Department of Homeland Security
Office of Inspector General

Federal Emergency Management Agency Privacy Stewardship

OIG-13-87

May 2013

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

May 1, 2013

MEMORANDUM FOR: Richard Serino
Deputy Administrator
Federal Emergency Management Agency

FROM: Frank Deffer
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Federal Emergency Management Agency Privacy Stewardship*

Attached for your action is our final report, *Federal Emergency Management Agency Privacy Stewardship*. We incorporated the formal comments from the Federal Emergency Management Agency in the final report.

The report contains four recommendations aimed at improving privacy stewardship within the Federal Emergency Management Agency. Your office concurred with all recommendations. As prescribed by the Department of Homeland Security Directive 077-1, Follow-Up and Resolutions for the Office of Inspector General Report Recommendations, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

Consistent with our responsibility under the *Inspector General Act*, we are providing copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Marj Leaming, Director, System Privacy Division, at (202) 254-4172.

Attachment

Table of Contents

Appendixes

Abbreviations

CIO	Chief Information Officer
DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
FEKC	FEMA Employee Knowledge Center
FISMA	*Federal Information Security Management Act of 2002*
IT	information technology
NEMIS	National Emergency Management Information System
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	personally identifiable information
PIA	privacy impact assessment
PTA	privacy threshold analysis
SORN	system of records notice
TAFISMA	Trusted Agent *Federal Information Security Management Act*

Executive Summary

We performed an audit of the Federal Emergency Management Agency's (FEMA) privacy stewardship. Our audit objectives were to determine whether FEMA's plans and activities instill a culture of privacy that protects sensitive personally identifiable information and whether FEMA ensures compliance with Federal privacy laws and policies.

FEMA has made progress in implementing plans and activities to instill a culture of privacy. Specifically, it has established a privacy office that, among other functions, prepares reports on FEMA's privacy activities to the Department of Homeland Security Privacy Office, reviews suspected privacy incidents, and oversees FEMA's privacy training. However, FEMA faces a number of challenges in ensuring that personally identifiable information is protected. Specifically, it needs an accurate inventory of its information technology systems that impact privacy. In addition, FEMA needs to complete required privacy compliance analyses, including privacy threshold analyses, privacy impact assessments, and system of records notices, for 430 information technology systems that were reported as unauthorized.

FEMA also must address challenges with protecting personally identifiable information at disaster relief sites. Specifically, FEMA needs to conduct privacy assessments at disaster relief sites to improve accountability, identify risks, and implement appropriate privacy safeguards for the protection of personally identifiable information collected during field operations. In addition, FEMA needs to provide specialized field training to the disaster relief workforce, including procedures on properly collecting and handling personally identifiable information from applicants immediately after a disaster.

Finally, although FEMA has implemented a standardized privacy training course, it does not have an effective system to enforce the employee training requirement. We are making four recommendations to FEMA, which if implemented, should improve privacy stewardship and enhance protection of personally identifiable information.

Background

The *Privacy Act of 1974* (*Privacy Act*), as amended, imposes various requirements on agencies whenever they collect, use, maintain, or disseminate personally identifiable information (PII) in a system of records.[1] The Department of Homeland Security (DHS) defines PII as any information that permits an individual to be identified directly or indirectly from any information that can be linked to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the United States, employee, or contractor to the Department. Federal laws, regulations, policies, and guidelines set the minimum standards for handling PII. Appendix C lists requirements related to FEMA's privacy stewardship.

To accomplish its mission to prepare for, prevent, respond to, and recover from domestic disasters and emergencies, FEMA collects, uses, maintains, or disseminates significant amounts of PII daily. FEMA has more than 7,300 full-time employees at Headquarters, 10 regional offices, 3 national processing service centers, 2 mail processing centers, and additional sites across the country. FEMA also has more than 10,400 temporary employees who are available for deployment to disaster areas, as needed. Figure 1 lists three key purposes for which FEMA collects PII from the public.

Figure 1. Key Purposes for Collection of Personally Identifiable Information

Purposes for Collection	From Whom or What	PII That May Be Collected
Flood Insurance	Flood insurance applicants, agents, policy holders, and companies	Name, information on insurance claims, building contents, and payments
Grants	State, territorial, and tribal officials; port and transit authorities; nonprofit organizations; and companies	Grant information, organization name, bank routing and account number, Social Security or employer identification number, point of contact's work and email addresses, and numbers for work phone, cell phone, and fax
Disaster Recovery Assistance	Individuals	Name, address, Social Security number, birth date, phone, disaster-related damage information, insurance information, and financial information

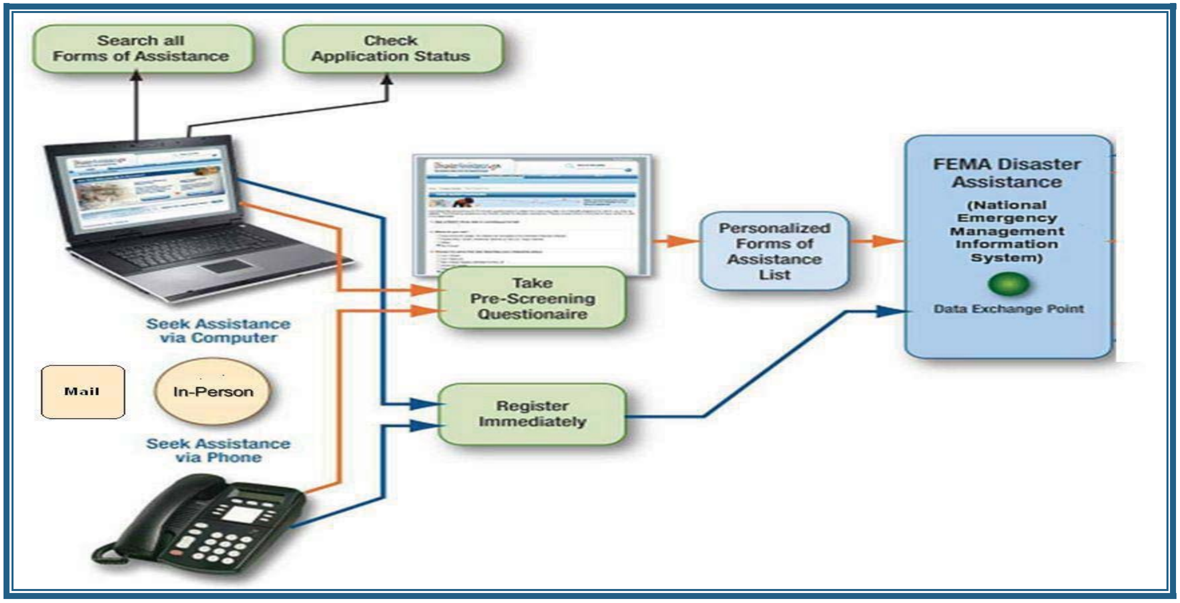
Source: FEMA Privacy Impact Assessments

Through its disaster assistance application process, FEMA collects PII from applicants each year. For example, more than 1,500,000 disaster applicants completed the registration process in 2008. Following Hurricane Katrina, FEMA collected PII from more than 2,000,000 applicants. Figure 2 illustrates the flow of applicant PII in the disaster assistance application process. FEMA sends applicant PII to the National Emergency Management Information System (NEMIS), an information technology (IT) system that

[1] A system of records is a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual.

supports disaster response and recovery operations. NEMIS maintains the PII of more than 2,000,000 current applicants.

Figure 2. Flow of PII in FEMA's Disaster Assistance Application Process


Search all Forms of Assistance
Check Application Status
Seek Assistance via Computer
Mail
In-Person
Seek Assistance via Phone
Take Pre-Screening Questionaire
Register Immediately
Personalized Forms of Assistance List
FEMA Disaster Assistance
(National Emergency Management Information System)
Data Exchange Point

Source: OIG analysis of FEMA process

Workers deployed to disaster relief sites help survivors by empathizing with them, explaining available disaster relief programs, and listening carefully to understand their needs. Workers collect applicant PII to register them for essential services and discuss their case status. Figure 3 shows the variety of environments where FEMA conducts disaster relief operations.

Figure 3. Environments for Disaster Response and Recovery

Source: FEMA

An agency's culture of privacy reflects the extent to which its executives, managers, and employees understand, implement, and enforce its commitment to protect privacy and comply with legislative and DHS mandates. The promotion of an effective culture of privacy leads to shared attitudes, goals, and practices that comply with the requirements for proper handling of PII. The Privacy Office assists system and program managers in conducting reviews to identify privacy risks related to their specific processes and implementing an appropriate privacy stewardship framework.[2] This framework includes management accountability, physical or IT safeguards, specialized privacy training, as well as coordination among privacy, legal counsel, IT, and records management services.

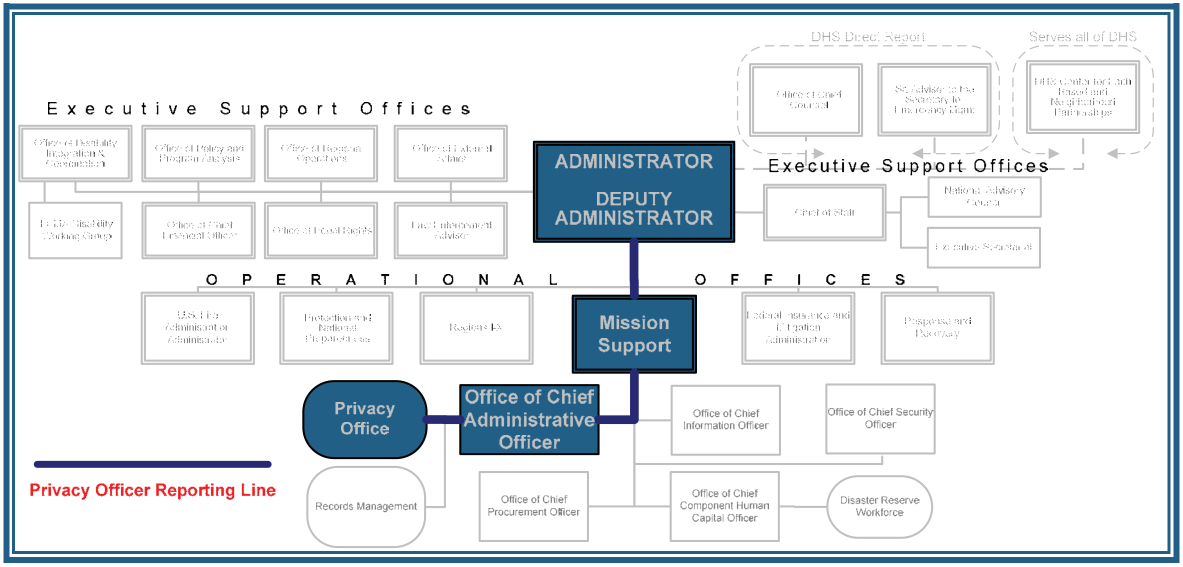
According to the Federal Chief Information Officer (CIO) Council, *Best Practices: Elements of a Federal Privacy Program*, protecting privacy is a core consideration for every Federal agency, and it is best achieved when it is an integral part of the agency's business operations.[3] Privacy must be considered as part of policy assessment, programmatic decision-making, and business operations; privacy should not be an afterthought. The agency's managers monitor and enforce Federal privacy laws and policies to establish effective privacy oversight.

[2] In this report, "system and program manager" refer to the agency employee who is responsible for the operation and management of the system to which a System of Records Notice pertains. IT system managers, and program managers are responsible for preparing privacy compliance documentation for technologies, rulemakings, programs, and activities. These managers may be located at FEMA headquarters, regions, or disaster relief sites.

[3] The Privacy Committee of the Federal Chief Information Officer Council improves agency practices for the protection of privacy, serving as the interagency coordination group for Senior Agency Officials for Privacy and Chief Privacy Officers in Federal Government. The Privacy Committee has five subcommittees: Best Practices, Innovation and Emerging Technology, International, Identity Management, and Development and Education. The Best Practices Subcommittee is a forum to develop and promote best practices for Federal privacy programs and policies.

On June 5, 2009, the DHS Deputy Secretary issued the *DHS Memorandum Designation of Component Privacy Officers*, which directed 10 components, including FEMA, to designate a senior-level Federal employee as a full-time Privacy Officer who reports directly to the component head. FEMA has designated a full-time Privacy Officer. The present location of the Privacy Office is in the Office of the Chief Administrative Officer. Figure 4 shows how the Privacy Officer reports through the Headquarters Mission Support Bureau to the FEMA Administrator.

Figure 4. FEMA Privacy Office Placement


DHS Direct Report
Serves all of DHS
Office of Chief Counsel
Sr. Advisor to the Secretary for Emergency Mgmt
DHS Center for Faith Based and Neighborhood Partnerships
Executive Support Offices
Office of Disability Integration & Coordination
Office of Policy and Program Analysis
Office of Regional Operations
Office of External Affairs
FEMA Disability Working Group
Office of Chief Financial Officer
Office of Equal Rights
Law Enforcement Advisor
ADMINISTRATOR
DEPUTY ADMINISTRATOR
Executive Support Offices
Chief of Staff
National Advisory Council
Executive Secretariat
OPERATIONAL OFFICES
U.S. Fire Administrator Administrator
Protection and National Preparedness
Regions I-X
Mission Support
Federal Insurance and Mitigation Administrator
Response and Recovery
Privacy Office
Office of Chief Administrative Officer
Office of Chief Information Officer
Office of Chief Security Officer
Privacy Officer Reporting Line
Records Management
Office of Chief Procurement Officer
Office of Chief Component Human Capital Officer
Disaster Reserve Workforce

Source: OIG analysis of FEMA organizational chart

Results of Audit

Efforts To Improve Privacy Stewardship

FEMA has made progess in developing a culture of privacy and addressing compliance with privacy requirements. FEMA established its Privacy Office in 2006. In 2011, the Privacy Officer reorganized staff assignments to promote information sharing with staff and other mission support areas, such as legal counsel, IT, and records management. The Privacy Office supports key projects, such as the Identity Theft Project and the Social Media Program.

Privacy Office staff perform their responsibilities in accordance with DHS Management Instruction 047-01-001, *Privacy Policy and Compliance.* (See appendix D for a list of all privacy office duties.) Key responsibilities include the following:

- Provide reports on FEMA's privacy activities and accomplishments to the DHS Privacy Office for reporting to Congress or the Office of Management and Budget (OMB);

- Review suspected and confirmed privacy incidents, provide an analysis of ways to minimize the loss of PII, evaluate the reasonable risk of harm, and ensure that privacy incidents have been properly mitigated, consistent with DHS Privacy Office *Privacy Incident Handling Guidance*;[4]

- Provide updates on the status of FEMA's privacy management to the DHS Privacy Office, pursuant to the *Federal Information Security Management Act of 2002* (FISMA);[5]

- Advise managers on information sharing that involves the receipt or disclosure of PII;

- Oversee FEMA privacy training and provide educational materials consistent with mandatory and supplementary training developed by the DHS Privacy Office; and

[4] A privacy incident is the loss of control, compromise, or situations in which persons other than authorized users have access or potential access to PII in usable form, whether physical or electronic, or in which authorized users access PII for an unauthorized purpose.

[5] The *Federal Information Security Management Act of 2002* directs agencies to identify security and privacy risks inherent in their systems, develop ways to mitigate those risks, and report to OMB the results of ongoing system assessments.

- Coordinate with system and program managers, together with the DHS Privacy Office and FEMA counsel, to complete privacy compliance analyses and documentation for systems of records to meet the requirements of the *Privacy Act.*

The FEMA Privacy Office has a plan and schedule to complete privacy compliance analyses for the 74 IT systems that have documented authorization to operate. The compliance process begins with a privacy threshold analysis (PTA), a required document that serves as the official determination by the DHS Privacy Office as to whether a Department program or system has privacy implications. Based on the results of the PTA, additional privacy compliance documentation may be required, such as a privacy impact assessment (PIA) and system of records notice (SORN). As of May 2012, 46 of the 74 (62 percent) IT systems had PTAs. The FEMA Privacy Office had improved its privacy scores for the systems holding PII from 80 percent in July 2011 to 97 percent in July 2012, by having a PIA for 37 of the required 38 (97 percent) systems that required additional privacy analysis. A PIA is a decision-making tool used to identify and mitigate privacy risks at the beginning of and throughout the development life cycle of a program or system. It helps the public understand what PII the Department is collecting; why it is being collected; and, how it will be used, shared, accessed, and stored.

In addition, FEMA published SORNs in the *Federal Register* to address 45 systems with PII. A SORN is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by the Department. FEMA’s SORNs and PIAs are also available on the DHS Privacy Office’s public website. (Appendix E contains the names and compliance status of the systems that affect privacy.) However, as discussed in the following sections, FEMA continues to face challenges in identifying a complete inventory of PII holdings and ensuring that it is protecting PII component-wide.

FEMA Needs To Address Compliance With Privacy Requirements

FEMA needs to take additional measures to ensure that PII is protected. At least 430 recently identified rogue or unauthorized IT systems are neither in FEMA’s inventory nor in compliance with both Federal privacy and security laws and policies.[6] The Office of the Chief Information Officer (OCIO), as well as system and program managers, need to coordinate with the Privacy Office to plan and conduct necessary PTAs, PIAs, and SORNs to meet privacy requirements. By not ensuring privacy compliance of IT systems, FEMA may be placing PII at unnecessary risk.

IT Systems Inventory Is Not Complete

FEMA is hindered in meeting its privacy compliance requirements because it does not have an accurate inventory of its IT systems. According to OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (OMB M-07-16), agencies are required to review their holdings of all PII and ensure that they are accurate, relevant, timely, and complete.[7] FEMA uses a software application, Trusted Agent Federal Information Security Management Act (TAFISMA), to track its inventory of electronic PII holdings, including the 38 authorized IT systems that have been identified as having impacted privacy.[8]

However, FEMA's TAFISMA inventory is incomplete. All holdings of PII have not been identified, documented, or authorized. Because there are unauthorized IT systems in operation that may not comply with Federal privacy and IT security laws and policies, FEMA is at risk of both Federal privacy and IT security laws and policies. Specifically, as of April 2012, at least 430 IT systems had been reported to the OCIO as unauthorized, in response to the *Unauthorized Information Technology Systems Memorandum*, dated March 2012. (See appendix F.) This memorandum directed all FEMA offices to report to the OCIO any systems that were in development or operating without government authority. We reviewed detailed reports on a sample of 226 of these unauthorized IT systems, which appeared to function as 170 administrative systems, 36 financial systems, and 20 program-related systems. These other systems support the following programs: the Federal Insurance and Mitigation Administration, United States Fire Administration, Protection and National Preparedness, and the Office of

[6] FEMA's *Unauthorized Information Technology Systems Memorandum* (dated March 13, 2012) characterizes rogue systems as those IT systems that are not properly documented and approved to operate by the Chief Information Officer and unauthorized systems as those IT systems that do not possess a recognized Federal Government certification and accreditation. For this report, we use "unauthorized" to refer to either rogue or unauthorized systems.

[7] IT systems, programs, technologies, pilot projects, information sharing, records, and rule-making may impact privacy or hold PII.

[8] The DHS Office of the Chief Information Officer uses TAFISMA as its software application to track major IT systems and general support systems, including those that affect privacy. TAFISMA contains privacy and IT security compliance documentation.

Response and Recovery. The FEMA OCIO and Privacy Officer will need a process to ensure that a timely review of privacy status can be made.

In May 2012, system and program managers had not provided the Privacy Office with essential information in a timely manner so that the office could assist them with initial privacy compliance analysis and determination. In addition, the Privacy Officer requested information from the OCIO on all unauthorized IT systems. This information is necessary for the Privacy Office to begin privacy compliance analyses. As of August 2012, the Privacy Officer had not received the information because OCIO was reviewing the 430 unauthorized IT systems to determine whether each system was a duplicate, a subsystem, an application already recorded in TAFISMA, or a temporary data extract that could be decommissioned or deleted. However, when we asked what would be a more timely solution, the FEMA CIO and Privacy Officer recommended that they address the unauthorized systems in tandem and resolve the various compliance issues posed by them.

Privacy Threshold Analyses for Unauthorized IT Systems

The DHS Privacy Office requires the completion of a PTA, using its template, when components propose new systems of records or make significant changes to existing systems.[9] The PTA must be updated every 3 years. The DHS template for a PTA will guide the analysis to determine the extent to which each of the newly identified IT systems impacts privacy. Then, system and program managers must coordinate PTA preparation with the FEMA Privacy Office. The DHS Privacy Office will review each PTA to determine the type of information it contains, the extent to which it impacts privacy, whether it requires a PIA, and whether an existing or new SORN is required.

Privacy Impact Assessments for Unauthorized IT Systems That Affect Privacy

DHS components must conduct PIAs of all systems that collect, use, maintain, or disseminate PII, consistent with the *E-Government Act of 2002*. According to *DHS Privacy Office Policy Guidance Memorandum 2008-02*, the completion of the DHS template for a PIA requires analysis, including that of technologies employed, life cycle of the PII in the system, and specific privacy risks and their mitigation.

[9] The privacy threshold analysis establishes the intended purpose of the system, identifies the system owner, and proposes types of PII collected and maintained by the system, such as the presence of Social Security numbers.

The FEMA Privacy Office estimates that it may need 4 to 6 weeks to assess each of those unauthorized IT systems that the DHS Privacy Office determines will require a PIA. The assessment will necessitate comments and analysis by system and program managers, legal counsel, OCIO, and the Headquarters Mission Support Bureau, as well as its workers in each of the 10 regions who perform onsite services for IT, acquisitions, security, and records management. Staff from external agencies may be involved, such as the DHS Privacy Office's compliance division, agencies that receive or share PII with FEMA, or OMB.[10]

System of Records Notices for Unauthorized IT Systems

The *Privacy Act* requires agencies to issue a public notice for every system of records under their control. Based on a review of the PTAs, the DHS Privacy Office determines which of the unauthorized IT systems will require a new SORN or will be covered by an existing SORN.

The FEMA Privacy Office estimates that it may take 4 to 6 weeks to complete each SORN that will be required for the identified unauthorized IT system. The review will require information from system and program managers, legal counsel, OCIO, and the Headquarters Mission Support Bureau. Also, staff from the DHS Privacy Office and DHS Office of General Counsel will be involved.

Recommendation

We recommend that the Deputy Administrator of FEMA:

Recommendation #1:

Implement a plan and timeline to identify and assess 430 unauthorized systems, and complete appropriate documentation to mitigate privacy risks in the unauthorized systems that contain PII.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Associate Administrator of FEMA's Office of Policy, Program Analysis and International Affairs. (See appendix B.)

[10] OMB clearance under the *Paperwork Reduction Act of 1995* (44 U.S.C. 3501 et seq.) is required for FEMA to conduct federally sponsored data collections involving 10 or more respondents unless an exemption applies. The general purpose of the *Paperwork Reduction Act* is to minimize the paperwork burden created by the Federal Government in collecting information.

FEMA concurred with our findings and recommendation #1. FEMA's Office of Chief Information Officer confirmed that it is making progress with its review of the unauthorized systems and is anticipating that less than 430 unauthorized systems will need to undergo further privacy compliance analysis and documentation. We consider this recommendation open and unresolved.

Privacy Protection Weak at Disaster Relief Sites

FEMA has not taken adequate steps to mitigate privacy risks to PII collected at its disaster relief sites. During our audit, we identified instances in the disaster assistance process where applicant PII was vulnerable at all 24 disaster relief sites that we visited in Alabama, California, Georgia, Indiana, Kentucky, Maryland, Texas, and Virginia. (See appendix A for details about the sites.) To address these vulnerabilities, FEMA needs to conduct privacy assessments at disaster relief sites. It also needs to provide specialized field training for disaster workers who handle PII.

Privacy Safeguards Needed

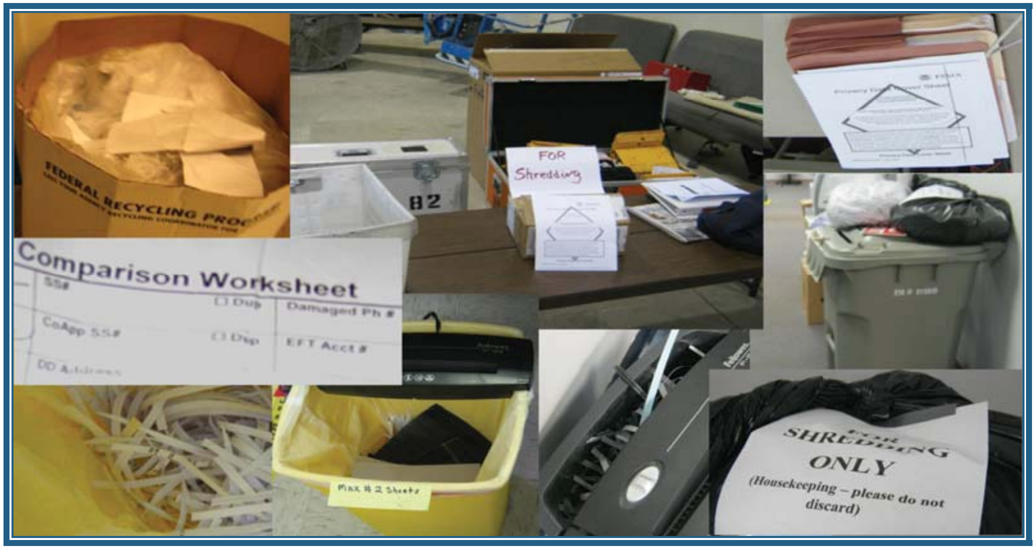
The *Privacy Act* requires agencies to implement technical, physical, and administrative safeguards to ensure the security and confidentiality of records. These safeguards also should protect against any anticipated threats or hazards that could result in substantial harm to individuals from whom information is collected. Specifically, PII could be compromised when it was overheard when applicants talked to disaster workers in person or over the telephone, or when PII was entered into laptops that do not have encryption software, left unsecured in stacks of paper awaiting application processing, and disposed of by using improper equipment. We identified the lack of the following privacy safeguards during our visits to 24 disaster relief sites:

- **IT Safeguards**: Regional IT managers and specialists are responsible for deploying encryption software to the laptops that are used at disaster relief sites. They estimated that less than 25 percent of the laptops that disaster workers used to collect PII had encryption software. We also observed that the laptops at 17 of 24 disaster relief sites did not have encryption software installed. Even if encryption software was installed, disaster workers do not always encrypt email attachments that contain PII. For example, a contractor emailed an unencrypted spreadsheet of 5,070 applicants' PII to an unintended recipient's email address. The PII included full names, addresses, and insurance payout amounts for applicants participating in the National Flood Insurance Program. The contractor later received training on encrypting email attachments, and the Privacy Office worked with the field office to notify the affected applicants.

Further, at all 24 sites, we observed instances of disaster workers not securing their laptops when stepping away from them. During a 3-year period (2010 to 2012), FEMA reported that 73 laptops were either stolen or lost; PII on these laptops could be stolen, lost, or compromised.

- **Physical Safeguards**: At all 24 disaster relief sites, we observed unsecured paper copies of applicant PII awaiting disposal or entry into NEMIS. In addition, 15 of 24 disaster relief sites either lacked cabinets or had storage equipment that did not meet privacy and security requirements. Disaster workers at four sites reported taking applicant files to their hotels to safeguard PII because they did not have locked storage capacity at the sites. Further, disposal equipment at these sites did not meet privacy and security requirements, as specified by *FEMA Standard Operating Procedure: Electronic and Hard Copy Media Sanitization and Release*. Figure 5 shows examples of unsecured storage and inadequate disposal of applicant PII.

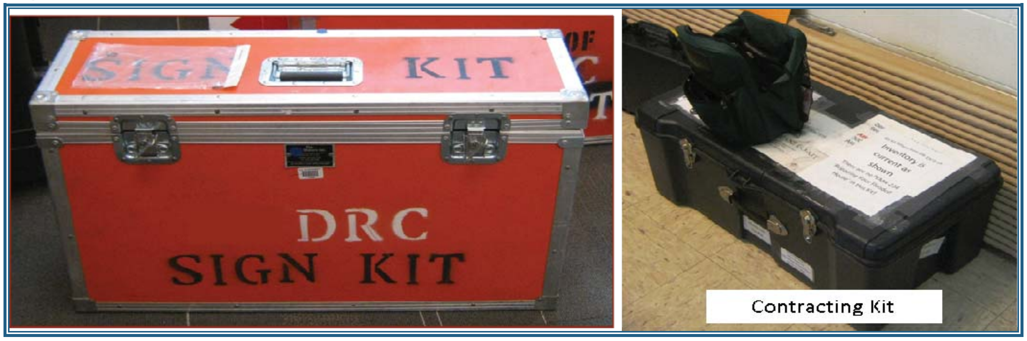
Figure 5. Inadequate Physical Safeguards at Disaster Relief Sites



Source: OIG

- **Administrative Safeguards**: Regional offices identify the location for disaster relief sites and send preassembled "Disaster Go" kits to the field managers who are setting up the sites. Each regional office customizes the content and materials that are included in the kits, based on the nature of the disaster and the particular environment of the specified disaster relief site. As shown in figure 6, the following are examples of two types of Disaster Go kits. However, regional and field managers had not considered adding pertinent privacy materials into these kits.

Figure 6. Examples of Disaster Go Kits



Source: OIG

a. Sign kits help the disaster applicants locate the FEMA disaster recovery center. However, the inclusion of some privacy-related materials would help increase awareness of the need to protect applicant PII, such as the *DHS Privacy Office's How To Safeguard Personally Identifiable Information Factsheet,* privacy posters, and instructions for workers on encrypting email attachments.

b. Contracting kits include paper copies of contract forms for use when electricity, computers, or Internet access is unavailable. However, this kit does not contain privacy clauses from FEMA or the *Federal Acquisition Regulation* that establish contractors' privacy responsibilities and accountability.

Privacy Assessments Needed at Disaster Relief Sites

Periodic privacy assessments can help managers reduce risk and build accountability for privacy compliance. Specifically, FEMA managers need to conduct privacy assessments to determine where specific privacy safeguards can be incorporated when they establish disaster relief sites and hire staff in response to a disaster. Annually, FEMA faces the challenge of protecting PII when disaster workers collect, use, maintain, or disseminate this information for more than 1,000,000 applicants under varying work conditions and environments. According to *OMB Memorandum M-12-20, FY 2012 Reporting Instructions for the*

Federal Information Security Management Act and Agency Privacy Management, agencies are required to identify and address gaps in privacy compliance, management, operational, and technical controls by conducting regular assessments. In addition, according to *The Fair Information Practice Principles at Work*, managers must build accountability into their programs through activities such as periodic reviews.[11] (See appendix G for the eight privacy principles.) Regardless of the location of the disaster relief site, which may be in a building, stadium, tent, mobile unit, or another accommodation, FEMA work processes and environments must meet privacy requirements.

Field managers whom we interviewed were concerned that the chaotic nature of the disaster response and relief work could place PII at risk, but had not considered the option of conducting a privacy assessment. For example, in 2011, cadres of temporary employees, contractors, and volunteers assisted applicants at nearly 500 disaster relief sites for periods ranging from 1 day to 3 months. However, FEMA has not conducted privacy assessments to help determine the risks and extent to which privacy protections are needed at these sites. Until field managers identify and mitigate the privacy vulnerabilities in processes, flow, and handling of applicant PII during higher risk operations and at disaster relief sites, FEMA will continue to expose PII to risk.

Specialized Field Training Needed for Disaster Relief Workforce

More than 10,400 temporary workers (disaster workers) process the PII of disaster survivors. FEMA faces challenges in protecting PII if this temporary work force has not received appropriate privacy training. Specifically, FEMA has not provided specialized field training to workers on how to protect and control applicant PII when collecting and handling it after a disaster. According to OMB M-07-16, specialized or advanced training is an effective way to improve employee understanding of privacy responsibilities in their daily work activities.

At the 24 disaster relief sites that we visited, managers explained that training for disaster workers is often not completed because there is little time between reporting for duty and when they must begin helping disaster survivors. In addition, managers noted that the standardized privacy training is web-based and Internet connectivity is not always available following a disaster. Further, according to field managers and disaster workers we interviewed, the content of

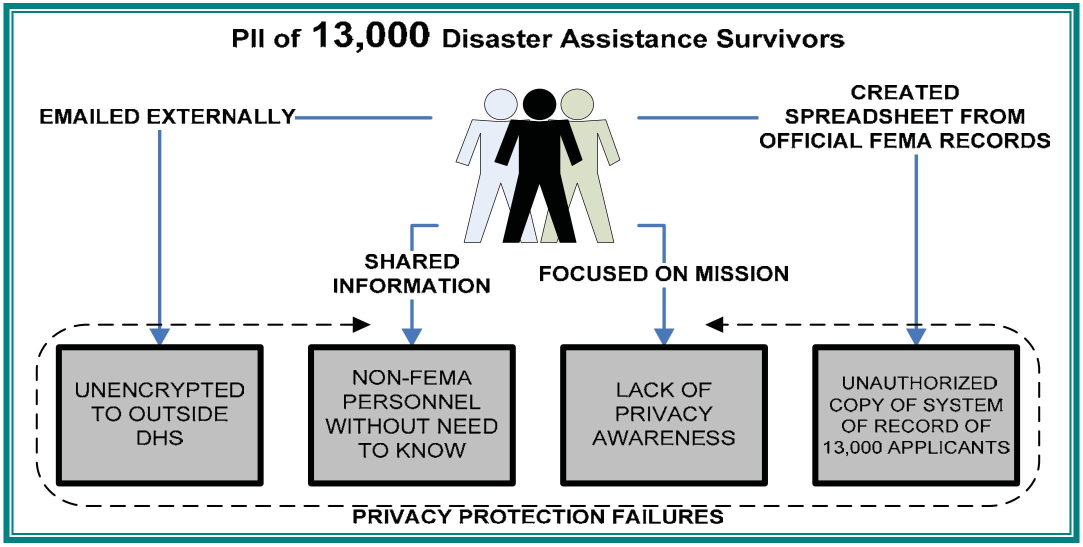
[11] *DHS Privacy Office Policy Guidance Memorandum 2008-02* requires reviews of processes, programs, IT systems, rule-making, or technologies that may impact privacy. In addition, the DHS Privacy Office also exercises its authority under Section 222 of the *Homeland Security Act* to ensure that technologies sustain and do not erode privacy protections, through the conduct of privacy compliance reviews.

standardized, FEMA-wide privacy training was too general to address the variety of conditions at disaster relief sites.

Without specialized field training, workers do not understand fully how to apply proper privacy practices and safeguards while performing services at disaster relief sites. Fifty-eight percent (103 of 177) of field managers we interviewed stated that specialized field training consistent with the *DHS Privacy Office Handbook for Safeguarding Sensitive Personally Identifiable Information* is needed to help disaster workers in protecting PII during disaster relief operations. In addition, 46 percent of survey comments from field managers and employees recommended specialized privacy training for the disaster relief workforce.[12]

When disaster workers are not adequately trained to safeguard PII while performing disaster relief operations, privacy incidents can occur. For example, as illustrated in figure 7, in October 2008, a disaster worker who had not received specialized field training on handling PII violated privacy requirements when acquiring a mailing distribution list to communicate with disaster applicants. He created an unauthorized copy of a system of records by downloading the PII of 13,000 applicants from the official database into spreadsheets. He did not encrypt the spreadsheets when he transmitted them over the Internet to an unauthorized third party, who used them to create the mailing distribution list.

Figure 7. FEMA Privacy Incident


PII of 13,000 Disaster Assistance Survivors
EMAILED EXTERNALLY
CREATED SPREADSHEET FROM OFFICIAL FEMA RECORDS
SHARED INFORMATION
FOCUSED ON MISSION
UNENCRYPTED TO OUTSIDE DHS
NON-FEMA PERSONNEL WITHOUT NEED TO KNOW
LACK OF PRIVACY AWARENESS
UNAUTHORIZED COPY OF SYSTEM OF RECORD OF 13,000 APPLICANTS
PRIVACY PROTECTION FAILURES

Source: OIG analysis of FEMA Privacy Incident Report, reported October 2008

[12] In January 2012, we emailed employees a survey on FEMA's culture of privacy that included questions on topics such as integrating privacy safeguards in daily operations. (See appendix H for the survey methodology.)

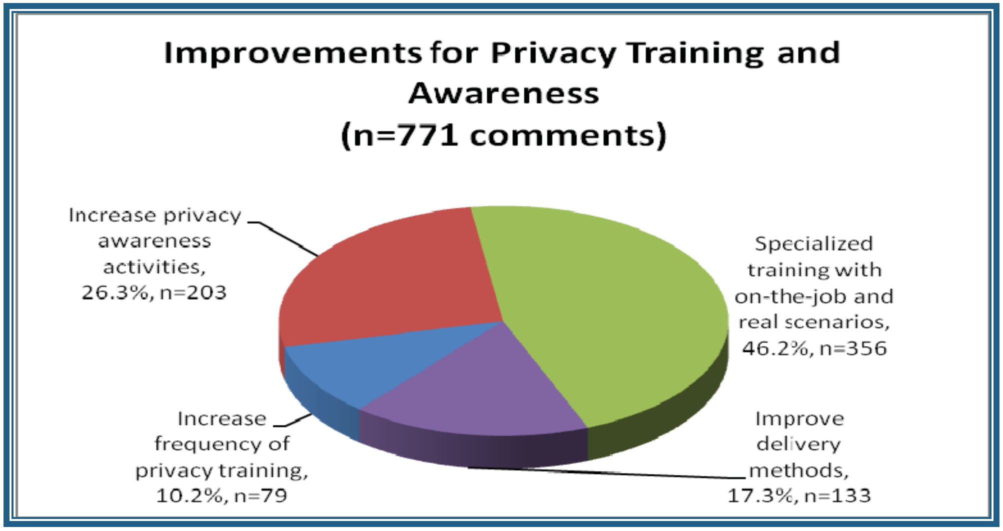
The disaster worker reported his actions as a privacy incident, but he was unable to confirm whether the third party had destroyed the spreadsheets and the mailing distribution list. After an investigation, FEMA compelled the third party to destroy the PII on his computer. FEMA issued a written reprimand to the disaster worker and required him to take additional privacy training on safeguarding PII.

In October 2012, a disaster worker caused another incident at a disaster relief site when he created a spreadsheet that contained the PII (names and Social Security numbers) of 1,000 other disaster workers and saved it on the local network. The PII was accessible to all users on the local network because the spreadsheet was not password protected. When another disaster worker opened the file and realized that the spreadsheet contained PII, he reported it as a privacy incident.

Survey Comments

We received 771 comments from survey respondents working at disaster relief sites who recommended numerous ways to make privacy training more useful and applicable to their work environments. Figure 8 presents the distribution of responses by topic.

Figure 8. Field Recommendations for Privacy Training and Awareness



Source: OIG

Field respondents to our survey indicated that specialized training and supplementary privacy awareness activities are necessary to improve current privacy training content, delivery methods, frequency, and effectiveness. The following are examples of improvements suggested by survey respondents:

- Specialized training customized to their duties, which would use realistic examples and scenarios.

- Increased privacy awareness activities, such as routine emails discussing core privacy principles and posters placed near frequently visited work areas (such as printers and file cabinets).

- Improved privacy training delivery, such as in-person training, privacy workshops, informative online videos, and videoconferencing.

- More frequent privacy training, such as scheduled, privacy-focused staff briefings and meetings related to recent projects during which supervisors incorporate practical privacy discussions.

Recommendations

We recommend that the Deputy Administrator of FEMA:

Recommendation #2:

Conduct privacy assessments of disaster relief operations to improve accountability and to meet privacy requirements.

Recommendation #3:

Implement specialized privacy training for the disaster relief workforce.

Management Comments and OIG Analysis

FEMA concurs with recommendation #2. The FEMA Privacy Officer is developing a framework for conducting privacy compliance site inspections, to include disaster relief operations. We consider this recommendation open and unresolved.

FEMA concurs with recommendation #3. The FEMA Privacy Officer is developing specialized privacy training. We consider this recommendation open and unresolved.

FEMA-wide Privacy Training and Awareness

Training and awareness activities help build an effective culture of privacy in the workplace. However, managers do not have an effective method to monitor the completion of FEMA's standardized privacy training. In addition, managers and employees suggested ways that FEMA could supplement privacy training through creative activities that reinforce employee privacy responsibilities.

Enforce Standardized, FEMA-wide Privacy Training

FEMA has implemented a standardized privacy training course, but it does not have an effective tracking system to monitor whether employees have completed the training requirement. This situation makes it difficult to enforce the privacy training requirement. *DHS Management Instruction 047-01-001, Privacy Policy and Compliance*, requires initial privacy training and annual refresher training for all managers, employees, and contractors. Although the FEMA workforce must complete the web-based course (IS-105), only 1,070 employees were reported to have completed the course. In addition, FEMA did not use the DHS Privacy Office's *Privacy at DHS: Protecting Personal Information*, which was created for department-wide implementation this year to meet the mandatory privacy training requirement. This course provides a broad overview of privacy responsibilities, privacy principles, legal requirements, and penalties.

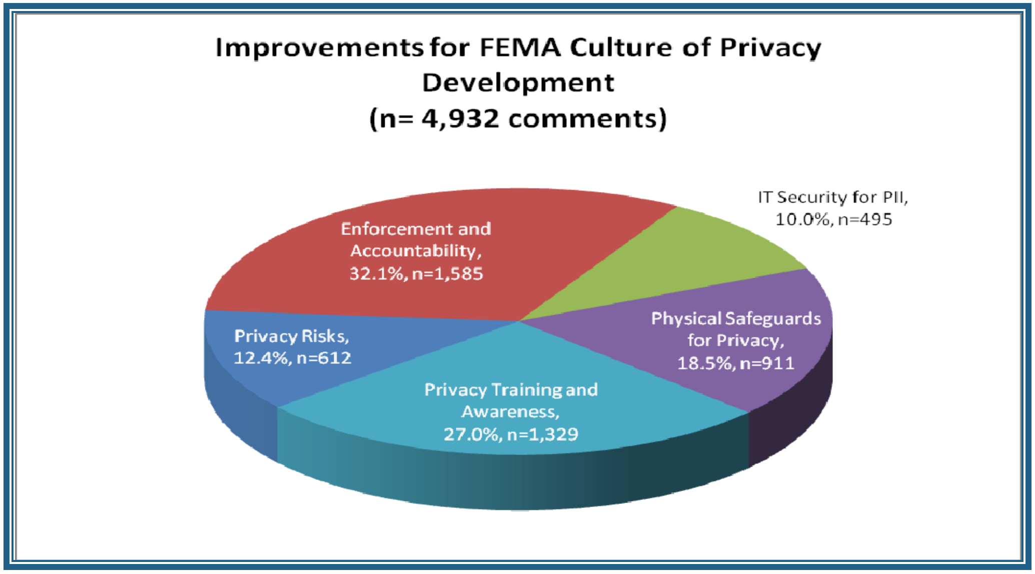
FEMA cannot efficiently identify and track employees who have not completed the required course. The Headquarters Office of Distance Learning did not purchase this capability because of budgetary constraints when it instituted the FEMA Employee Knowledge Center (FEKC) in February 2012. FEKC tracks only those who have completed the course. Therefore, to enforce the requirement, managers must compare personnel rosters, contractor lists, and the FEKC list to determine those who have not completed the course.

In addition, there is no centralized roster of FEMA personnel. Conducting a manual review is more complicated because thousands of workers and contractors are assigned to different managers, regions, or disaster relief sites each year. Field managers reported that they cannot enforce the training requirement because it is too time-consuming to determine which workers have not completed the course. In addition, Headquarters and regional training units declined to assist managers in performing manual reviews because of the amount of required work.

Survey Respondents Suggest Privacy Improvements

Survey respondents suggested ways that FEMA can improve its culture of privacy. We received 4,932 individual comments and suggestions from survey respondents on ways that FEMA could be more effective in protecting PII. Figure 9 shows the distribution of survey respondents' comments in five categories.

Figure 9. Improvements for FEMA Culture of Privacy Development



Source: OIG

According to survey respondents, FEMA could increase manager and employee awareness of privacy requirements. For example, they recommended that managers enforce privacy protections (32 percent of comments) and supplement privacy training to improve overall employee awareness of the importance of protecting PII (27 percent). In addition, respondents suggested privacy campaigns, periodic broadcast messages, and emails that remind employees on how to apply privacy policies on their jobs. Respondents also recommended that managers review and improve physical safeguards for PII (19 percent), identify and address specific privacy risks in different employee work environments (12 percent), and increase IT security for PII (10 percent).

Recommendation

We recommend that the Deputy Administrator of FEMA:

Recommendation #4:

Improve managers' capability to monitor and enforce the completion of the standardized, FEMA-wide privacy training requirements.

Management Comments and OIG Analysis

FEMA concurs with recommendation #4. The FEMA Privacy Officer and the FEMA Office of Training and Development are developing a more comprehensive compliance element into the annual privacy training. We consider this recommendation open and unresolved.

Appendix A
Objectives, Scope, and Methodology

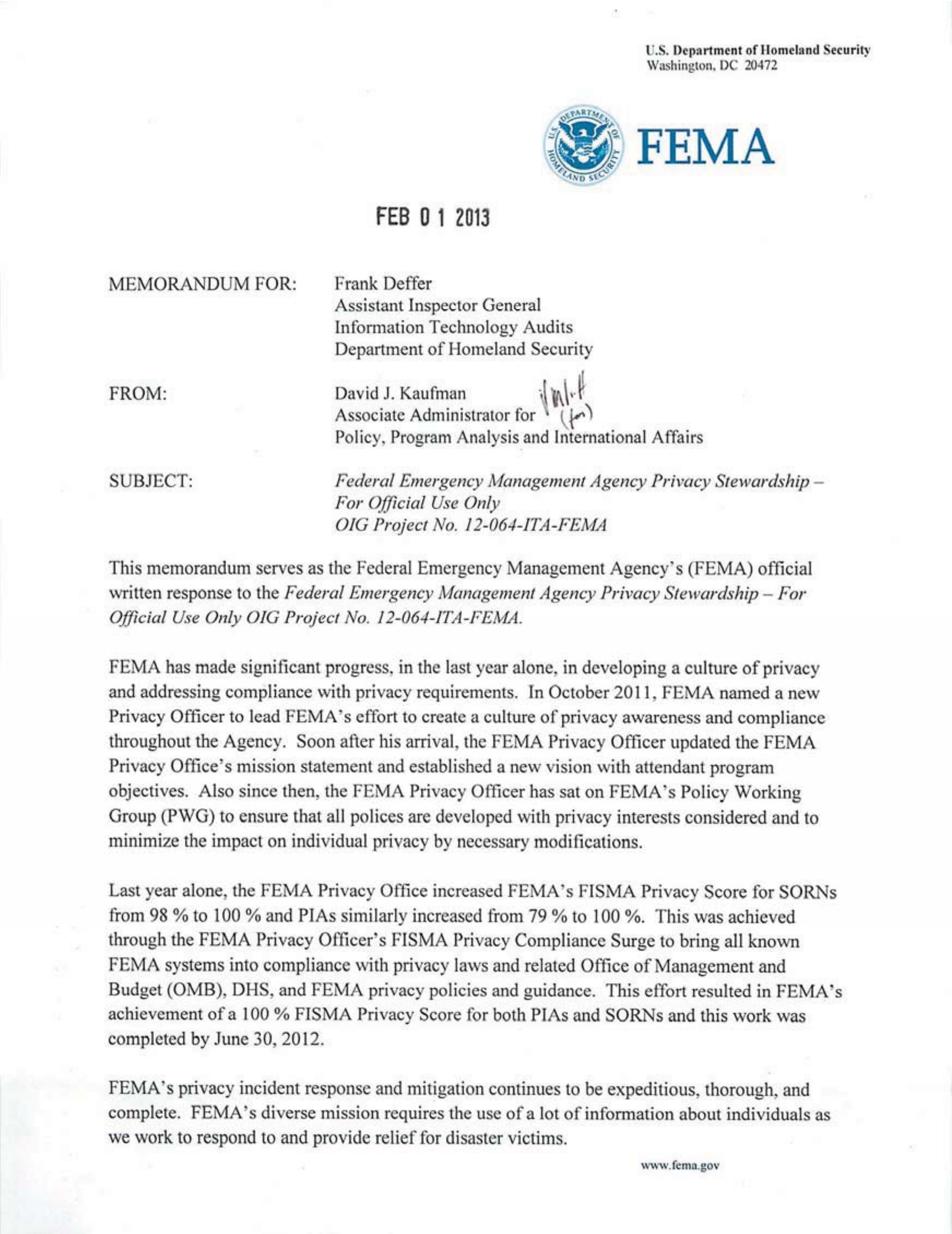
The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department. Our objectives were to determine whether FEMA has plans and activities that instill a culture of privacy that protects sensitive PII and ensures compliance with Federal privacy laws and regulations. As background for this audit, we reviewed Federal laws and guidance related to FEMA's responsibilities for privacy protections. In addition, we interviewed officials from the DHS Privacy Office on FEMA's privacy compliance status and reporting. Also, we reviewed testimonies, documentation, and reports about FEMA's privacy, IT security, and field program management.

As part of our fieldwork, we interviewed FEMA's Privacy Officer and 188 managers, employees, and disaster workers. We conducted field site evaluations at 3 national processing service centers (which included call centers), 1 mail center, 3 regional offices, 3 joint field offices, 1 initial operating facility, and 13 disaster recovery centers to determine areas for improvements in privacy controls. Also, we emailed a survey to FEMA employees to obtain their recommendations for improving their understanding of privacy and for an indication of their privacy knowledge. In response, we received 4,932 individual comments on privacy risks, integrating privacy in daily operations, and challenges in FEMA's privacy stewardship. (See appendix H for details.)

We analyzed training issues and FEMA guidance on privacy, IT, and records management to determine whether they met Federal privacy and security laws and regulations. (See appendix C for references.) We also reviewed PTAs, PIAs, and SORNs for 74 operational IT systems in the FEMA inventory. (See appendix E for details.) In addition, we interviewed IT professionals at FEMA headquarters and disaster relief sites, as well as reviewed reports regarding 430 rogue or unauthorized IT systems.

We conducted this performance audit between January and October 2012 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

Appendix B
Management Comments to the Draft Report



U.S. Department of Homeland Security
Washington, DC 20472

FEMA

FEB 0 1 2013

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General
Information Technology Audits
Department of Homeland Security

FROM: David J. Kaufman
Associate Administrator for
Policy, Program Analysis and International Affairs

SUBJECT: *Federal Emergency Management Agency Privacy Stewardship – For Official Use Only*
OIG Project No. 12-064-ITA-FEMA

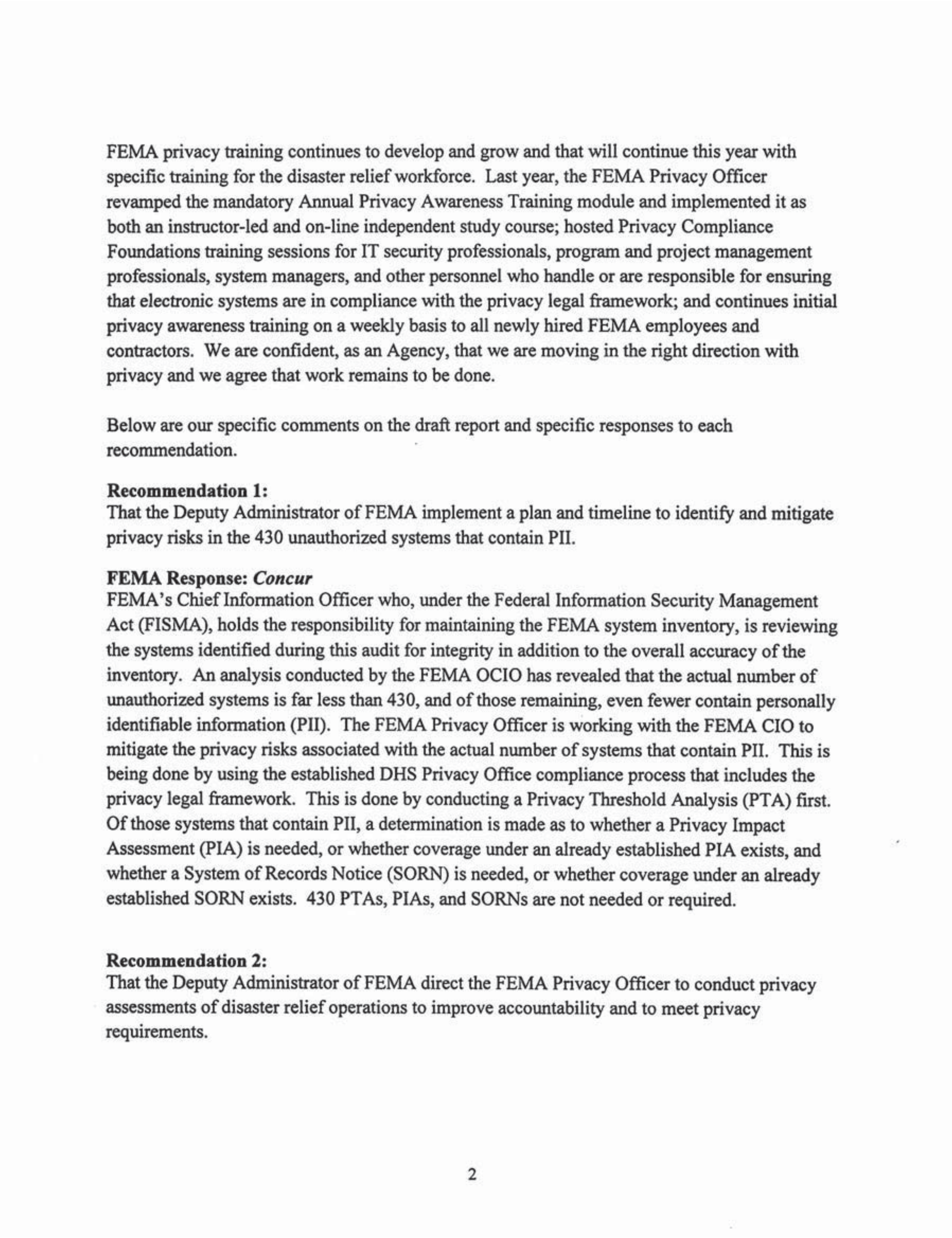
This memorandum serves as the Federal Emergency Management Agency's (FEMA) official written response to the *Federal Emergency Management Agency Privacy Stewardship – For Official Use Only OIG Project No. 12-064-ITA-FEMA.*

FEMA has made significant progress, in the last year alone, in developing a culture of privacy and addressing compliance with privacy requirements. In October 2011, FEMA named a new Privacy Officer to lead FEMA's effort to create a culture of privacy awareness and compliance throughout the Agency. Soon after his arrival, the FEMA Privacy Officer updated the FEMA Privacy Office's mission statement and established a new vision with attendant program objectives. Also since then, the FEMA Privacy Officer has sat on FEMA's Policy Working Group (PWG) to ensure that all polices are developed with privacy interests considered and to minimize the impact on individual privacy by necessary modifications.

Last year alone, the FEMA Privacy Office increased FEMA's FISMA Privacy Score for SORNs from 98 % to 100 % and PIAs similarly increased from 79 % to 100 %. This was achieved through the FEMA Privacy Officer's FISMA Privacy Compliance Surge to bring all known FEMA systems into compliance with privacy laws and related Office of Management and Budget (OMB), DHS, and FEMA privacy policies and guidance. This effort resulted in FEMA's achievement of a 100 % FISMA Privacy Score for both PIAs and SORNs and this work was completed by June 30, 2012.

FEMA's privacy incident response and mitigation continues to be expeditious, thorough, and complete. FEMA's diverse mission requires the use of a lot of information about individuals as we work to respond to and provide relief for disaster victims.

www.fema.gov



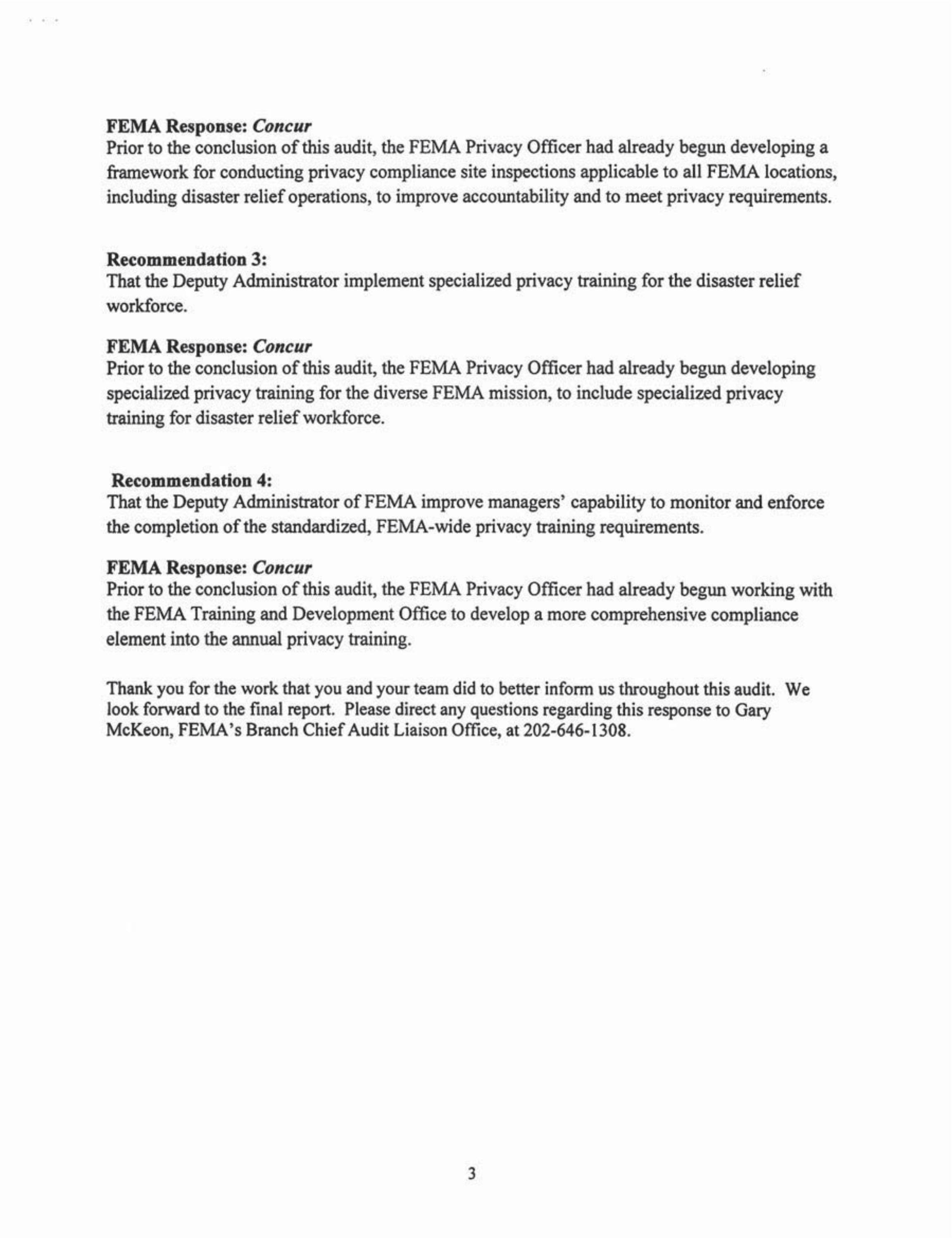
FEMA privacy training continues to develop and grow and that will continue this year with specific training for the disaster relief workforce. Last year, the FEMA Privacy Officer revamped the mandatory Annual Privacy Awareness Training module and implemented it as both an instructor-led and on-line independent study course; hosted Privacy Compliance Foundations training sessions for IT security professionals, program and project management professionals, system managers, and other personnel who handle or are responsible for ensuring that electronic systems are in compliance with the privacy legal framework; and continues initial privacy awareness training on a weekly basis to all newly hired FEMA employees and contractors. We are confident, as an Agency, that we are moving in the right direction with privacy and we agree that work remains to be done.

Below are our specific comments on the draft report and specific responses to each recommendation.

Recommendation 1:
That the Deputy Administrator of FEMA implement a plan and timeline to identify and mitigate privacy risks in the 430 unauthorized systems that contain PII.

FEMA Response: *Concur*
FEMA's Chief Information Officer who, under the Federal Information Security Management Act (FISMA), holds the responsibility for maintaining the FEMA system inventory, is reviewing the systems identified during this audit for integrity in addition to the overall accuracy of the inventory. An analysis conducted by the FEMA OCIO has revealed that the actual number of unauthorized systems is far less than 430, and of those remaining, even fewer contain personally identifiable information (PII). The FEMA Privacy Officer is working with the FEMA CIO to mitigate the privacy risks associated with the actual number of systems that contain PII. This is being done by using the established DHS Privacy Office compliance process that includes the privacy legal framework. This is done by conducting a Privacy Threshold Analysis (PTA) first. Of those systems that contain PII, a determination is made as to whether a Privacy Impact Assessment (PIA) is needed, or whether coverage under an already established PIA exists, and whether a System of Records Notice (SORN) is needed, or whether coverage under an already established SORN exists. 430 PTAs, PIAs, and SORNs are not needed or required.

Recommendation 2:
That the Deputy Administrator of FEMA direct the FEMA Privacy Officer to conduct privacy assessments of disaster relief operations to improve accountability and to meet privacy requirements.



FEMA Response: ***Concur***
Prior to the conclusion of this audit, the FEMA Privacy Officer had already begun developing a framework for conducting privacy compliance site inspections applicable to all FEMA locations, including disaster relief operations, to improve accountability and to meet privacy requirements.

Recommendation 3:
That the Deputy Administrator implement specialized privacy training for the disaster relief workforce.

FEMA Response: ***Concur***
Prior to the conclusion of this audit, the FEMA Privacy Officer had already begun developing specialized privacy training for the diverse FEMA mission, to include specialized privacy training for disaster relief workforce.

Recommendation 4:
That the Deputy Administrator of FEMA improve managers' capability to monitor and enforce the completion of the standardized, FEMA-wide privacy training requirements.

FEMA Response: ***Concur***
Prior to the conclusion of this audit, the FEMA Privacy Officer had already begun working with the FEMA Training and Development Office to develop a more comprehensive compliance element into the annual privacy training.

Thank you for the work that you and your team did to better inform us throughout this audit. We look forward to the final report. Please direct any questions regarding this response to Gary McKeon, FEMA's Branch Chief Audit Liaison Office, at 202-646-1308.

Appendix C
Legislation, Memoranda, Directives, and Guidance Related to the FEMA Privacy Stewardship Audit

LEGISLATION

Privacy Act of 1974, as amended, 5 U.S.C. § 552a.
http://www.gpo.gov/fdsys/pkg/USCODE-2011-title5/pdf/USCODE-2011-title5-partI-chap5-subchapII-sec552a.pdf

E-Government Act of 2002, Public Law 107-347, 116 Stat. 2899.
http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

Federal Information Security Management Act of 2002, 44 U.S.C. § 3541, et seq.
http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, 121 Stat. 266, 360.
http://www.nctc.gov/docs/ir-of-the-9-11-comm-act-of-2007.pdf

Homeland Security Act of 2002, as amended, Public Law 107-296, 116 Stat. 2135, 2179.
http://www.gpo.gov/fdsys/pkg/PLAW-107publ296/pdf/PLAW-107publ296.pdf

Paperwork Reduction Act of 1995, 44 U.S.C. § 3501, et seq.
http://www.gpo.gov/fdsys/pkg/PLAW-104pub13/html/PLAW-104publ13.htm

OMB MEMORANDA

OMB M-07-16: *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007).
http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf

OMB M-11-29: *Chief Information Officer Authorities* (August 8, 2011).
http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-29.pdf

OMB M-12-20: *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (October 2, 2012).
http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-20.pdf

DIRECTIVES AND GUIDANCE

DHS Management Directive Number 047-01: *Privacy Policy and Compliance* (July 7, 2011). (No External Link Available)

DHS Management Instruction Number 047-01-001: *Privacy Policy and Compliance* (July 25, 2011). (No External Link Available)

DHS Memorandum: *Designation of Component Privacy Officers* (June 5, 2009). (No External Link Available)

DHS Privacy Office Privacy Policy Guidance Memorandum Number 2008-02: *DHS Policy Regarding Privacy Impact Assessments* (December 30, 2008). http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-02.pdf

DHS Privacy Office: *Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security* (March 2012). http://www.dhs.gov/xlibrary/assets/privacy/dhs-privacy-safeguardingsensitivepiihandbook-march2012.pdf

DHS Privacy Office: *Guide to Implementing Privacy* (June 2010).
http://www.dhs.gov/xlibrary/assets/privacy/dhsprivacyoffice-guidetoimplementingprivacy.pdf

DHS Privacy Office: *Privacy Incident Handling Guidance* (January 26, 2012).
http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf

DHS Privacy Office: *Privacy Technology Implementation Guide* (August 16, 2007).
http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_ptig.pdf

DHS Privacy Office: *Privacy Impact Assessments: The Privacy Office Official Guidance* (June 2010).
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_june2010.pdf

DHS Privacy Office: *System of Records Notices: The Privacy Office Official Guidance* (April 2008).
http://www.dhs.gov/xlibrary/assets/privacy/privacy_guidance_sorn.pdf

DHS Management Directive Number 0007.1: *Information Technology Integration and Management* (March 15, 2007). (No External Link Available)

DHS 4300A: *Sensitive Systems Policy Directive Version 9.0.2* (March 19, 2012). (No External Link Available)

National Institute of Standards and Technology Special Publication 800-88: *Guidelines for Media Sanitization* (September 2006).
http://www.nist.gov/customcf/get_pdf.cfm?pub_id=50819

Federal CIO Council, Privacy Committee: *Best Practices: Elements of a Federal Privacy Program Version 1.0* (June 2010).
http://www.cio.gov/Documents/Elements-Federal-Privacy-Program-v1.0_June-2010.pdf

U.S. Chief Information Officer: *25 Point Implementation Plan to Reform Federal Information Technology Management* (December 9, 2010). http://www.cio.gov/documents/25-Point-Implementation-Plan-to-Reform-Federal%20IT.pdf

FEMA DOCUMENTS

44 C.F.R. Ch. I, Subpart E*, Report on New Systems and Alterations of Existing Systems, Section 6.70* (October 1, 2011).
http://www.gpo.gov/fdsys/pkg/CFR-2011-title44-vol1/pdf/CFR-2011-title44-vol1-sec6-70.pdf

FEMA Standard Operating Procedure: *Electronic and Hard Copy Sanitization and Release* (September 2, 2011). (No External Link Available)

FEMA Directive 140-1**:** *Information Technology Security Policy* (January 14, 2012). (No External Link Available)

FEMA Directive 140-2**:** *Information Technology Integration and Management* (February 10, 2012). (No External Link Available)

FEMA Memorandum: *Unauthorized Information Technology Systems* (March 13, 2012). (No External Link Available)

FEMA Memorandum: *Delegating Authorities to Regional Administrators* (February 6, 2012). (No External Link Available)

FEMA Memorandum: *Regional Staffing Initiative* (August 4, 2010). (No External Link Available)

Appendix D
Component-Level Privacy Officer Designation and Duties

Figure 10. Component-Level Privacy Officer Designation and Duties

COMPONENTS TO DESIGNATE PRIVACY OFFICERS
▪ Federal Emergency Management Agency ▪ National Protection and Programs Directorate ▪ Office of Intelligence and Analysis ▪ Science & Technology Directorate ▪ Transportation Security Administration ▪ U.S. Citizenship and Immigration Services ▪ U.S. Coast Guard ▪ U.S. Customs and Border Protection ▪ U.S. Immigration and Customs Enforcement ▪ U.S. Secret Service

Source: DHS Designation Memorandum, June 5, 2009

COMPONENT PRIVACY OFFICER DUTIES
Maintain an ongoing review of component IT systems, technologies, rulemakings, programs, pilot projects, information sharing, and other activities to identify collections and uses of PII and any other attendant privacy impacts.
Coordinate with system and program managers, together with the DHS Privacy Officer and component counsel to complete required privacy compliance documentation.
Review component policies and directives to ensure compliance with DHS privacy policy, privacy laws applicable to DHS, and Federal Government-wide privacy policies.
Oversee component implementation of DHS privacy policy.
Provide the DHS Privacy Officer all component information necessary to meet the Department's responsibilities for reporting to Congress or OMB on DHS activities that involve PII or otherwise impact privacy.
Oversee component's implementation of procedures and guidance issued by the DHS Privacy Officer for handling suspected and confirmed privacy incidents; notify the DHS Privacy Officer and other Department offices of such incidents as component procedures dictate; ensure that privacy incidents have been properly mitigated; and recommend that the DHS Privacy Officer close privacy incidents upon mitigation.
Process privacy complaints from organizations, DHS employees, and other individuals, whether received directly or by referral from the DHS Privacy Officer.
Oversee component privacy training and provide educational materials, consistent with mandatory and supplementary training developed by the DHS Privacy Officer.
Maintain an ongoing review of component data collection forms, whether electronic or paper-based, to ensure compliance with the Privacy Act Statements and implementation of regulations and guidelines.
Review component record retention schedules for paper or electronic records that contain PII to ensure privacy interests are considered in the establishment of component record disposition policies.
Advise component on information sharing activities that involve the disclosure or receipt of PII and participate in the review of Information Sharing Access Agreements.
Document and implement procedures for identifying, processing, tracking, and reporting on Privacy Act Amendment requests.

Source: DHS Management Instruction Number 047-01-001

Appendix E
TAFISMA Systems That Affect Privacy: Compliance Status

Privacy protections must be incorporated during the development and operation of systems and programs that affect privacy. DHS privacy policy guidance requires that components conduct a privacy threshold analysis (PTA) when they propose a new system of records or make significant changes to an existing system. The analysis of each approved system must be updated every three years. DHS components are to conduct privacy impact assessments (PIA) of all systems that collect, use, maintain, or disseminate PII, consistent with the *E-Government Act of 2002*. The *Privacy Act of 1974* requires agencies to issue public notice for systems of records under their control. A system of records notice (SORN) informs the public about what, why, and how PII are to be collected, retained, shared, accessed, and corrected. The status of FEMA's privacy compliance analysis and documentation may affect how well it addresses privacy issues and mitigates risks to PII.

Figure 11. FEMA PII Compliance Status for 46 IT Systems

Legend	Description
PIA/SORN Name Date of Document	Privacy impact assessment or system of records notice completed.
Completed Date of Document	Privacy threshold analysis completed.
Completed Date of Document	Privacy threshold analysis completed but expired.
Not Completed	Privacy impact assessment not completed.
Not Applicable	Privacy impact assessment or system of records notice not required.

Name of IT System	Privacy Threshold Analysis (Required: 46)	Privacy Impact Assessment (Required: 38)	System of Records Notice (Required: 45)
Disaster Response and Recovery Programs Information Technology Systems and Associated Applications support the efforts of FEMA's disaster assistance mission for individuals and families. Collections may include name, address, Social Security number, birthdates, telephone number, National Emergency Management Information System (NEMIS) registration ID, disaster-related damage information, insurance information, financial information, education records, vehicle identifiers, criminal history information, and information to verify identity.			
Disaster Assistance Improvement Program (DAIP)	Completed Jan 18, 2011	DHS/FEMA/PIA-012 Dec 31, 2008	DHS/FEMA-008, 74 FR 48763 Sep 24, 2009
National Emergency Family Registry and Locator System (NEFRLS)	Completed Mar 8, 2010	DHS/FEMA/PIA-14(a) Jul 14, 2011	DHS/FEMA-008, 74 FR 48763 Sep 24, 2009
Emergency Notification System (ENS)	Completed Oct 21, 2010	Not Applicable	DHS/ALL-014, 73 FR 61888 Oct 17, 2008

Name of IT System	Privacy Threshold Analysis (Required: 46)	Privacy Impact Assessment (Required: 38)	System of Records Notice (Required: 45)
NEMIS Individual Assistance	Completed Dec 29, 2011	DHS/FEMA/PIA-027 June 29, 2012	DHS/FEMA-008, 74 FR 48763 Sep 24, 2009
Grant Programs Information Technology Systems and Associated Applications support the efforts of FEMA's proactive nondisaster grant programs. Collections may include name, work address, Social Security number (used as Employer Identification Number), financial information, work email address, and work numbers for telephone, fax, and, cell phone, and information on activity funded by the grant.			
Assisted Firefighters Grant (AFG)	Completed Dec 9, 2011	DHS/FEMA/PIA-013 Jul 14, 2009	DHS/FEMA-004, 74 FR 39705 Aug 7, 2009
Grants Reporting Tool	Completed Nov 3, 2009	DHS/FEMA/PIA-013 Jul 14, 2009	DHS/FEMA-004, 74 FR 39705 Aug 7, 2009
Non-Disaster (ND) Grants	Completed Jul 2, 2008	DHS/FEMA/PIA-013 Jul 14, 2009	DHS/FEMA-004, 74 FR 39705 Aug 7, 2009
Hazard Mitigation Grant Program	Completed Feb 15, 2012	DHS/FEMA/PIA-025 Jun 28, 2012	DHS/FEMA-009, 77 FR 17783 Jul 23, 2012
Mitigation Programs Information Technology Systems and Associated Applications support the efforts of FEMA's mitigation and disaster grants missions implementing mitigation activities to reduce or eliminate risk of future damage to life or property. Collected information may include name, address of damaged property, mailing address, telephone number, financial information, insurance status, insurance claims, and damaged property contents.			
Mapping Information Platform – Data Center 2	Completed Feb 2, 2011	DHS/FEMA/PIA-003 Jan 27, 2006	DHS/FEMA/NFIP/LOMA-1, 71 FR 7990 Feb 15, 2006
eGrants	Completed Feb 10, 2011	DHS/FEMA/PIA-006 Jan 19, 2007	DHS/FEMA/2006-002, 69 FR 75079 Dec 15, 2004
Map Service Center	Completed Sep 7, 2006	DHS/FEMA/PIA-007 Feb 12, 2007	DHS/FEMA-003, 73 FR 77747 Dec 19, 2008
Map Service Center – On-Line Digital Distribution Center (MSC On-Line DDC)	Completed May 7, 2010	DHS/FEMA/PIA-007 Feb 12, 2007	DHS/FEMA-003, 73 FR 77747 Dec 19, 2008
Total Records Information Management	Completed May 3, 2012	DHS/FEMA/PIA-009 Sep 8, 2008	DHS/ALL-003, 73 FR 71656 Nov 25, 2008
National Flood Insurance Program Information Technology Systems	Completed Jul 1, 2009	DHS/FEMA/PIA-011 Nov 26, 2008	DHS/FEMA-003, 73 FR 77747 Dec 19, 2008
Emergency Management Mission Integrated Environment	Completed Jan 17, 2012	DHS/FEMA/PIA-013 Jul 14, 2009	DHS/FEMA-004, 74 FR 39705 Aug 7, 2009
Enterprise Coordination and Approval Process System	Completed Mar 7, 2011	DHS/FEMA/PIA-023 May 21, 2012	Not Applicable
Community Information System	Completed Dec 13, 2011	Not Completed	DHS/FEMA-003, 73 FR 77747 Dec 19, 2008
National Preparedness Programs Information Technology Systems and Associated Applications support FEMA's mission to assist citizens and first responders in preparation for all hazards through training and exercise programs. Collections may include name, address, telephone number, email address, citizenship, employment status, organizational affiliations, professional credentials, user names, and passwords.			
Lessons Learned Information Sharing	Completed Feb 10, 2011	DHS/ALL/PIA-015 Jun 15, 2009	DHS/ALL-004, 74 FR 49882 Sep 29, 2009
First Responder Training	Completed Nov 16, 2009	DHS/FEMA/PIA-008 Jul 16, 2008	DHS/ALL-004, 74 FR 49882 Sep 29, 2009

Name of IT System	Privacy Threshold Analysis (Required: 46)	Privacy Impact Assessment (Required: 38)	System of Records Notice (Required: 45)
Corrective Action Planning System	Completed Aug 10, 2009	DHS/FEMA/PIA-016 Mar 3, 2011	DHS/FEMA-011, 76 FR 19107 Apr 6, 2011
Design and Development System	Completed Jan 26, 2010	DHS/FEMA/PIA-016 Mar 3, 2011	DHS/FEMA-011, 76 FR 19107 Apr 6, 2011
National Exercise Master Scenario Event List (NxMSEL)	Completed Nov 15, 2010	DHS/FEMA/PIA-016 Mar 3, 2011	DHS/FEMA-011, 76 FR 19107 Apr 6, 2011
National Exercise Scheduling System	Completed Aug 21, 2009	DHS/FEMA/PIA-016 Mar 3, 2011	DHS/FEMA-011, 76 FR 19107 Apr 6, 2011
Center for Domestic Preparedness Learning Management System	Completed Jun 18, 2008	DHS/FEMA/PIA-022 Mar 29, 2012	DHS/FEMA-011, 76 FR 19107 Apr 6, 2011
FEMA Employee Knowledge Center (FEKC)	Completed Jul 19, 2006	Not Applicable	DHS/ALL-003, 73 FR 71656 Nov 25, 2008
United States Fire Administration Programs Information Technology Systems and Associated Applications support the training programs of the National Fire Academy and other United States Fire Administration programs. Collected information may include name, address, telephone number, email address, citizenship, educational information, disability information, organizational affiliation, and fire department identification number.			
United States Fire Administration Web Farm	Completed Sep 17, 2009	DHS/ALL/PIA-006 Jun 15, 2007	DHS/ALL-002, 73 FR 71659 Nov 25, 2008
National Emergency Training Center Learning Resource Center	Completed April 5, 2010	DHS/FEMA/PIA-022 Mar 29, 2012	DHS/ALL-003, 73 FR 71656 Nov 25, 2008
United States Fire Administration Systems	Completed Jan 18, 2012	DHS/FEMA/PIA-022 Mar 29, 2012	DHS/FEMA-011, 76 FR 19107 Apr 6, 2011
National Fire Incident Reporting System	Completed Feb 6, 2009	Not Applicable	DHS/FEMA-008, 74 FR 48763 Sep 24, 2009
Mission Support Systems and Associated Applications support all of FEMA's missions in disaster assistance, proactive grants programs, disaster mitigation grants, and training activities. These overarching systems' collections may include: name, address, Social Security number, birthdates, telephone number, email address, NEMIS registration ID, disaster-related damage information, insurance information, financial information, education records, vehicle identifiers, criminal history information, identity verification methods, and biometric (fingerprint) data.			
Logistics Information Management System (LIMS) – FEMA	Completed Feb 8, 2011	DHS/ALL/PIA-006 Jun 15, 2007	DHS/ALL-010, 73 FR 63181 Oct 23, 2008
Executive Management System	Completed Nov 15, 2010	DHS/ALL/PIA-012 Jan 14, 2009	DHS/ALL-002, 73 FR 71659 Nov 25, 2008
Electronic Fingerprint System (EFS)	Completed Feb 2, 2009	DHS/ALL/PIA-014(a) Jun 18, 2009	DHS/ALL-024, 75 FR 5609 Feb 30, 2010
Velocity Security Management System (Hirsch) – Unclassified	Completed Jul 29, 2010	DHS/ALL/PIA-014(a) Jun 18, 2009	DHS/ALL-024, 75 FR 5609 Feb 30, 2010
The Full-Spectrum Risk Knowledgebase	Completed May 2, 2011	DHS/ALL/PIA-015 Jun 15, 2009	DHS/ALL-004, 74 FR 49882 Sep 29, 2009
Integrated Situational Awareness Visualization Environment	Completed Aug 31, 2011	DHS/ALL/PIA-036 Mar 8, 2011	DHS/ALL-004, 74 FR 49882 Sep 29, 2009

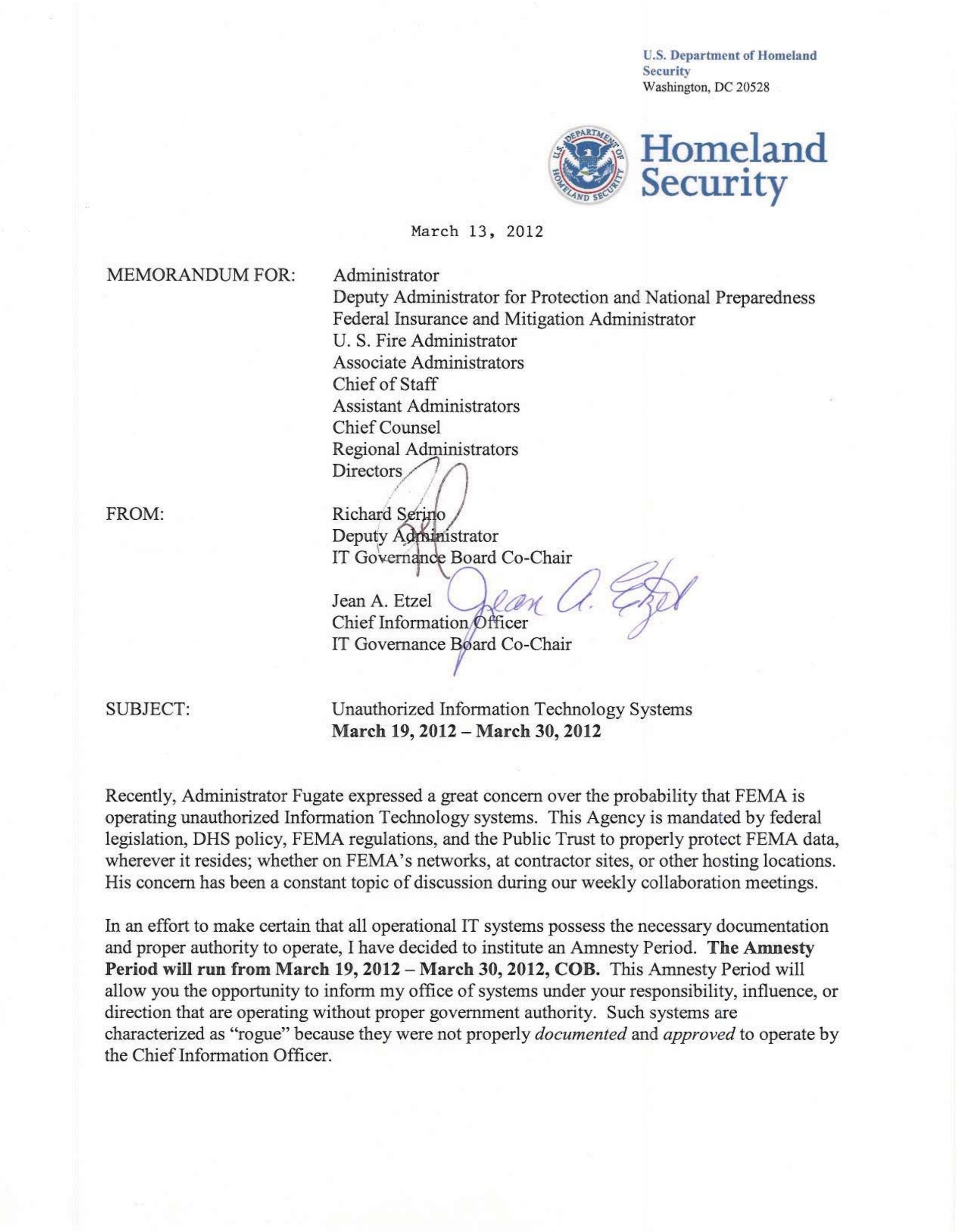
Name of IT System	Privacy Threshold Analysis (Required: 46)	Privacy Impact Assessment (Required: 38)	System of Records Notice (Required: 45)
Document Management and Records Tracking System	Completed Jan 10, 2007	DHS/FEMA/PIA-009 Sep 10, 2008	DHS/FEMA-008, 74 FR 48763 Sep 24, 2009
Quality Assurance Recording System	Completed Apr 25, 2012	DHS/FEMA/PIA-015 Nov 10, 2010	DHS/FEMA-002, 76 FR 8758 Feb 15, 2011
Firehouse Database – Unclassified	Completed Dec 16, 2011	DHS/FEMA/PIA-019 Dec 15, 2011	DHS/OHA-002[1], 76 FR 53921 Aug 30, 2011
Integrated Financial Management Information System (IFMIS)-Merger	Completed Nov 23, 2011	DHS/FEMA/PIA-020 Dec 16, 2011	DHS/FEMA-008[2], 74 FR 48763 Sep 24, 2009
Authentication and Provisioning Services	Completed Jul 25, 2006	Not Applicable	DHS/ALL-002, 73 FR 71659 Nov 25, 2008
Enterprise Wireless LAN	Completed Mar 7, 2012	Not Applicable	DHS/ALL-004, 74 FR 49882 Sep 29, 2009
Intelligent Roads and Rail Information System	Completed Jun 5, 2009	Not Applicable	DHS/ALL-004, 74 FR 49882 Sep 29, 2009
Real Property Management System (RPMS)	Completed Jan 19, 2011	Not Applicable	DHS/ALL-004, 74 FR 49882 Sep 29, 2009
Resource Management Online	Completed Apr 5, 2010	Not Applicable	DHS/ALL-004, 74 FR 49882 Sep 29, 2009
Accounting Package System (ACCPAC)	Completed Aug 12, 2010	DHS/FEMA/PIA-024 Jun 8, 2012	DHS/ALL-008, 73 FR 61880 Oct, 17 2008
Enterprise Data Warehouse	Completed Dec 30, 2011	DHS/FEMA/PIA-026 Jun 29, 2012	DHS/ALL-004, 74 FR 49882 Sep 29, 2009

Source: TAFISMA

[1] DHS SORN listed in figure 11. Additional SORNs apply to this IT system: OPM/GOVT-10 Employee Medical File System of Records, Jun 19, 2006, 71 FR 35360 and OPM/GOVT-1 General Personnel Records, Jun 19, 2006, 71 FR 35342.

[2] FEMA SORN listed in figure 11. Additional SORNs apply to this IT system: DHS/ALL-007 Accounts Payable System of Records, Oct 17, 2008, 73 FR 61880; DHS/ALL-008 Accounts Receivable System of Records, Oct 17 2008, 73 FR 61885; DHS/ALL-019 Payroll, Personnel, Time, and Attendance Records, Oct 23, 2008, 73 FR 62172; DHS/FEMA-2006-0002 National Emergency Management Information System – Mitigation Electronic Grants Management System (NEMIS-MT eGrants), Dec 15, 2004, 69 FR 75079; and, GSA/Government-wide 4 Contracted Travel Services Program, Jun 3, 2009, 41 FR 26700.

Appendix F
FEMA Unauthorized Information Technology Systems Memorandum



U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

March 13, 2012

MEMORANDUM FOR: Administrator
Deputy Administrator for Protection and National Preparedness
Federal Insurance and Mitigation Administrator
U. S. Fire Administrator
Associate Administrators
Chief of Staff
Assistant Administrators
Chief Counsel
Regional Administrators
Directors

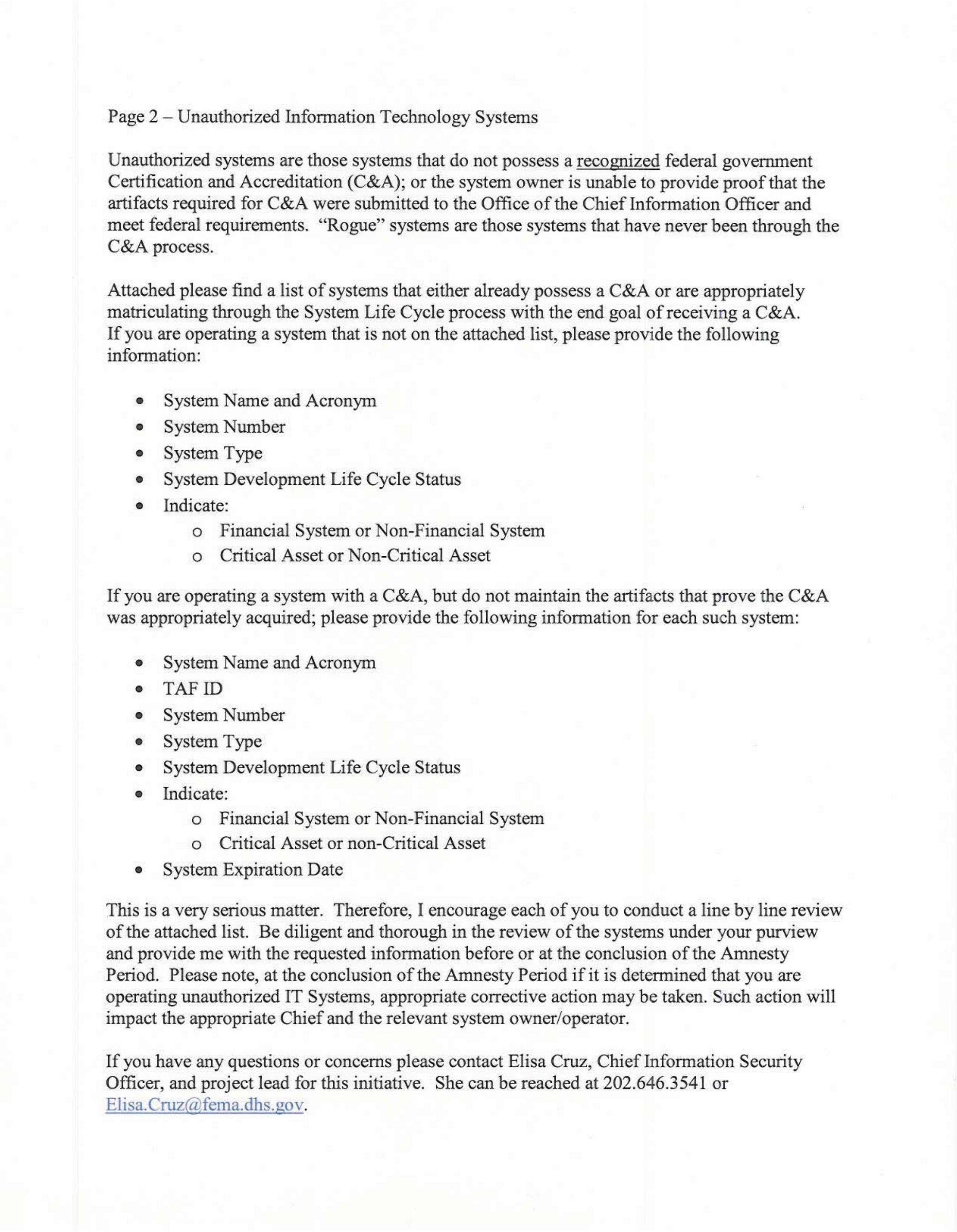
FROM: Richard Serino
Deputy Administrator
IT Governance Board Co-Chair

Jean A. Etzel Jean A. Etzel
Chief Information Officer
IT Governance Board Co-Chair

SUBJECT: Unauthorized Information Technology Systems
March 19, 2012 – March 30, 2012

Recently, Administrator Fugate expressed a great concern over the probability that FEMA is operating unauthorized Information Technology systems. This Agency is mandated by federal legislation, DHS policy, FEMA regulations, and the Public Trust to properly protect FEMA data, wherever it resides; whether on FEMA's networks, at contractor sites, or other hosting locations. His concern has been a constant topic of discussion during our weekly collaboration meetings.

In an effort to make certain that all operational IT systems possess the necessary documentation and proper authority to operate, I have decided to institute an Amnesty Period. **The Amnesty Period will run from March 19, 2012 – March 30, 2012, COB.** This Amnesty Period will allow you the opportunity to inform my office of systems under your responsibility, influence, or direction that are operating without proper government authority. Such systems are characterized as "rogue" because they were not properly *documented* and *approved* to operate by the Chief Information Officer.



Page 2 – Unauthorized Information Technology Systems

Unauthorized systems are those systems that do not possess a recognized federal government Certification and Accreditation (C&A); or the system owner is unable to provide proof that the artifacts required for C&A were submitted to the Office of the Chief Information Officer and meet federal requirements. "Rogue" systems are those systems that have never been through the C&A process.

Attached please find a list of systems that either already possess a C&A or are appropriately matriculating through the System Life Cycle process with the end goal of receiving a C&A. If you are operating a system that is not on the attached list, please provide the following information:

- System Name and Acronym
- System Number
- System Type
- System Development Life Cycle Status
- Indicate:
  - Financial System or Non-Financial System
  - Critical Asset or Non-Critical Asset

If you are operating a system with a C&A, but do not maintain the artifacts that prove the C&A was appropriately acquired; please provide the following information for each such system:

- System Name and Acronym
- TAF ID
- System Number
- System Type
- System Development Life Cycle Status
- Indicate:
  - Financial System or Non-Financial System
  - Critical Asset or non-Critical Asset
- System Expiration Date

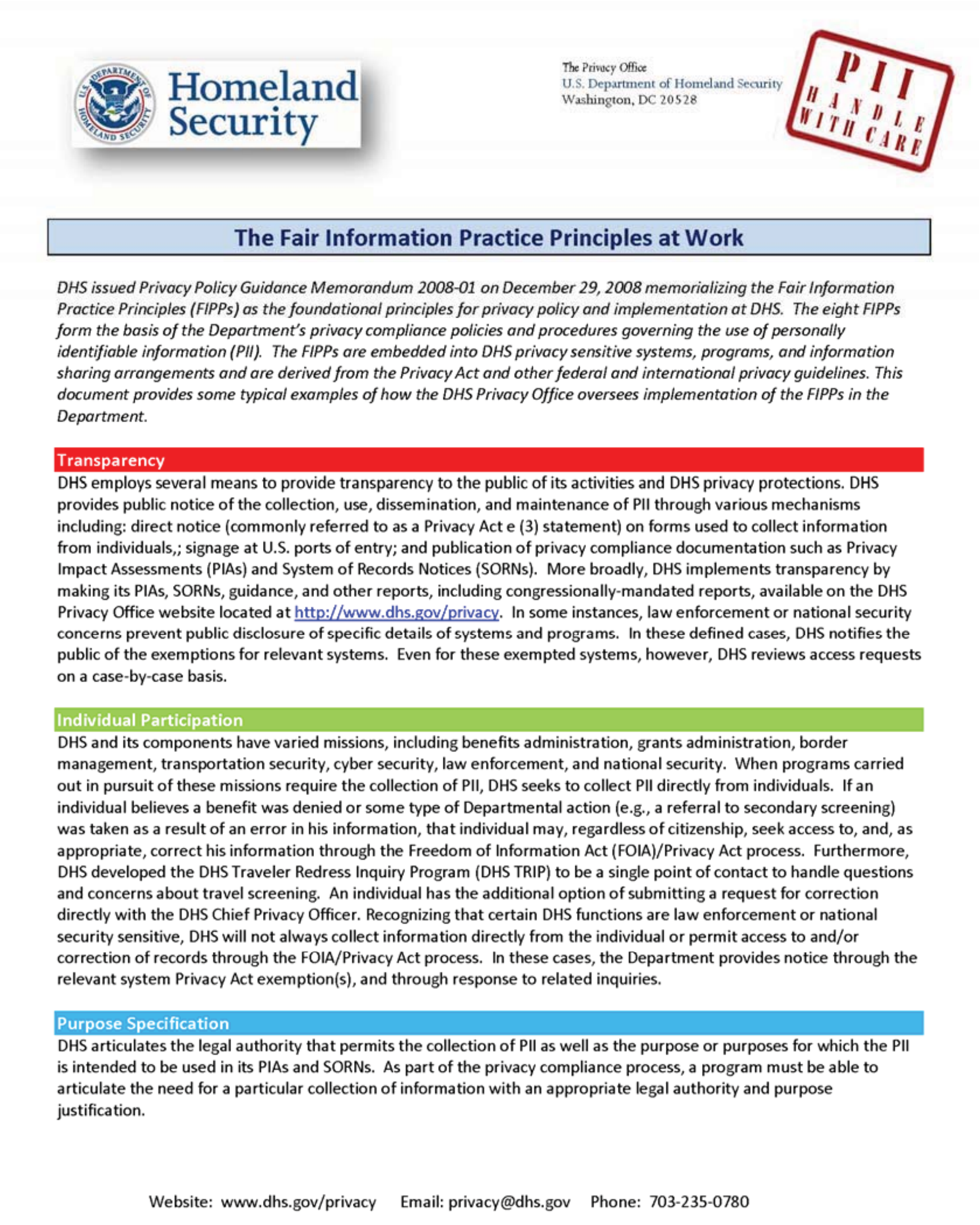
This is a very serious matter. Therefore, I encourage each of you to conduct a line by line review of the attached list. Be diligent and thorough in the review of the systems under your purview and provide me with the requested information before or at the conclusion of the Amnesty Period. Please note, at the conclusion of the Amnesty Period if it is determined that you are operating unauthorized IT Systems, appropriate corrective action may be taken. Such action will impact the appropriate Chief and the relevant system owner/operator.

If you have any questions or concerns please contact Elisa Cruz, Chief Information Security Officer, and project lead for this initiative. She can be reached at 202.646.3541 or Elisa.Cruz@fema.dhs.gov.

Source: FEMA

Appendix G
DHS Fair Information Practice Principles at Work

Figure 12. DHS Fair Information Practice Principles at Work



Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

PII HANDLE WITH CARE

The Fair Information Practice Principles at Work

DHS issued Privacy Policy Guidance Memorandum 2008-01 on December 29, 2008 memorializing the Fair Information Practice Principles (FIPPs) as the foundational principles for privacy policy and implementation at DHS. The eight FIPPs form the basis of the Department's privacy compliance policies and procedures governing the use of personally identifiable information (PII). The FIPPs are embedded into DHS privacy sensitive systems, programs, and information sharing arrangements and are derived from the Privacy Act and other federal and international privacy guidelines. This document provides some typical examples of how the DHS Privacy Office oversees implementation of the FIPPs in the Department.

Transparency

DHS employs several means to provide transparency to the public of its activities and DHS privacy protections. DHS provides public notice of the collection, use, dissemination, and maintenance of PII through various mechanisms including: direct notice (commonly referred to as a Privacy Act e (3) statement) on forms used to collect information from individuals,; signage at U.S. ports of entry; and publication of privacy compliance documentation such as Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs). More broadly, DHS implements transparency by making its PIAs, SORNs, guidance, and other reports, including congressionally-mandated reports, available on the DHS Privacy Office website located at http://www.dhs.gov/privacy. In some instances, law enforcement or national security concerns prevent public disclosure of specific details of systems and programs. In these defined cases, DHS notifies the public of the exemptions for relevant systems. Even for these exempted systems, however, DHS reviews access requests on a case-by-case basis.

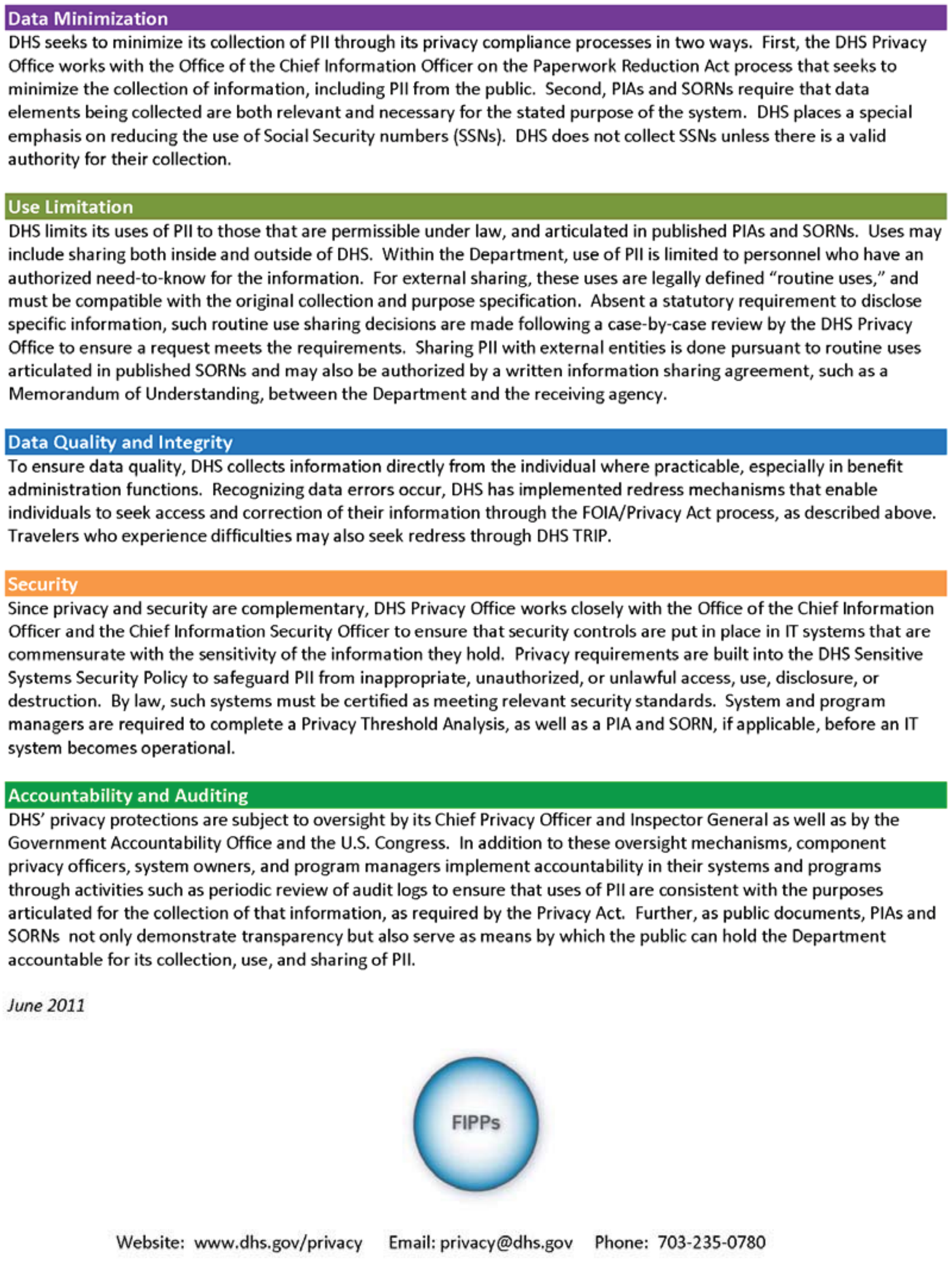
Individual Participation

DHS and its components have varied missions, including benefits administration, grants administration, border management, transportation security, cyber security, law enforcement, and national security. When programs carried out in pursuit of these missions require the collection of PII, DHS seeks to collect PII directly from individuals. If an individual believes a benefit was denied or some type of Departmental action (e.g., a referral to secondary screening) was taken as a result of an error in his information, that individual may, regardless of citizenship, seek access to, and, as appropriate, correct his information through the Freedom of Information Act (FOIA)/Privacy Act process. Furthermore, DHS developed the DHS Traveler Redress Inquiry Program (DHS TRIP) to be a single point of contact to handle questions and concerns about travel screening. An individual has the additional option of submitting a request for correction directly with the DHS Chief Privacy Officer. Recognizing that certain DHS functions are law enforcement or national security sensitive, DHS will not always collect information directly from the individual or permit access to and/or correction of records through the FOIA/Privacy Act process. In these cases, the Department provides notice through the relevant system Privacy Act exemption(s), and through response to related inquiries.

Purpose Specification

DHS articulates the legal authority that permits the collection of PII as well as the purpose or purposes for which the PII is intended to be used in its PIAs and SORNs. As part of the privacy compliance process, a program must be able to articulate the need for a particular collection of information with an appropriate legal authority and purpose justification.

Website: www.dhs.gov/privacy Email: privacy@dhs.gov Phone: 703-235-0780



Data Minimization

DHS seeks to minimize its collection of PII through its privacy compliance processes in two ways. First, the DHS Privacy Office works with the Office of the Chief Information Officer on the Paperwork Reduction Act process that seeks to minimize the collection of information, including PII from the public. Second, PIAs and SORNs require that data elements being collected are both relevant and necessary for the stated purpose of the system. DHS places a special emphasis on reducing the use of Social Security numbers (SSNs). DHS does not collect SSNs unless there is a valid authority for their collection.

Use Limitation

DHS limits its uses of PII to those that are permissible under law, and articulated in published PIAs and SORNs. Uses may include sharing both inside and outside of DHS. Within the Department, use of PII is limited to personnel who have an authorized need-to-know for the information. For external sharing, these uses are legally defined "routine uses," and must be compatible with the original collection and purpose specification. Absent a statutory requirement to disclose specific information, such routine use sharing decisions are made following a case-by-case review by the DHS Privacy Office to ensure a request meets the requirements. Sharing PII with external entities is done pursuant to routine uses articulated in published SORNs and may also be authorized by a written information sharing agreement, such as a Memorandum of Understanding, between the Department and the receiving agency.

Data Quality and Integrity

To ensure data quality, DHS collects information directly from the individual where practicable, especially in benefit administration functions. Recognizing data errors occur, DHS has implemented redress mechanisms that enable individuals to seek access and correction of their information through the FOIA/Privacy Act process, as described above. Travelers who experience difficulties may also seek redress through DHS TRIP.

Security

Since privacy and security are complementary, DHS Privacy Office works closely with the Office of the Chief Information Officer and the Chief Information Security Officer to ensure that security controls are put in place in IT systems that are commensurate with the sensitivity of the information they hold. Privacy requirements are built into the DHS Sensitive Systems Security Policy to safeguard PII from inappropriate, unauthorized, or unlawful access, use, disclosure, or destruction. By law, such systems must be certified as meeting relevant security standards. System and program managers are required to complete a Privacy Threshold Analysis, as well as a PIA and SORN, if applicable, before an IT system becomes operational.

Accountability and Auditing

DHS' privacy protections are subject to oversight by its Chief Privacy Officer and Inspector General as well as by the Government Accountability Office and the U.S. Congress. In addition to these oversight mechanisms, component privacy officers, system owners, and program managers implement accountability in their systems and programs through activities such as periodic review of audit logs to ensure that uses of PII are consistent with the purposes articulated for the collection of that information, as required by the Privacy Act. Further, as public documents, PIAs and SORNs not only demonstrate transparency but also serve as means by which the public can hold the Department accountable for its collection, use, and sharing of PII.

June 2011

Website: www.dhs.gov/privacy Email: privacy@dhs.gov Phone: 703-235-0780

Source: DHS Privacy Office

Appendix H
Culture of Privacy Survey

We developed a privacy questionnaire with assistance from the FEMA Privacy Officer. In January 2012, we emailed the FEMA employees a hyperlink to a secure site and asked them to complete an online culture of privacy survey. Survey participation was voluntary, confidential, and accessible only by OIG. The purposes of the survey were to assess privacy knowledge of rules, regulations, and legislation and to obtain employees' responses to five questions pertaining to privacy risks, examples of privacy risks, improvements to privacy training, integrating privacy safeguards in daily operations, and promoting a privacy culture at FEMA.

FEMA's employee list was used to generate survey invitations. A total of 2,290 respondents completed the FEMA Culture of Privacy Survey. The completed survey response rate was 2,290 (12.8 percent) of 17,837. Figure 13 presents the levels of job responsibility, locations, job types, and lengths of service of respondents who completed the survey.

Figure 13. Demographics of Survey Respondents

DEMOGRAPHICS (n = 2,290 Survey Respondents)	
LEVEL OF JOB RESPONSIBILITY	LOCATION
Entry-level Employees (11.9%) Mid to High-level (Nonmanager) Employees (65.4%) Supervisors/First-Line Managers (19.3%) Executive/Senior Managers (3.4%)	FEMA Headquarters (18.8%) FEMA Regions I-X, and Field Activities (40.1%) Other, including National Processing Service Centers (41.1%)
TYPE OF JOB	LENGTH OF SERVICE OF PERMANENT EMPLOYEES
Permanent, Full-time Employees (42.1%) Cadre of On-Call Response/Recovery Employees (27.6%) Disaster Assistance Employees (29.0%) Other Employees (1.3%)	Less than 3 months (0.2%) 3–12 months (2.0%) 1–3 years (25.2%) More than 3 years (72.6%)

Source: OIG

Appendix I
Major Contributors to This Report

Marj Leaming, Director
Eun Suk Lee, Privacy Audit Manager
Kevin Mullinix, Program Analyst
Bridget Glazier, Referencer

Appendix J
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Administrator of FEMA
Acting Chief Privacy Officer
Chief Information Officer
FEMA Audit Liaison Office
FEMA Privacy Office

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this document, please call us at (202) 254-4100, fax your request to (202) 254-4305, or e-mail your request to our Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

For additional information, visit our website at: www.oig.dhs.gov, or follow us on Twitter at: @dhsoig.

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to: DHS Office of Inspector General, Attention: Office of Investigations Hotline, 245 Murray Drive, SW, Building 410/Mail Stop 2600, Washington, DC, 20528; or you may call 1 (800) 323-8603; or fax it directly to us at (202) 254-4297.

The OIG seeks to protect the identity of each writer and caller.