is a list of privacy compliance documents supporting this system;

PIA: DHS/FEMA/PIA-013 Grant Management Programs, July 14, 2009.

SORN: DHS/FEMA-004-Grant Management Information Files, 74 FR 39,705 (Aug. 7, 2009).

GFI: Generic Financial Interface provides basic information about accounting general ledgers. The following is a list of privacy compliance documents supporting this system;

PIA: PIA is in development.

SORN: DHS/ALL-007 Accounts Payable System of Records, 73 FR 61,880 (Oct. 17, 2008); DHS/ALL-008 Accounts Receivable System of Records, 73 FR 61,885 (Oct. 17, 2008).

AAMS: Automated Acquisition Management System enables the procurement, grant, and program management offices to provide customers with integrated delivery of policy, regulatory content, data collection, and process tracking. This is not a privacy sensitive system and a PIA and SORN are not required.

AFG: Assistance to Firefighters Grant Application is the competitive grant opportunity that is administered by the Assistance to Firefighters Program Office and assesses the needs of each individual applicant compared to the other applicants interested in the opportunity. The following is a list of privacy compliance documents supporting this system;

PIA: DHS/FEMA/PIA-013 Grant Management Programs, July 14, 2009.

SORN: DHS/FEMA-004GMIF, 74 FR 39,705 (Aug. 7, 2009).

MT e-Grants: State, Territory, and Native American Tribe grant program is the online grant application and grant management information system. The following is a list of privacy compliance documents supporting this system;

PIA: DHS/FEMA/PIA-006 FEMA National Emergency Management Information System Mitigation Electronic Grants Management System, January 16, 2007.

SORN: DHS/FEMA-009 – Hazard Mitigation Assistance Grant Programs, 77 FR 17,783 (July 23, 2012).

ACCPAC: Accounts Package Systems tracks, monitors, and manages debts owed to FEMA. The following is a list of privacy compliance documents supporting this system;

PIA: DHS/FEMA/PIA-024- Accounting Package (ACCPAC), June 8, 2012.

SORN: DHS/ALL-007- Accounts Payable System of Records, 73 FR 61,880 (Oct. 17, 2008); DHS/ALL-008 Accounts Receivable System of Records, 73 FR 61,885 (Oct. 17, 2008).

NFC: Payroll/Personnel Systems is the online database that maintains employee personnel records and time and attendance reports. The following is a list of privacy compliance documents supporting this system;

PIA: National Finance Center (NFC) Personnel/Payroll System, available at: http://www.usaid.gov/policy/egov/2009-10-27_NFC%20PIA%20Summ.pdf.

SORN: DHS/ALL-019-DHS Payroll, Personnel, Time, and Attendance Records, 73 FR 63,172 (Oct. 23, 2008).

FedTraveler.com: E-Gov Travel Service generates service to plans, books, tracks, approves, and request reimbursement for travel services to federal employees. The following is a list of privacy compliance documents supporting this system;

PIA: General Services Administration (GSA), E-Travel Initiative, Electronic Data System (EDS), FedTraveler.com, August 20, 2007, available at: http://www.usitc.gov/policies/documents/PublicPIA_E-Traveller.pdf, August 20, 2007.

SORN: General Services Administration (GSA)/GOVT-4 - Contracted Travel Services Program, 41 FR 26,700, (June 3, 2009), available at: http://edocket.access.gpo.gov/2009/pdf/E9-12951.pdf.

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, Web-IFMIS does not use information from commercial sources, nor does it use publicly available data.

2.4 Discuss how accuracy of the data is ensured.

FEMA provides specific training on the different Web-IFMIS modules to users as a means of ensuring the accuracy of data entry and the proper interpretation of on-line data and printed reports. Web-IFMIS also employs business rules throughout the system to verify the accuracy of the transactions and ensure reconciliation of financial data.

Treasury payments also cross-reference the total account balances to ensure the accounting records are accurate. Web-IFMIS accountants further verify and ensure the integrity of the financial data and the system is subject to quarterly audits.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that Web-IFMIS may receive more information than is needed to provide accounting of financial status.

Mitigation: FEMA mitigates this privacy risk through training, education, and awareness programs associated with Web-IFMIS and through financial policies and procedures that dictate employees use only information that is relevant and necessary to provide accounting of financial status.

Privacy Risk: There is a privacy risk that Web-IFMIS could collect/use erroneous or inaccurate information.

Mitigation: FEMA mitigates this privacy risk because Web-IFMIS relies on the source systems to ensure the accuracy of the information Web-IFMIS pulls. The source systems collect directly from individuals who have been provided notice of the uses of the system and therefore are likely to provide accurate information. No additional information is collected on paper or verbally.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

Web-IFMIS uses information pulled from various subsystems (see section 5.1 for a listing of modules) in order to make payments to entitled groups (grantees), FEMA employees for payroll and travel reimbursement, as well as contractors and other vendors for payment of services. In order to facilitate payment requests received from the subsystems, Web-IFMIS will require PII (i.e., full name, address, bank account, routing number, bank information including bank name, address, and phone), to ensure the Web-IFMIS transaction is processed accurately. Treasury sends a payment by check or electronic funds transfer to the applicant using the data retained by Web-IFMIS from the subsystems. The information maintained in Web-IFMIS is also used to generate internal reports of financial activity and to respond to management requests for data.

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, the project does not use such technology.

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

FEMA's Web-IFMIS system is internal and only used by FEMA OCFO and FEMA components.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk associated with this system that too much information is disclosed to individuals without authorization.

Mitigation: FEMA mitigates this privacy risk by monitoring that the system is used only for official purposes and only by the system steward and the Information Systems Security Officer (ISSO) in conjunction with the governance information outline in this PIA. Information collected includes only those data fields necessary for the Web-IFMIS.

Section 4.0 Notice

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

Web-IFMIS does not collect information directly from individuals; the information is pulled by Web-IFMIS from subsystems described in section 2.2. However, notice is provided to the individual at the subsystem point of collection through Privacy Act notices that accompany electronic or paper forms, by way of this PIA, and the SORNs described in Section 1.2 above.

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

Information in Web-IFMIS is required to make payments to individuals, entitled groups, or entities, and to account for the expenditure of public funds. Requests to opt out would be processed through the FEMA programs that operate the subsystems that interface with Web-IFMIS as described in Section 3.3 above. Once data is stored in the subsystem individuals have no opportunity to consent to its inclusion in Web-IFMIS.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a privacy risk that the individual will not have prior or existing notice of the collection.

Mitigation: FEMA mitigates this privacy risk by providing notice to individuals, entitled groups, and entities at the subsystem point of collection through Privacy Act notices that accompany electronic or paper forms, by way of this PIA, and the SORNs described in Section 1.2 above.

Section 5.0 Data Retention by the project

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

The retention periods for Web-IFMIS data are consistent with retention schedules established by NARA and Treasury. Specific retention schedules for Web-IFMIS data are based on its five modules:

Funding Module: FEMA Records Schedules GRS-5-2 and NI-311-01-2.

- Destroy 1 year after the close of the fiscal year covered by the budget.
- PERMANENT. Cut off at close of fiscal year. Retire to Federal Records Center (FRC) 2 years after cutoff. Transfer to NARA in 5-year blocks 20 years after cutoff.

Cost Posting Module: FEMA Records Schedule GRS-7-4a.

- Destroy when 3 years old.

Disbursements Module: FEMA Records Schedule GRS-5-2.

- Destroy when 2 years old.

Accounts Receivable Module: FEMA Records Schedule GRS-7-2.

- Destroy when 6 years old, 3 months after the close of the fiscal year involved.

General Ledger Module: FEMA Records Schedule GRS-7-3.

- Destroy when 6 years old, 3 months after the close of the fiscal year involved.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that PII will be retained longer in Web-IFMIS than in the source system.

Mitigation: FEMA mitigates this privacy risk by establishing a retention schedule as outlined in Section 5.1 that must be followed by each source system. FEMA's policies and procedures for expunging data, including records pertaining to approved and unapproved applications, at the end of retention period are consistent with NARA and DHS policy and guidance. The procedures are documented by the FEMA Records Officer and follow NARA's GRS guidelines for both paper and electronic copies.

Section 6.0 Information Sharing

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.

Web-IFMIS shares information with Treasury. Treasury uses the information in order to make payment requests from Treasury to grantees or vendors. Data elements include: full name, address, bank account, routing number, bank information (bank name, address, phone, etc.). This information is encrypted and transmitted electronically using the Treasury-mandated encryption software. These transmissions to Treasury occur in order for Treasury to process payments. After processing, Treasury sends a control number for each batch file to FEMA that becomes part of the records within the OCFO. FEMA finance analysts verify payments by reconciling Treasury control numbers with the payment requests to ensure and Web-IFMIS deducts the paid funds from the appropriate accounts.

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

Sharing of Web-IFMIS records is compatible with the SORNs outlined in Section 1.2 and is consistent with the published routine uses therein.

6.3 Does the project place limitations on re-dissemination?

In accordance with the Interconnection Security Agreement (ISA) between Treasury and DHS/FEMA, information shared between agencies is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with the DHS/FEMA policy regarding sensitive but unclassified (SBU) information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior written approval of Treasury Financial Management Service (FMS) and DHS/FEMA Disclosure Offices.

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

Web-IFMIS shares information with Treasury. Treasury uses the information in order to make payment requests from Treasury to grantees or vendors. Data elements include: full name, address, bank account, routing number, bank information (bank name, address, phone, etc.). This information is encrypted and transmitted electronically using the Treasury-mandated encryption software. These transmissions to Treasury occur in order for Treasury to process payments. After processing, Treasury sends a control number for each batch file to FEMA that becomes part of the records within the OCFO. FEMA finance analysts verify payments by reconciling Treasury control numbers with the payment requests to ensure accuracy and to ensure Web-IFMIS deducts the paid funds from the appropriate accounts.

As identified in the SORNs outlined in Section 1.2, requests for financial transactions within Web-IFMIS are made to the DHS/FEMA Disclosure Office, which maintains the accounting of what records were disclosed and to whom.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a privacy risk of unauthorized disclosure of the information in Web-IFMIS.

Mitigation: FEMA mitigates this privacy risk through a March 2009 ISA, between Treasury's FMS and DHS/FEMA. The data sensitivity classification is: confidentiality high, integrity high, and availability high. FMS and FEMA have agreed to the following:

FMS and the DHS/FEMA shall protect the data in order to maintain confidentiality, integrity, and availability of the data and information systems. The data and information systems will be protected in accordance with DHS Sensitive Systems Policy Directive MD4300A, the NIST SP 800-53 assigned minimum security controls, and FIPS 199 Security Categorization of both systems to ensure that the connection will be protected to the requirements of higher categorized system.

Section 7.0 Redress

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

Individuals may submit a Privacy Act (PA) or Freedom of Information Act (FOIA) request to gain access to their information within one of the subsystems outlined in Section 2.2. and request that it be corrected. Redress is provided through Web-IFMIS subsystems. When these corrections and updates are made they are automatically transferred and updated to Web-IFMIS as well.

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

Individuals may submit PA or FOIA requests to gain access to their information within one of the subsystems outlined in Section 2.2. and request that it be corrected. Redress is provided through Web-IFMIS subsystems. When these corrections and updates are made they are automatically transferred and updated to Web-IFMIS as well.

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

Individuals are notified about the procedures for correcting their information through this PIA and the SORNs listed in Section 1.2.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a privacy risk that individuals will not know how to amend the Web-IFMIS record.

Mitigation: FEMA mitigates this privacy risk because the systems listed in Section 2.2 provide information directly to Web-IFMIS and correction or redress may be made through those subsystems.

Section 8.0 Auditing and Accountability

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

The Web-IFMIS system owner and designated financial administrators are responsible for the creation of new users, assignment of roles and privileges, and Web-IFMIS user account management. Users of Web-IFMIS are identified by the establishment of a user ID providing access to the FEMA network. The security measures for Web-IFMIS user-IDs are consistent with the security controls employed by the FEMA network. No one can access Web-IFMIS outside the FEMA network. ISAAC[2] (Integrated Security and Access Control) and additional security layers in the Web-IFMIS application protects user account information and authorizes users to specific roles within the system through account replication. The OCFO also established the OCFO Internal Control Office to conduct regular reviews of

[2] For further details on ISAAC, reference the APS (Authentications and Provisioning Services) PIA.

Web-IFMIS authorized users to ensure that their access aligns with the appropriate roles in the system. Likewise, the ISSO receives and reviews daily logs including failed login attempts, database users that should be removed, and super-user activity.

In addition to the system administrator, database administrator, and developer roles, OCFO employs additional separation of duties/roles within the Web-IFMIS application to ensure against fraud, waste, or abuse. The basic objective of the Web-IFMIS separation of duties standard is to safeguard the assets of FEMA by ensuring that no single individual has the ability to complete all the Web-IFMIS data entry transactions necessary to disburse FEMA funds.

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

Annual privacy training is required of all employees and contractors who use Web-IFMIS. It is the policy of FEMA that all personnel successfully complete a Web-IFMIS training course before being granted access to Web-IFMIS. The Web-IFMIS training course must correspond with the type of access required. In addition, new users must sign the Web-IFMIS user access form, which includes user standards of behavior and user responsibilities.

FEMA has established a Web-IFMIS separation of duties standard that, in accordance with OMB Circular A-123, defines FEMA's internal control standard for user access privileges. This standard is applied to all requests for Web-IFMIS access to ensure FEMA assets are protected from fraud, waste, and misuse.

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

FEMA uses *Web-IFMIS User Access Policy and Procedure* as the instruction to establish the policy and procedures for personnel requesting access to the system as well as the procedures for terminating Web-IFMIS user access for personnel who no longer have a need to access Web-IFMIS or separate from FEMA. The instruction is applicable to all FEMA personnel in the National Capital Region, regions, and field establishments, including disaster field offices, and disaster fixed sites that have a need to access the Web-IFMIS. The provisions of the instruction also apply to employees and contractors from other agencies that require access to the Web-IFMIS while performing official duties in support of FEMA's mission.

In addition, OCFO has developed the following new standard operating procedures listed below:

- Web-IFMIS User Access;
- Web-IFMIS and PARS Emergency and Temporary Access;
- Annual Recertification of Web-IFMIS User Accounts;
- Web-IFMIS and PARS Oracle Database User Access and Termination; and
- Annual Recertification of Web-IFMIS and PARS Oracle Database User Accounts.

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?

Any Web-IFMIS system interface or information data sharing within DHS or other outside organizations will require an MOU and/or ISA reviewed by the system steward, and will be fully vetted through the FEMA IT Security Branch, FEMA Privacy Officer, and legal counsel prior to sending to DHS for a formal review.

Responsible Officials

Eric M. Leckey
Privacy Officer
Federal Emergency Management Agency
Department of Homeland Security

Approval Signature

Original signed and on file at the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security