Privacy Impact Assessment
for the

Integrated Financial Management Information System (IFMIS) Merger

DHS/FEMA/PIA-020

December 16, 2011

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

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

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 Integrated Financial Management Information System (IFMIS)-Merger system. IFMIS-Merger[1] is FEMA's official accounting and financial management system that pulls all 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 IFMIS-Merger collects, uses, maintains, retrieves, and disseminates personally identifiable information (PII) once pulled from the subsystems.

Overview

IFMIS-Merger is FEMA's official accounting and financial management system that tracks all financial transactions. IFMIS-Merger does not collect information directly from an individual (such as through a survey); the information within the system is pulled from other systems. IFMIS-Merger provides FEMA's financial managers a global view of all FEMA's financial systems. IFMIS-Merger utilizes information provided through these various subsystems 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. IFMIS-Merger is also used to account for the expenditure of public funds as mandated under the 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, IFMIS-Merger is comprised of various modules. IFMIS-Merger collects information on grantees, payrollers, employee travelers, contractors and vendors. To account for expenditures, IFMIS-Merger generates report invoices, payment receipts, cash receipts, commitments, obligations, receiving reports, expenditures and advanced charges.

IFMIS-Merger 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 IFMIS-Merger to correspond with the funding appropriated by Congress and approved by OMB. FEMA program offices then request allocation of funds, via IFMIS-Merger's subsystems, as part of FEMA's annual and ongoing budgeting, financial, and accounting processes.

---

[1] Between October 1, 2009 and February 22, 2010, Grants & Training (G&T) IFMIS and the core IFMIS system were both operational and used to process FEMA financial data. On February 23, 2010, FEMA transitioned the functionalities and data of G&T IFMIS to the core IFMIS system, and suspended further use of G&T IFMIS. The merged system was renamed IFMIS-Merger instead of IFMIS as it is technically regarded as a new system for FISMA compliance purposes.

FEMAs OCFO receives funding requests from the various program offices and they process 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 IFMIS-Merger 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. Vendor accounts are established based on PII including name and a unique identifier (e.g., social security number, employer identification number, etc.). Once funding is appropriated and committed and the proper vendor accounts are established, FEMA is now able to process payments and 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 IFMIS-Merger and transmit an electronic and encrypted file to the Department of the Treasury (DTR) on a daily basis. DTR 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 DTR control numbers with the payment requests and IFMIS-Merger 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 DTR guidance, regulations, and DHS and FEMA policies:

- Debt Collection Act of 1996;
- Federal Claims Collection Act, 31 U.S.C. § 3711, et. seq.;
- 31 C.F.R. part 370;
- Federal Records Act, 44 U.S.C. §§ 2901 et. seq., and chapters 21, 25, 31, and 33 of this title, 44 U.S.C. §§ 2101 et. seq., 3101 et seq., and 3301 et seq.;
- Robert T. Stafford Disaster Relief and Emergency Assistance Act (Public Law 100-707);
- Homeland Security Act of 2002 (Pub. L. 107-296);
- Federal Managers' Financial Integrity Act of 1982 (Pub. L. 97-255);
- Chief Financial Officers Act of 1990 (Pub. L. 101-576);
- Federal Financial Management Improvement Act of 1996 (Pub. L. 104-208);
- Executive Order 9397;
- Executive Order 121072;
- 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-007 Accounts Payable System of Records, 73 FR 61880, October 17, 2008.
- DHS/ALL-008 Accounts Receivable System of Records, 73 FR 61885, October 17, 2008.
- DHS/ALL-019 Payroll, Personnel, Time, and Attendance Records, 73 FR 63172, October 23, 2008.
- DHS/FEMA-004 Grant Management Information Files, 74 FR 39705, August 7, 2009.
- DHS/FEMA-008 Disaster Recovery Assistance Files, 74 FR 48763, September 24, 2009.
- DHS/FEMA-2006-0002 National Emergency Grants Management System, 69 FR 75079, December 15, 2004.
- General Services Administration (GSA)/government-wide 4 - Contracted Travel Services Program, 41 FR 26700, June 3, 2009.

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

A Systems Security Plan (SSP) has been completed for IFMIS-Merger. IFMIS-Merger is operational and was granted an Authority to Operate (ATO) on June 3, 2011 for two years. IFMIS-Merger has a "high" categorization in accordance with FIPS 199. The IFMIS-Merger SSP complies with DHS Directive 4300A.

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

IFMIS-Merger 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.

IFMIS-Merger 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 IFMIS-Merger. 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);
- 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;
- 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?

IFMIS-Merger does not collect information directly from any individual (such as through a survey); 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.

DAIP/IAC: Disaster Assistance Improvement Program/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-012 - Disaster Assistance Improvement Plan, December 31, 2008.

> SORN: DHS/FEMA-008 - Disaster Recovery Assistance Files 74 FR 48763, September 24, 2009.

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 39705, August 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 39705, August 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 61880, October 17, 2008; DHS/ALL-008 Accounts Receivable System of Records, 73 FR 61885, October 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-004 Grant Management Information Files, 74 FR 39705, August 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-2006-0002 National Emergency Management Information System - Mitigation Electronic Grants Management System, 69 FR 75079, December 15, 2004.

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: PIA is in development.
>
> SORN: DHS/ALL-007 Accounts Payable System of Records, 73 FR 61880, October 17, 2008; DHS/ALL-008 Accounts Receivable System of Records, 73 FR 61885, October 17, 2008.

NFC: Payroll/Personnel Systems is the online database which 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 63172, October 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)/Government-wide 4 - Contracted Travel Services Program, 41 FR 26700, 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, IFMIS-Merger does not use information from commercial sources, nor does it use publicly available data.

2.4 Discuss how accuracy of the data is ensured.

Specific training on the different IFMIS-Merger modules is provided to

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

DTR payments also cross-reference the total account balances to ensure the accounting records are accurate. IFMIS-Merger 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 risk that IFMIS-Merger may receive more information than is needed to provide accounting of financial status.

Mitigation: IFMIS-Merger only receives the data elements relevant from the source systems. The source systems collect directly from individual who has been provided notice of the uses of the system and therefore is likely to provide accurate information. No additional information is collected on paper or verbally.

Privacy Risk: One privacy risk associated with this system include collecting/using erroneous or in accurate information.

Mitigation: IFMIS-Merger relies heavily on the data quality and integrity fed to it by the independent systems outlined in Section 2.2.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

IFMIS-Merger utilizes information provided through various subsystems 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, IFMIS-Merger will require PII (i.e., full name, address, bank account, routing number, bank information including bank name, address, and phone), to ensure IFMIS-Merger transaction is processed accurately. DTR sends a payment by check or electronic funds transfer to the applicant using the data retained by IFMIS-Merger from the subsystems. The information maintained in IFMIS-Merger is also utilized 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 IFMIS-Merger system is internal and only used by FEMA OCFO and FEMA components.

3.4   <u>Privacy Impact Analysis</u>: Related to the Uses of Information

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

<u>Mitigation</u>: This privacy risk is mitigated by monitoring the use of the system for official purposes only by the system steward and the ISSO in conjunction with governance information outline in this PIA.   Information collected is only those data fields necessary for the IFMIS-Merger.

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.

IFMIS-Merger does not collect information directly from individuals; the information is pulled by IFMIS-Merger from subsystems described in section 2.2. However, notice is provided to the public with respect to records maintained in IFMIS-Merger 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 IFMIS-Merger 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 which operate the subsystems that interface with IFMIS-Merger as described in Section 3.3 above.

4.3   <u>Privacy Impact Analysis</u>: Related to Notice

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

<u>Mitigation</u>: This privacy risk is mitigated by providing notice to individuals, entitled groups, and entities by way of this PIA which also covers the associated PIAs and SORNs in Section 1.2.

<u>Privacy Risk</u>: Privacy risks associated with this system includes having no PIA documentation conducted on some of the systems.

<u>Mitigation</u>: The privacy risk is mitigated by FEMA privacy and program managers completing PIAs and SORNs on systems without privacy assessments identifying the need to collect PII and addressing all risks and mitigations.

Section 5.0 Data Retention by the project

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

The data in the system is considered to be federal government records that ties to each individual subsystem listed in Section 2.2 that feeds IFMIS-Merger. Pursuant to OMB Circular A-130, electronic records are given the same validity as paper-based records. The retention periods for IFMIS-Merger data are consistent with retention schedules established by NARA and DTR. Specific retention schedules for IFMIS-Merger data are based on its five modules:

<u>Funding Module</u>: 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.

<u>Cost Posting Module</u>: FEMA Records Schedule GRS-7-4a.
- Destroy when 3 years old.

<u>Disbursements Module</u>: FEMA Records Schedule GRS-5-2.
- Destroy when 2 years old.

<u>Accounts Receivable Module</u>: FEMA Records Schedule GRS-7-2.
- Destroy when 6 years old, 3 months after the close of the fiscal year involved.

<u>General Ledger Module</u>: 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: Privacy risks associated with this system includes PII being retained for longer than necessary in IFMIS-Merger than in the source system.

Mitigation: The privacy risk is mitigated 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.

IFMIS-Merger shares information with DTR. DTR uses the information in order to make payment requests from DTR 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 utilizing the DTR-mandated encryption software. These transmissions to DTR occur in order for DTR to process payments. After processing, DTR sends a control number for each batch file to FEMA which becomes part of the records within the OCFO. FEMA finance analysts verify payments by reconciling DTR control numbers with the payment requests to ensure and IFMIS-Merger 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 IFMIS-Merger records is compatible with the SORNs outlined in Section 1.2 and is only done consistent with the published routine uses therein which are also compatible with the purpose collection.

6.3 Does the project place limitations on re-dissemination?

In accordance with the Interconnection Security Agreement (ISA) between DTR and DHS/FEMA, information shared between agencies is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS/FEMA policy relating to 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 DTR FMS and DHS/FEMA Disclosure Offices.

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

IFMIS-Merger shares information with DTR. DTR uses the information in order to make payment requests from DTR 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 utilizing the DTR-mandated encryption software. These transmissions to DTR occur in order for DTR to process payments. After processing, DTR sends a control number for each batch file to FEMA which becomes part of the records within the OCFO. FEMA finance analysts verify payments by reconciling DTR control numbers with the payment requests to ensure and IFMIS-Merger deducts the paid funds from the appropriate accounts.

As identified in the SORNs outlined in Section 1.2, requests for financial transactions within IFMIS-Merger are made to the DHS/FEMA Disclosure Offices who 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 associated with this system that includes unauthorized disclosure of the information in IFMIS-Merger.

Mitigation: The privacy risk is mitigated through a March 2009 Interconnection Security Agreement (ISA), between DTR's FMS and DHS/FEMA. The data sensitivity classification for 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 IFMIS-Merger subsystems. When these corrections and updates are made they are automatically transferred and updated to IFMIS-Merger 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 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 IFMIS-Merger subsystems. When these corrections and updates are made they are automatically transferred and updated to IFMIS-Merger as well.

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

Individuals are notified through this PIA as well as the SORNs listed in Section 1.2 of how to correct their information.

7.4 <u>Privacy Impact Analysis</u>: Related to Redress

Privacy Risk: There is a privacy risk associated with this system that includes individuals not knowing that if a correction or redress action must be made that IFMIS-Merger needs to be amended.

Mitigation: The FEMA systems listed in Section 2.2 provide direct information to IFMIS-Merger 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 IFMIS-Merger system owner and those financial administrators designated are responsible for the creation of new users, assignment of roles and privileges, and IFMIS-Merger user account management. Users of IFMIS-

Merger are identified by the establishment of a user ID providing access to the FEMA network. The security measures for IFMIS-Merger user-IDs are consistent with the security controls employed by the FEMA network. No one can access IFMIS-Merger outside the FEMA network. Protection of user account information is through the FEMA network administration and the additional security layer in the IFMIS-Merger application that authenticates users to specific roles. The OCFO also established the OCFO Internal Control Office to conduct regular reviews of IFMIS-Merger authorized users to ensure 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 IFMIS-Merger application to ensure against fraud, waste, or abuse. The basic objective of the IFMIS-Merger separation of duties standard is to safeguard the assets of FEMA by ensuring that no single individual has the ability to complete all the IFMIS-Merger 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 IFMIS-Merger. It is the policy of FEMA that all personnel successfully complete an IFMIS-Merger training course before being granted access to IFMIS-Merger. The IFMIS-Merger training course must correspond with the type of access required. In addition, new users must sign the IFMIS-Merger user access form which includes user standards of behavior and user responsibilities.

FEMA has established an IFMIS-Merger 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 IFMIS-Merger 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 *IFMIS-Merger User Access Policy and Procedure* is used as the instruction to establish the policy and procedures for personnel requesting access to the system as well as the procedures for terminating IFMIS-Merger user access for personnel who no longer have a need to access IFMIS-Merger 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 IFMIS-Merger. The

provisions of the instruction also apply to employees and contractors from other agencies that require access to the IFMIS-Merger while performing official duties in support of FEMA's mission.

In addition, OCFO has developed the following new SOPs listed below:

- IFMIS User Access;
- IFMIS and PARS Emergency and Temporary Access;
- Annual Recertification of IFMIS-Merger User Accounts;
- IFMIS and PARS Oracle Database User Access and Termination; and
- Annual Recertification of 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 IFMIS-Merger 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 copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security