EDDIE BERNICE JOHNSON, Texas
CHAIRWOMAN

FRANK D. LUCAS, Oklahoma
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6301

(202) 225–6375
www.science.house.gov

April 4, 2019

The Honorable Pete T. Gaynor
Acting Administrator
Federal Emergency Management Agency
500 C Street SW
Washington, D.C. 20472

Dear Acting Administrator Gaynor,

The Committee on Science, Space, and Technology is conducting oversight of a recent privacy incident at the Federal Emergency Management Agency (FEMA). To assist the Committee's oversight of this important matter, we write to request a briefing on the privacy incident, its potential impacts on affected individuals, and FEMA's response.

On March 22, 2019, the Department of Homeland Security (DHS) Office of Inspector General (OIG) published a *Management Alert*[1] that revealed FEMA violated Federal law and DHS policy by inappropriately releasing to a contractor the PII and SPII[2] of 2.3 million disaster survivors—including survivors of the California wildfires in 2017, and hurricanes Harvey, Irma, and Maria.[3] The DHS OIG found that the privacy incident occurred because FEMA failed to employ proper controls to ensure it provided only required data elements to its contractor.[4] According to DHS OIG, absent corrective action, FEMA's error and the resulting privacy incident places roughly 2.3 million disaster survivors at increased risk of identity theft and fraud.[5] To assist the Committee's oversight of this matter, we write to request a briefing and information related to the privacy incident and FEMA's response and to determine if the Committee needs to conduct additional oversight through a document request related to the incident.

---

[1] Office of the Inspector General, *Management Alert – FEMA Did Not Safeguard Disaster Survivors' Sensitive Personally Identifiable Information*, U.S. DEPARTMENT OF HOMELAND SECURITY (Mar. 22, 2019), *available at* https://www.oig.dhs.gov/sites/default/files/assets/2019-03/OIG-19-32-Mar19.pdf. [hereinafter *Management Alert*].
[2] PII refers to personally identifiable information. SPII, or sensitive PII, 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.
[3] *See Management Alert* at 2.
[4] *Id.*
[5] *Id.*

FEMA's Transitional Sheltering Assistance (TSA) program provides short-term housing assistance for survivors that cannot return home for an extended or intermediate period of time following a disaster.[6] The initiative is intended to provide lodging for disaster survivors whose communities are uninhabitable or inaccessible due to disaster-related damages.[7] Disaster survivors eligible for the TSA program are notified by FEMA and can then check into a participating lodging provider, where room costs and taxes are paid by FEMA and the State.[8]

To facilitate these accommodations, FEMA must transfer certain elements of disaster survivor data to contracting lodging providers.[9] Specifically, FEMA is required to provide 13 data elements to its contractor to verify disaster survivor eligibility during the TSA check-in process.[10] Importantly, while some of the data elements that FEMA must provide contain PII, none contain SPII.[11] The DHS OIG, however, found that, "FEMA provided and continues to provide [its contractor] with more than 20 unnecessary data fields for survivors participating in the TSA program."[12] Moreover, of these unnecessary data fields, six contained disaster survivors' SPII, including: street address; city name; zip code; financial institution name; electronic funds transfer number; and bank transit number.[13] This is not acceptable.

The privacy incident at FEMA is particularly concerning to the Committee, as this sensitive information can be used to prey upon individuals in a variety of ways, including identity theft, fraud, targeted scams, and spear phishing. Unfortunately, fraud and scams abound in the wake of natural disasters as nefarious actors seek to capitalize on the misfortune of affected communities. Disaster survivors, as they navigate the significant amount of paperwork and logistics required to apply for assistance, pay medical bills, and find temporary lodging, are particularly vulnerable to these schemes. Of this fact FEMA is keenly aware. "After a disaster, scam artists, identity thieves, and other criminals often attempt to take advantage of vulnerable survivors," FEMA advises on its website.[14] The agency also warns, "Above all, do not give out any money or personal information unless you feel confident doing so."[15] This is sound advice, but it appears that FEMA has failed to practice what it preaches.

The Committee is also concerned this privacy incident may undermine survivors' confidence in their ability to safely and securely share their personal information with FEMA, which could unnecessarily delay survivors' access to the critical services FEMA provides. Given FEMA's warnings about identity theft, its release of sensitive data is all the more troubling. Instead of serving their stakeholders, FEMA has greatly increased the risk that identity theft and

---

[6] *See* Federal Emergency Management Agency, *Transitional Sheltering Assistance*, (Oct. 24, 2018), https://www.fema.gov/transitional-shelter-assistance.
[7] *See id.*
[8] *See id.*
[9] *See Management Alert* at 9.
[10] *See Management Alert* at 3.
[11] *See id.*
[12] *Management Alert* at 4.
[13] *See id.*
[14] Federal Emergency Management Agency, *Disaster Fraud*, (Oct. 19, 2018), https://www.fema.gov/disaster-fraud.
[15] Federal Emergency Management Agency, *Defend Against Disaster-Related Scams*, (Mar. 4, 2019), https://www.fema.gov/news-release/2019/03/04/defend-against-disaster-related-scams.

To help ameliorate the Committee's concerns, we ask that you provide Committee staff with a briefing about this privacy incident. The briefing should include specific details about why the privacy incident occurred, how the affected survivors may be impacted, and what steps FEMA has taken to prevent similar privacy incidents from occurring in the future. All attending presenters should also be prepared to discuss FEMA's adherence to the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and other NIST products governing proper controls for protecting PII. We ask that you or your designee provide this briefing as soon as possible, but no later than Thursday, April 18, 2019.

Pursuant to House Rule X, the Committee on Science, Space, and Technology has jurisdiction over the National Institute of Standards and Technology, which develops cybersecurity standards and guidelines for the Federal government and recommendations for the private sector. Additionally, under the Federal Information Security Modernization Act of 2014 (FISMA 2014), Federal departments and agencies are required to report to the Science Committee annually and circumstantially, in cases of a major cybersecurity breach. This request and any documents created as a result of this request will be deemed congressional documents and property of the House Science Committee.

If you have any questions about this request, please contact Tom Connally or Jenn Wickre of the Committee's minority staff at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Frank D. Lucas
Ranking Member

Bill Posey
Member of Congress

Randy Weber
Member of Congress

Brian Babin
Member of Congress

Roger Marshall
Member of Congress

Ralph Norman
Member of Congress

Michael Cloud
Member of Congress

Jim Baird
Member of Congress

Jennifer González Colón
Member of Congress

Cc: The Honorable Eddie Bernice Johnson, Chair, House Committee on Science, Space, and Technology