BENNIE G. THOMPSON, MISSISSIPPI
CHAIRMAN

MIKE ROGERS, ALABAMA
RANKING MEMBER

One Hundred Sixteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

March 29, 2019

The Honorable Peter T. Gaynor
Acting Administrator
Federal Emergency Management Agency
500 C St. SW
Washington, DC 20024-2523

Dear Acting Administrator Gaynor:

I was troubled to learn about the Federal Emergency Management Agency's (FEMA) release of millions of disaster survivors' personally identifiable information (PII) and sensitive PII (SPII) to a contractor.[1] It is particularly alarming that some of the data released included sensitive banking details of disaster survivors.

According to March 15, 2019 findings by the Department of Homeland Security Office of Inspector General (DHS OIG), FEMA unnecessarily shared PII and SPII of nearly 2.3 million individuals, all of whom were affected by natural disasters in 2017, including the California wildfires and Hurricanes Harvey, Irma, and Maria.[2]

While it is unclear whether this unfortunate event resulted in any survivor data being compromised, merely being exposed to the risk of identity theft and fraud compounds the stress of having gone through a disaster. It is completely unacceptable for the Federal government to place Americans' PII and SPII in jeopardy of exploitation by malicious actors, especially when these disaster survivors have already lost so much. Accordingly, please respond to the following inquiries by April 12, 2019:

1. FEMA advised my staff that those impacted by this privacy incident have not been notified. Is FEMA planning to issue notifications to disaster survivors whose PII and SPII were unnecessarily shared? If so, when will FEMA issue notifications, and how will these disaster survivors be notified?

2. What services or remedies will FEMA make available to disaster survivors whose PII and SPII were unnecessarily shared?

---

[1] "Management Alert—FEMA Did Not Safeguard Disaster Survivors' Sensitive Personally Identifiable Information (Redacted)," Office of the Inspector General, Department of Homeland Security. March 15, 2019. Accessed on March 25, 2019. Available at: https://www.oig.dhs.gov/sites/default/files/assets/2019-03/OIG-19-32-Mar19.pdf.
[2] Ibid.

3. FEMA advised my staff that the agency is "still assessing the contractor's technology environment." Please describe this process. How long will the assessment take? What party or parties are conducting the assessment? Have any conclusions been reached? Have any remedial actions been taken?

4. According to DHS OIG findings, the contractor was under no requirement to notify FEMA officials of the unnecessary sharing of PII and SPII; however, had the contractor provided earlier notification, the situation could have been remedied earlier. Has FEMA updated its policies for contractors providing notification to FEMA about unnecessary sharing of PII and SPII? If yes, please provide the updated policies. If no, please explain.

5. Has FEMA assessed whether any other disaster assistance program has overshared sensitive personal information? If yes, please detail the findings of the assessment. If no, please explain.

6. Please describe any controls FEMA has put in place to ensure that agency oversharing of survivor PII and SPII does not occur in the future.

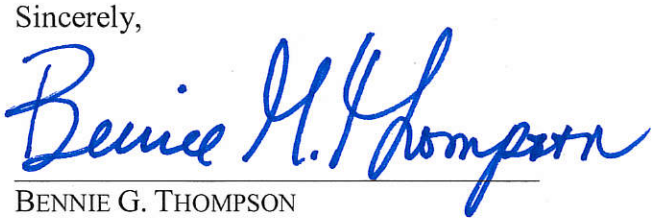
7. Please describe FEMA's efforts to ensure contractor compliance with the National Institute of Standards and Technology's Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

8. Following the Office of Personnel Management data breach in 2015, the Office of Management and Budget ordered agencies to identify and review the security of high-value assets, including those containing critical data attractive to bad actors as part of the "cyber sprint." Does FEMA consider PII and SPII to be critical data? During the "cyber sprint," did FEMA review the manner in which it collects, stores, and shares PII and SPII?

9. Please describe the data loss protection technology FEMA currently uses to limit unnecessary sharing of PII and SPII.

Thank you for your prompt attention to this important matter. If you have any questions or need additional information, please contact Alison Northrop, Oversight Director, at 202-226-2616.

Sincerely,



BENNIE G. THOMPSON
Chairman

cc: Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security