OFFICE OF INSPECTOR GENERAL

Management Alert – FEMA Did Not Safeguard Disaster Survivors' Sensitive Personally Identifiable Information (REDACTED)

Homeland Security

March 15, 2019

OIG-19-32

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

March 15, 2019

MEMORANDUM FOR: Peter T. Gaynor
Acting Administrator
Federal Emergency Management Agency

FROM: John V. Kelly
Acting Inspector General

SUBJECT: *Management Alert – FEMA Did Not Safeguard Disaster Survivors' Sensitive Personally Identifiable Information – ~~For Official Use Only~~*

For your action is our *Management Alert – FEMA Did Not Safeguard Disaster Survivors' Sensitive Personally Identifiable Information – ~~For Official Use Only~~*. We considered technical comments and incorporated the formal comments provided by your office.

This alert contains two recommendations directing actions Federal Emergency Management Agency (FEMA) should take to safeguard both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII) of disaster survivors and prevent additional privacy incidents similar to one we identified during our ongoing audit of FEMA's Transitional Sheltering Assistance (TSA) program. FEMA concurred with both recommendations.

Based on information provided in your response to the draft alert, we consider the recommendations resolved and open. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions.

Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our alert to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post a redacted version of the alert on our website.

Please call me with any questions, or your staff may contact Sondra McCauley, Assistant Inspector General for Audits, at (202) 981-6000.

Results in Brief

During our ongoing audit of the Federal Emergency Management Agency's (FEMA) Transitional Sheltering Assistance (TSA) program, we determined that FEMA violated the *Privacy Act of 1974*[1] and Department of Homeland Security policy[2] by releasing to [redacted] the PII and SPII of 2.3 million survivors of hurricanes Harvey, Irma, and Maria and the California wildfires in 2017.[3] FEMA should only provide [redacted] with limited information needed to verify disaster survivors' eligibility for the TSA program. The privacy incident[4] occurred because FEMA did not take steps to ensure it provided only required data elements to [redacted] Without corrective action, the disaster survivors involved in the privacy incident are at increased risk of identity theft and fraud.

Background

Through the TSA program, FEMA provides transitional sheltering in hotels to disaster survivors displaced by emergencies or major disasters. TSA reduces the number of survivors in congregate emergency shelters by providing hotel lodging. The contractor administering the TSA program, [redacted] helps disaster survivors obtain short-term lodging at participating hotels. FEMA identified more than 2.3 million disaster survivor registrants eligible for the TSA program during the response to hurricanes Harvey, Irma, and Maria, and the California wildfires in 2017.

When applying for FEMA disaster assistance, applicants are required to provide PII and SPII. *The Privacy Act of 1974* (the Act) protects individuals by ensuring personal information collected by Federal agencies is limited to what is legally authorized and necessary. The Act also dictates that agencies maintain PII and SPII to preclude unwarranted intrusions upon individual privacy. DHS'

[1] Privacy Act of 1974, 5 USC 552a, as amended
[2] DHS Management Directive 11042.1 - Safeguarding Sensitive but Unclassified (For Official Use) Information (January 6, 2005)
[3] Hurricane Harvey (DR-4332); Hurricane Irma (DR-4336 in Puerto Rico; DR 4337 in Florida); Hurricane Maria (DR-4339); and the California Wildfires (DR-4344)
[4] A privacy incident is defined as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence when (1) a person other than the authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an unauthorized purpose. The term encompasses both suspected and confirmed incidents involving PII, whether intentional or inadvertent, which raises a reasonable risk of harm. The term "privacy incident' can be used synonymously with the term "breach" (DHS Privacy Policy Instruction 047-01-008, Privacy Incident Handling Guidance).

Handbook for Safeguarding Sensitive Personally Identifiable Information (December 2017) defines these terms as follows:

- Personally Identifiable Information (PII) is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor to the Department. This includes complete name, home address, and birthdate when combined.

- Sensitive PII (SPII) is a subset of PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. SPII requires stricter handling guidelines because of the increased risk to an individual if the data are compromised. This includes financial account information.

As required by the *E-Government Act of 2002*, FEMA completed a Privacy Impact Assessment for the Individual Assistance Program, which includes the TSA program. The assessment identifies the PII, including SPII that will be collected from applicants, and includes details on the use of this information in implementing FEMA's Individual Assistance programs.

Additionally, DHS' *Handbook for Safeguarding Sensitive PII* (December 4, 2017) states that only PII necessary for agency staff to perform their official duties should be collected, used, and disseminated to individuals on a need-to-know basis.

Survivor Information at Risk

FEMA released unnecessary PII and SPII for approximately 2.3 million disaster survivors to its contractor, [redacted] in direct violation of Federal and DHS requirements and its August 2015 TSA program *Performance Work Statement.* The *Performance Work Statement* identifies 13 data elements FEMA must send to [redacted] to verify disaster survivor eligibility during the TSA check-in process at participating hotels. Some of the data elements contain PII, but none of the individual data elements contain SPII.[5] The data elements that FEMA must share include:

[5] Some data elements by themselves rise to a level of SPII (called standalone SPII), while other data elements of PII grouped together jointly rise to the level of SPII.

- Applicant First Name
- Applicant Middle Name
- Applicant Last Name
- Applicant Date of Birth
- Last 4 digits of Applicant's Social Security Number
- Disaster Number
- Authorization for TSA
- Number of Occupants in Applicants Household
- Eligibility Start Date
- Eligibility End Date
- Global Name
- Export Sequence Number
- FEMA Registration Number

A privacy incident occurred because FEMA did not ensure it shared with the contractor only the data elements the contractor requires to perform its official duties administering the TSA program. FEMA provided and continues to provide [redacted] with more than 20 unnecessary data fields for survivors participating in the TSA program. Of the 20 unnecessary data fields, FEMA does not safeguard and improperly releases 6 that include SPII:

- Applicant Street Address
- Applicant City Name
- Applicant Zip Code
- Applicant's Financial Institution Name
- Applicant's Electronic Funds Transfer Number
- Applicant's Bank Transit Number

FEMA's *Performance Work Statement* identified the data elements [redacted] needed, yet FEMA did not take steps to ensure it provided only the required data elements. FEMA only confirmed that [redacted] received the data transmitted. Prior iterations of the TSA program required additional information such as bank names and account numbers; however, the current TSA program does not require the additional personal information.

FEMA headquarters officials told us it may be feasible to change the data transfer script to remove the unnecessary PII, but such change would need to be coordinated with the Individual Assistance and Mass Care program offices, which may be time consuming.

[redacted] also did not notify FEMA that it was providing information unnecessary to fulfilling the contract terms. Although not required to do so, had [redacted] officials notified FEMA officials that the agency was providing unnecessary PII and SPII

for eligible survivors, FEMA may have been able to remedy this situation earlier and avoid additional privacy incidents.

FEMA's failure to provide only required data elements to [redacted] has placed approximately 2.3 million disaster survivors at increased risk of identity theft and fraud. FEMA must take corrective action to safeguard against improperly releasing PII and SPII of disaster survivors in the future.

Recommendations

Recommendation 1: We recommend that the Federal Emergency Management Agency's Assistant Administrator for the Recovery Directorate implement controls to ensure that the agency only sends required data elements of registered disaster survivors to contractors, such as [redacted].

Recommendation 2: We recommend that the Federal Emergency Management Agency's Assistant Administrator for the Recovery Directorate assess the extent of this privacy incident and implement a process for ensuring that Personally Identifiable Information, including Sensitive Personally Identifiable Information, of registered disaster survivors previously released to [redacted] is properly destroyed pursuant to DHS policy.

Management Comments and OIG Analysis

FEMA concurred with our two recommendations. We included a copy of the Department's management comments in their entirety in appendix A. We also received technical comments to the draft report and revised the report as appropriate.

In its written comments, FEMA indicated it has begun to implement measures to assess and mitigate this privacy incident, including deploying a Joint Assessment Team of cyber security personnel to the contractor's facilities. FEMA indicated that the Joint Assessment Team had documented the sanitization and removal of the unnecessarily shared PII and SPII from the contractor's system and performed an in-depth assessment of the contractor's network. According to FEMA, these assessments found no indication of intrusion within the last 30 days although the assessment identified that the contractor did not maintain logs past 30 days. The Joint Assessment Team also identified several security vulnerabilities. As of March 2019, four vulnerabilities had been remediated and the contractor was developing remediation plans for the remaining seven. FEMA's estimated completion date for implementing the recommendations is June 30, 2020. Given the sensitive nature of these

findings, we urge FEMA to expedite this timeline.

FEMA Response to Recommendation 1: Concur. In agreement with OIG's observations, FEMA determined that numerous elements constituting SPII were not necessary to administer the TSA program. FEMA stated it had implemented immediate measures to discontinue sharing the unnecessary data and had begun an on-site assessment of [redacted] network.

Estimated Completion Date: June 30, 2020.

OIG Analysis: We consider these actions responsive to the recommendation. This recommendation is resolved and open until FEMA:

1) provides a report about the controls implemented to ensure that the agency only sends required data elements on registered disaster survivors to contractors;
2) provides a report on the final outcome of the on-site assessment of [redacted] network;
3) provides copies of the contract amendments, including the Homeland Security Acquisition Regulation clause requiring annual privacy and security awareness training of [redacted] staff; and
4) provides a report on FEMA's annual privacy and security training of FEMA employees to mitigate future privacy incidents similar to the one we identified.

FEMA Response to Recommendation 2: Concur. FEMA's Office of the Chief Information Officer (OCIO) has begun taking corrective actions to conduct an on-site security and risk assessment of [redacted] data systems and network. Upon completion of initial assessment activities, FEMA worked with [redacted] to sanitize all previously transferred, non-required PII/SPII from [redacted] system. FEMA stated the OCIO will continue to assess [redacted] systems on a regular basis to assure [redacted] maintains a security posture in accordance with Federal security standards on handling PII/SPII, as well as the FEMA Records Retention Schedule covering this information.

Estimated Completion Date: June 30, 2020.

OIG Analysis: We consider these actions responsive to the recommendation. This recommendation is resolved and open until FEMA provides a report on its actions to mitigate this privacy incident and its ongoing assessments to ensure the contractor maintains a security posture in accordance with Federal standards for handling PII/SPII.

Objective, Scope, and Methodology

The DHS Office of Inspector General was established by the *Homeland Security Act of 2002*, Pub. L. No. 107–296, 116 Stat. 2135, which amended the *Inspector General Act of 1978*. We issued this management alert during an ongoing audit of FEMA's TSA program. The objective of our ongoing audit is to determine to what extent FEMA ensured compliance with contract requirements concerning the TSA program.

We conducted interviews in June 2018 with FEMA headquarters officials in charge of the TSA program; and in July 2018 with FEMA financial management, information technology, and contracting officials in Winchester, Virginia, to inform them of the privacy incident. We also interviewed state and FEMA officials in Texas, specifically concerning the use of the TSA program following Hurricane Harvey in 2017.

We reviewed Federal, DHS, and FEMA criteria related to transitional sheltering and contracting; TSA process workflows and standard operating procedures; [redacted] policies, procedures and other documentation; and TSA data from Hurricanes Harvey, Irma, and Maria (from August 2017 to August 2018), and California wildfires in 2017, including all eligible households, program recipients of TSA, and program costs.

We conducted our work under the *Inspector General Act of 1978*, as amended, Section 2.2(b), to promote economy, efficiency, and effectiveness in the administration of; and to prevent and detect fraud and abuse in, such programs and operations. This management alert focuses only on FEMA's release of PII and SPII. We are continuing this audit, so additional recommendations regarding this issue may be included in the full audit report. Any corrective actions FEMA takes in response to this management alert will be addressed in our full audit report.

Office of Audits major contributors to this management alert are Yesi Starinsky, Director; Andrew Smith, Audit Manager; David Kinard, Auditor-in-Charge; Keith Lutgen, Program Analyst; Haidee Lai, Auditor; Edward Brann, Program Analyst; Daniel Malone, Program Analyst; Deborah Mouton-Miller, Communications Analyst; and John Skrmetti, Independent Report Referencer.

Appendix A
FEMA Comments to the Draft Alert

FOR OFFICIAL USE ONLY

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

FEMA

March 8, 2019

MEMORANDUM FOR: John V. Kelly
Senior Official Performing the Duties of the
Inspector General

FROM: Joel Doolin
Associate Administrator
Office of Policy and Program Analysis

SUBJECT: Management Response to Draft Report: "Management Alert – FEMA Did Not Safeguard Disaster Survivors' Sensitive Personally Identifiable Information" (Project No. OIG-18-082)

Thank you for the opportunity to review and comment on this draft report. The Federal Emergency Management Agency (FEMA) appreciates the work of the Office of Inspector General (OIG) in conducting its review and issuing this report.

FEMA has taken aggressive action to mitigate the issues raised within this report and strengthen the protection of survivor data. For example, upon the receipt of OIG's draft report on November 9, 2018, FEMA acted immediately to stop the flow of excess data and ensure the continued safeguarding of disaster survivors' Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). FEMA considers any unnecessary sharing of survivor data to be a serious matter and is dedicating substantial resources to address this issue, as appropriate.

Significant additional progress has also been made during the last four months to further mitigate the issued identified in the draft report. This includes changing program practices and procedures; conducting substantial forensic analysis of contractor information systems; providing technical assistance to our contractor to remove unneeded data and upgrade protection of data; and updating and changing contract terms and conditions. As a result of these actions, FEMA's safeguarding of information used to administer the Transitional Sheltering Assistance (TSA) program has substantially improved.

FOR OFFICIAL USE ONLY

1

FEMA's TSA program provides short-term lodging assistance for disaster survivors who are not able to return home for an extended or indeterminate period of time following a disaster. Disaster survivors eligible for the program are notified by FEMA and may then check into a participating lodging provider. The costs of the room and taxes are paid by FEMA and the State. Any other expenses remain the responsibility of the disaster survivor.

In certain disaster responses, TSA serves as a critical element of the strategy to provide support to survivors. In 2017, the program provided more than 4.9 million room nights through program activations in North Carolina, Texas, Florida, Puerto Rico, and California. To facilitate these rooms stays, FEMA must transfer certain elements of disaster survivor data to its contracted lodging provider.

In a previous version of the TSA program, FEMA required the temporary lodging payment process to include a capability for direct reimbursement of disaster survivors. This iteration of TSA, known as the TSA-Reimbursable Program (TSAR), required the provision of additional applicant data to the contractor, including bank account information. However as noted in OIG's report, this information is no longer necessary to administer TSA and this data was unnecessarily shared with the contractor.

As part of the response to the report, FEMA conducted a review of all data elements shared from FEMA to the contractor. In agreement with the OIG's observations, FEMA determined that elements which constitute SPII were not necessary for administering TSA. FEMA implemented immediate measures to discontinue sharing the unnecessary data and confirmed that unnecessary data fields were no longer being transferred to the contractor as of December 7, 2018. FEMA and DHS also deployed a Joint Assessment Team (JAT), consisting of incident response cybersecurity professionals from the FEMA Security Operations Center and the Department's Enterprise Security Operations Center, on two separate occasions to the contractor's corporate and data center locations. The first visit was to conduct a policy and compliance assessment. This visit included documenting the sanitization and removal from the contractor's information systems of the data that had been unnecessarily shared, which was completed December 21, 2018. The second visit focused on an in-depth security assessment of the contractor's network which included a compromise, vulnerability and penetration assessment. This visit was conducted February 12-23, 2019. The results were twofold: (1) JAT found no indicators of compromise of survivor data from the duration of the on-site continuous monitoring and review of the logs from the previous 30 days as the contractor did not retain logs beyond 30 days; and (2) JAT found the network to be of moderate risk with eleven (11) security vulnerability findings as stated below. Four (4) have been remediated and the contractor is developing remediation plans for the seven (7) open findings.

- Compromise Assessment (HUNT) (3 findings / 1 remediated)
- Vulnerability Assessment Team (VAT) (4 findings / 0 remediated)
- Penetration Testing (4 findings / 3 remediated)

~~FOR OFFICIAL USE ONLY~~

FEMA also performed unilateral modification to contract terms and conditions to incorporate required cyber security clauses on December 7, 2018. These clauses establish the contractor's responsibility for robust cybersecurity practices in all phases of program administration and mandates that the most current DHS privacy training is conducted as related to the management of Personally Identifiable Information and Sensitive Personally Identifiable Information and sustained on an annual basis. In addition to addressing the 11 findings, the contractor has taken additional actions to become compliant with the updated cybersecurity requirements in the contract and communicate any changes (technical and process) they have made based on the JAT recommendations. The contractor is also capturing all changes in the updated security documentation.

The draft report contained two recommendations with which FEMA concurs. Attached is our detailed response to each recommendation. Technical comments were previously provided under separate cover.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Attachment

~~FOR OFFICIAL USE ONLY~~

3

FOR OFFICIAL USE ONLY

Attachment: Management Response to Recommendations Contained in OIG-18-082

The OIG recommended that FEMA's Branch Chief for Mass Care:

Recommendation 1: Implement controls to ensure that the agency only sends required data elements of registered disaster survivors to contractors, such as [redacted]

Response: Concur. FEMA's Office of Response and Recovery has taken or will take the following corrective actions in response to this Recommendation:

1. FEMA has discontinued sharing non-required PII data with [redacted] FEMA deployed a filter on December 4, 2018 and December 7, 2018. The filter prevents unnecessary PII/SPII from leaving FEMA's system of record for those survivors newly identified as TSA eligible.
2. FEMA updated its agreements with [redacted] to ensure compliance with current DHS information technology standards on December 7, 2018. FEMA will amend its [redacted] contract document(s) to include a Homeland Security Acquisition Regulation clause, thereby requiring annual privacy and security awareness training by [redacted] staff.

Estimated Completion Date (ECD): June 30, 2020.

Recommendation 2: Assess the extent of this privacy incident and implement a process for ensuring that PII/SPII, of registered disaster survivors previously released to [redacted] is properly destroyed pursuant to DHS policy.

Response: Concur. FEMA's Office of the Chief Information Officer (OCIO) has taken or will take the following corrective actions in response to this Recommendation:

1. FEMA OCIO deployed internal resources, via the FEMA Security Operations Center and the Department's Enterprise Security Operations Center, to conduct an on-site security and risk assessment of [redacted] data systems and network on December 7, 2018. A second security and risk assessment was conducted from February 12 – February 23, 2019.
2. Upon completion of initial assessment activities, FEMA OCIO collaborated with [redacted] to sanitize all previously transferred EFT and non-required PII/SPII from [redacted] system; and
3. FEMA OCIO will continue to assess [redacted] systems on a regular basis to assure [redacted] maintains a security posture that is in accordance with federal security standards to manage the handling of PII/SPII, as well as the FEMA Records Retention Schedule that covers this information.

ECD: June 30, 2020.

FOR OFFICIAL USE ONLY

4

Appendix B
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
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
FEMA Audit Liaison

Congress

Congressional Oversight and Appropriations Committee

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