

FEMA Continues to Experience Challenges in Protecting Personally Identifiable Information at Disaster Recovery Centers





DHS OIG HIGHLIGHTS

FEMA Continues to Experience Challenges in Protecting Personally Identifiable Information at Disaster Recovery Centers

June 9, 2016

Why We Did This Audit

We issued this advisory report to notify the Federal Emergency Management Agency (FEMA) of an issue that requires its immediate attention. During our audit of FEMA's initial response to the 2015 wildfires in Northern California, we observed personnel mishandling Personally Identifiable Information (PII) at disaster relief sites. FEMA officials need to take quick action to ensure the protection of PII in future disasters.

What We Recommend

FEMA must ensure that disaster assistance personnel are aware of their responsibilities to safeguard PII, and create a system to document and enforce compliance with Federal standards.

For Further Information:

Contact our Office of Public Affairs at (202) 254-4100, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

During our deployment to the 2015 California wildfire disaster, we observed that FEMA personnel at Disaster Recovery Centers did not properly safeguard PII, as Federal guidelines require. The mishandling of PII increases the risk of identity theft and can result in substantial harm, embarrassment, inconvenience, or unfairness to individuals. We also determined that some FEMA officials are not fully aware of Federal privacy standards. Moreover, FEMA management and trainers lack an effective method to track employee compliance with privacy training or to promote privacy awareness at disaster relief sites.

In May 2013, we reported similar deficiencies. As a result, FEMA officials stated that they would implement corrective actions, including conducting privacy compliance inspections at all disaster relief sites. However, FEMA officials at Disaster Recovery Centers for the 2015 California wildfire disaster were not aware of any privacy compliance inspections conducted at this disaster. While FEMA has made significant progress in developing a culture of privacy protection, it clearly needs to do more to safeguard private information at these sites.

FEMA Response

FEMA officials agreed with our findings and recommendations. Appendix B includes FEMA's written response in its entirety.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

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

June 9, 2016

MEMORANDUM FOR: Elizabeth Zimmerman
Associate Administrator
Office of Response and Recovery

FROM: John V. Kelly
Assistant Inspector General
Office of Emergency Management Oversight

SUBJECT: *FEMA Continues to Experience Challenges in
Protecting Personally Identifiable Information
at Disaster Recovery Centers*
Audit Report Number OIG-16-102-D

We issued this advisory report to notify the Federal Emergency Management Agency (FEMA) of a condition that requires its immediate attention. We are currently auditing FEMA's initial response to wildfires that occurred from September 9, 2015, to October 30, 2015, in Lake and Calaveras Counties, California. During our deployment to this disaster (DR-4240-CA), we observed that FEMA personnel at Disaster Recovery Centers¹ were not protecting personally identifiable information (PII) as Federal guidelines require. We discussed our observations with FEMA officials at the Joint Field Office² during our deployment and with FEMA's Privacy Officer in December 2015. In this report, we make recommendations to FEMA for ensuring the proper handling of PII in future disasters.

¹ A Disaster Recovery Center is a facility for applicants to obtain information about FEMA or other disaster assistance programs, such as small business loans, administered by the U.S. Small Business Administration.

² The Joint Field Office provides a temporary field facility to co-locate staff and facilitate functions of existing multiagency coordinating centers by integrating the processes of the relevant jurisdictions into a unified organizational structure. This facility accommodates all entities essential to incident management, information sharing, and the delivery of disaster assistance and other support.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Background

On September 9, 2015, wildfires swept through several communities in Northern California and continued to burn for at least 3 weeks. To provide Federal assistance to the people affected by the fire, the President signed a major disaster declaration (DR-4240-CA) on September 22, 2015, for Individual Assistance.³ On October 8, 2015, FEMA amended the declaration to include Federal assistance under the Public Assistance Program.⁴ Within 9 days of the declaration, FEMA opened a Joint Field Office and three Disaster Recovery Centers. Disaster Recovery Centers help survivors apply for Federal assistance (see figure 1). From October 28, to November 23, 2015 (date Disaster Recovery Centers closed), FEMA processed and collected PII from approximately 4,000 applicants at the centers.

Figure 1: FEMA Recovery Center for Disaster 4240, Middletown, California



Source: Department of Homeland Security (DHS) Office of Inspector General (OIG)

³ FEMA's Individual Assistance program provides housing assistance and assistance for medical, funeral, and transportation expenses to eligible individuals who, because of a federally declared major disaster or emergency, have necessary expenses and serious needs that are unmet through insurance or other means.

⁴ FEMA's Public Assistance program awards grants to state, local, and tribal governments and certain private non-profit entities to assist them with the response to and recovery from disasters.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

DHS defines PII as “any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to that individual.” Table 1 provides examples of the type of PII FEMA collects from individuals at disasters.

Table 1: Examples of PII

1. Name, telephone numbers, email, and home address
2. Social Security Number
3. Alien Registration number
4. Driver’s license or Passport number
5. Financial and medical records
6. Account numbers

Source: DHS OIG

Results of Audit

During our deployment to the 2015 California wildfire disaster, we observed that FEMA personnel at Disaster Recovery Centers did not properly safeguard PII, as Federal guidelines require. The mishandling of PII increases the risk of identity theft and can result in substantial harm, embarrassment, inconvenience, or unfairness to individuals. We also determined that some FEMA officials are not fully aware of Federal privacy standards. Moreover, FEMA management and trainers lack an effective method to track employee compliance with privacy training or to promote privacy awareness at disaster relief sites.

In May 2013, we reported similar deficiencies. As a result, FEMA officials stated that they would implement corrective actions, including conducting privacy compliance inspections at all disaster relief sites. However, FEMA officials at Disaster Recovery Centers for the 2015 California wildfire disaster were not aware of any privacy compliance inspections conducted at this disaster. While FEMA has made significant progress in developing a culture of privacy protection, it clearly needs to do more to safeguard private information at these sites.

Challenges Handling PII

We visited Disaster Recovery Centers located in Middletown and San Andreas, California, on October 14, 2015, and October 23, 2015, respectively, and observed that FEMA’s handling of PII did not meet Federal privacy and security standards. The *Privacy Act of 1974* requires agencies to implement administrative, physical, and technical safeguards to ensure the security and confidentiality of records. Specifically, we observed that FEMA did not equip the centers with lockable containers for safeguarding PII. Instead, it stored PII



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

records in open, unsecured cardboard boxes. We also observed PII records in file folders sitting on top of tables.

Officials at the centers said that FEMA seldom supplies Disaster Recovery Centers with qualified equipment to safeguard or dispose of PII, including secured document containers or bins, or shredders approved by the General Services Administration (GSA). These officials added that, without qualified disposal equipment, they must send PII collected from Disaster Recovery Centers by contract courier to the Joint Field Office for proper disposal.

We informed FEMA officials of our PII observations on November 25, 2015, when we returned to complete our audit field work. However, FEMA had closed the last Disaster Recovery Center by November 23, before our return visit. FEMA officials explained that they had expected to keep the Disaster Recovery Centers open through January 2016, but by early November, the number of applicants visiting Disaster Recovery Centers sufficiently declined for FEMA to make the decision to close them. As a result, FEMA did not have an opportunity to take corrective actions on mishandling of PII as it pertained to the Disaster Recovery Centers. We did not observe any mishandling of PII at the Joint Field Office.

Lack of Awareness of Federal PII Requirements

FEMA officials at the Disaster Recovery Centers had some knowledge of proper methods for handling PII, but were not fully aware of all applicable Federal standards. For instance, officials did not know that they were responsible for ensuring Disaster Recovery Centers were properly equipped to safeguard and dispose of PII.

The DHS Privacy Office, *Guide to Implementing Policy*, Section 3.1 (June 2010), states that all FEMA staff shall be aware of and comply with the *Privacy Act* and ensure that information about individuals is collected, maintained, used, and disseminated in accordance with the *Privacy Act* and DHS rules. Moreover, the *DHS Handbook for Safeguarding Sensitive PII*, Appendix C, (1) *How to Safeguard Sensitive Personally Identifiable Information (March 2012)*, requires that FEMA employees, contractors, consultants, interns, and temporary employees properly collect, access, use, share, and dispose of PII to protect the privacy of individuals.

FEMA officials' lack of expertise in handling PII increases the risk that applicants may be subject to identity theft. In addition, the mishandling—such as loss, compromise, or unauthorized disclosure—of PII can result in substantial harm, embarrassment, inconvenience, or unfairness to individuals.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Unreliable Methods for Training and Promoting Privacy Awareness

We found that FEMA did not provide management or training officials with a reliable method to track mandatory training or promote privacy awareness. Specifically, FEMA officials were unable to ensure that personnel had completed mandatory annual training such as Privacy at DHS: *Protecting Personally Identifiable Information*.

In May 2013, we reported similar deficiencies in privacy training and awareness.⁵ FEMA responded by stating it would implement corrective actions, including conducting privacy compliance inspections using a framework applicable at all FEMA locations including disaster relief sites. However, FEMA officials at Disaster Recovery Centers for the 2015 California wildfires said they were not aware of any privacy compliance inspections at this disaster.

Improvements Needed to Safeguard PII at Disaster Sites

While FEMA has made significant progress in developing a culture of privacy protection, it needs more work to increase the privacy footprint at disaster relief sites. In response to our May 2013 audit report, FEMA developed corrective action plans to—

- create privacy awareness throughout the agency;
- establish a FEMA Privacy Office Disaster Operations Branch;
- outline a Privacy Compliance Site Assessment process and tool to assess the privacy compliance of disaster relief facilities, systems, processes, programs, and procedures; and
- provide specialized privacy training that is better tailored for the disaster relief workforce.

In July 2013, we closed all recommendations from the May 2013 report based on documentation that FEMA had completed these actions. While FEMA's actions may have increased the agency's protection of PII under normal operating conditions, FEMA clearly needs to take additional steps to protect PII at disaster sites.

⁵ *Federal Emergency Management Agency Privacy Stewardship* (OIG-13-87), issued May 1, 2013.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Recommendations

We recommend that the Associate Administrator, FEMA Office of Response and Recovery:

Recommendation 1: Ensure that all employees, contractors, consultants, and other personnel at FEMA disaster relief sites—

- are aware of, and comply with, their responsibilities to safeguard and dispose of PII in accordance with Federal standards, DHS Management Directives, and FEMA guidelines;
- comply with all applicable privacy principles; and
- annually complete mandatory privacy awareness training.

Recommendation 2: Ensure all disaster relief sites receive a timely privacy compliance assessment.

Discussion with Management and Audit Follow-Up

We discussed our observations with FEMA officials at the Joint Field Office during our audit and included their comments in this report, as appropriate. We also provided a draft report in advance to these officials on February 8, 2016, and discussed it at an exit conference with FEMA officials on March 15, 2016. FEMA officials agreed with the findings.

FEMA officials provided a written response on April 21, 2016, agreeing with our findings and recommendations (see appendix B). FEMA expects to complete its proposed corrective actions to address our recommendations by April 30, 2017. Therefore, we consider the two report recommendations to be resolved but open. We will close these recommendations when we receive and review documentation that FEMA has completed its proposed corrective actions. Please email closeout documentation and request to Humberto.Melara@oig.dhs.gov.

The Office of Emergency Management Oversight major contributors to this report are Humberto Melara, Director; Louis Ochoa, Audit Manager; Renee Gradin, Auditor-in-charge; and Paul Sibal, Auditor.

Please call me with any questions at (202) 254-4100, or your staff may contact Humberto Melara, Director, Western Regional Office, at (510) 637-1463.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix A

Objective, Scope, and Methodology

We are currently auditing FEMA's initial response to wildfires that occurred from September 9, 2015, to October 30, 2015, in Lake and Calaveras Counties, California. The overall objective of our audit is to determine whether FEMA's initial response to the California wildfires is effective, and to evaluate FEMA's actions, resources, and authorities according to Federal regulations and FEMA guidelines in effect at the time of our fieldwork. The purpose of this advisory report is to notify FEMA of conditions we observed during our deployment to this disaster (DR-4240-CA). At the conclusion of our audit, we plan to issue our complete audit report, including any additional findings and recommendations.

To accomplish our objective, we deployed to the disaster on October 7, 2015. We co-located at the Joint Field Office in Sacramento, California, with FEMA officials and based our operations at that office as practicable. We interviewed officials within FEMA Senior Leadership (Federal Coordinating Officer and Disaster Recovery Coordinator); FEMA Section Leadership (Operations, Logistics, Planning, and Finance and Administration); FEMA Privacy Officer; FEMA Security Manager; FEMA Office of External Affairs; FEMA Infrastructure Branch Director; and FEMA Individual Assistance Branch Director.

We conducted fieldwork activities at the Joint Field Office (Sacramento, California); FEMA Area Field Office (San Andreas, California); Disaster Recovery Centers (Middletown, and San Andreas, California); and California Office of Emergency Services (Mather, California). We reviewed FEMA reports specific to the disaster; a previous OIG audit report related to mishandling of PII (OIG-13-87) and documents FEMA provided in response to that audit; the *Privacy Act*, and other statutes and Federal regulations applicable to this audit. We also performed other procedures considered necessary to accomplish our objective(s). We did not assess the adequacy of FEMA's internal controls applicable to disaster response because it was not necessary to accomplish our audit objective.

We are conducting this performance audit 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objective. We are conducting this audit by applying the statutes, regulations, and FEMA policies and guidelines in effect at the time of the disaster.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B

FEMA Comments to the Draft Report

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

 **FEMA**

APR 21 2016

MEMORANDUM FOR: John V. Kelly
Assistant Inspector General
Office of Emergency Management Oversight

FROM: David Bibo 
Associate Administrator (Acting)
Office of Policy and Program Analysis

SUBJECT: FEMA's Response to the Management Advisory Report:
"FEMA Continues to Experience Challenges in Protecting Personally Identifiable Information at Disaster Recovery Centers" (OIG-16-013)

Thank you for the opportunity to review and comment on this Draft Management Advisory Report, "FEMA Continues to Experience Challenges in Protecting Personally Identifiable Information at Disaster Recovery Centers." FEMA is grateful for the Office of Inspector General's (OIG) work in conducting its review and issuing this Draft Report.

FEMA appreciates the OIG's recognition of the significant progress the Agency has made in developing a culture of privacy protection. As FEMA continues to promote privacy awareness and improve compliance with Federal privacy standards, it has instituted various short and long term initiatives to engage FEMA leadership and staff in achieving these goals.

These initiatives have already shown an increase of over 4,000 FEMA employees and reservists trained in privacy awareness. FEMA concurs with the two (2) recommendations contained in the report and has established a corrective action plan to address both recommendations.

Recommendation 1: Ensure that all employees, contractors, consultants, and other personnel at FEMA disaster relief sites –

- Are aware of, and comply with, their responsibilities to safeguard and dispose of PII in accordance with Federal standards, DHS Management Directives, and FEMA guidelines;
- Comply with all applicable privacy principles; and
- Annually complete mandatory privacy awareness training.

www.fema.gov



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B (continued)

Response: Concur. FEMA has taken action to raise awareness of the importance of protecting privacy and personal information with senior leadership. On March 16, 2016, the FEMA Privacy Office conducted a privacy briefing and training with Missouri Field Leadership Cadre (which included the Federal Coordinating Officer and all leadership personnel assigned to the Missouri Floods Disaster). All FEMA Federal Coordinating Officers received a brief on how to implement an effective privacy program at disaster sites on April 6, 2016.

To ensure long term compliance and achieve the goals of Recommendation 1, FEMA will expand the Privacy Office's current Privacy Points of Contact (PPOC) program to serve as an extension of the FEMA HQ Privacy Office during disaster operations (i.e., at Joint Field Offices (JFOs), Branch Offices, Disaster Recovery Centers (DRCs), etc.). This function will be integrated into the existing disaster operations infrastructure to ensure that every disaster has at least one designated PPOC.

The expanded PPOC effort will employ a "Train-the-Trainer" approach whereby appointed and trained PPOCs will provide privacy training and resource materials to the disaster cadre to ensure they are equipped with the tools and working knowledge needed to minimize privacy risks during disaster operations. Duties and responsibilities of the PPOCs will include:

- Providing periodic and "just-in-time" privacy training/briefings to the disaster cadre being mobilized for deployment to disaster sites;
- Ensuring privacy resource materials (i.e., poster, privacy data cover sheets, training slides, and other materials) are disseminated to the disaster cadre; and
- Conducting privacy compliance site assessments to ensure that privacy protections are being implemented.

Complementing the privacy awareness training included among FEMA's suite of mandatory annual trainings, the expanded PPOC approach will reinforce the importance of protecting privacy and personal information and ensure that disaster operations personnel are trained and aware of their responsibilities to protect privacy and personal information. Likewise, it will facilitate a standard approach to privacy oversight at every disaster.

The FEMA Privacy Office will actively track workforce compliance with the mandatory privacy awareness training accessible through the FEMA Employee Knowledge Center.

Finally, the FEMA Privacy Office will continue to engage the Office of Response and Recovery (ORR), Individual Assistance Division, Field Operations Directorate, and other stakeholders to ensure privacy is being considered and implemented at all hierarchical levels of the disaster operations framework, to include the initial stand-up of each disaster operations site (i.e., JFOs, DRCs, Branch Offices, etc.).



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B (continued)

Interim Milestones	Estimated Completion Date	Status
1. Incorporate privacy resource materials into Disaster Recovery Center set-up kits.	February 2016	Complete
2. Conduct Agency-wide privacy awareness training refresh with goal of 100% compliance	April 15, 2016	In progress
3. Develop PPOC for Disaster Operations Program Delivery Curriculum and Guide	June 30, 2016	In progress
4. Incorporate PPOC for Disaster Operations function into existing disaster cadre Operational Concept and Position Task Book to formalize the role	September 30, 2016	In progress
5. Appoint and train PPOCs for Disaster Operations	January 30, 2017	To be completed
6. Mobilize PPOCs for Disaster Operations so they are ready for deployment	April 30, 2017	To be completed

Estimated Completion Date (ECD): April 30, 2017.

FEMA considers this recommendation resolved and open.

Recommendation 2: Ensure all disaster relief sites receive a timely privacy compliance assessment.

Response: Concur. In response to the recommendations from the 2013 FEMA Privacy Stewardship audit, the FEMA Privacy Office developed a framework for conducting privacy compliance site assessments applicable to all FEMA locations, including disaster relief sites. FEMA is expanding the PPOC program to serve as an extension of the FEMA HQ Privacy Office at disaster relief sites to ensure compliance site assessments are performed at all disaster relief sites as soon as possible after stand-up, PPOC's duties and responsibilities, include:

- Providing privacy training/briefings and resource materials to the cadre being mobilized for deployment;
- Ensuring privacy resource materials (i.e., poster, privacy data cover sheets, training slides, and other materials) are disseminated to the disaster cadre; and
- Conducting privacy compliance site assessments to ensure that privacy protections are being implemented.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix B (continued)

The FEMA Privacy Office, ORR-Field Operations Directorate and the Office of the Chief Security Officer will integrate the PPOC disaster operations function into the security cadre's operational concept and position task book. The FEMA Privacy Office will also engage with the field and security cadre, through outreach and training, to ensure these groups better understand privacy protection risks and safeguards, how to perform their new training/briefing, and privacy compliance assessment responsibilities.

Interim Milestones	Estimated Completion Date	Status
1. Incorporate privacy resource materials into Disaster Recovery Center set-up kits.	February 2016	Complete
2. Brief all FEMA Federal Coordinating Officers on how to implement an effective privacy program at disaster sites and the PPOC for the Disaster Operations program.	April 5, 2016	Complete
3. Develop PPOC for Disaster Operations Program Delivery Curriculum and Guide	June 30, 2016	In progress
4. Incorporate PPOC for Disaster Operations function into existing disaster cadre Operational Concept and Position Task Book to formalize the role	September 30, 2016	To be completed
5. Appoint and train PPOCs for Disaster Operations	January 30, 2017	To be completed
6. Mobilize PPOCs for Disaster Operations so they are ready for deployment	April 30, 2017	To be completed

ECD: April 30, 2017

FEMA considers this recommendation resolved and open.

Thank you for the opportunity to comment on this Draft Management Advisory Report. Please contact Gary McKeon, FEMA's Audit Liaison Office Director, at (202) 646-1308, if you have any questions. We look forward to working with you in the future.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix C

Report Distribution

Department of Homeland Security

Secretary
Chief of Staff
Chief Financial Officer
Under Secretary of Management
Executive Secretary
Chief Privacy Officer
Audit Liaison, DHS

Federal Emergency Management Agency

Administrator
Chief of Staff
Chief Financial Officer
Chief Counsel
Chief Procurement Officer
Privacy Officer
Associate Administrator, Response and Recovery
Director, Risk Management and Compliance
Regional Administrator, Region IX
Audit Liaison, FEMA (Job Code G-16-013)
Audit Liaison, FEMA Region IX

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.



OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305