Privacy Compliance Review of the Federal Emergency Management Agency's Information Sharing Practices

October 21, 2019

Contact Point
Peter T. Gaynor
Acting Administrator
Federal Emergency Management Agency
(202) 646 3899

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

I. Background

The Department of Homeland Security (DHS) Privacy Office recently conducted a Privacy Compliance Review (PCR)[1] of the Federal Emergency Management Agency (FEMA) that focused on information sharing practices and oversight in response to two major privacy incidents[2] occurring during Fiscal Year (FY) 2019.

On November 30, 2018, DHS and FEMA determined that a major privacy incident occurred because of the oversharing of disaster survivors' personal information with a FEMA contactor as part of the Transitional Sheltering Assistance (TSA) program. This incident met the "major incident" threshold as defined in Section 3554(b)(7)(C)(iii)(III)(aa) of the Federal Information Security Modernization Act of 2014 (FISMA)[3] and in the Office of Management and Budget's (OMB) Memorandum M 19-02, due to the incident impacting 100,000 or more individuals' personally identifiable information (PII).

Separately, on January 17, 2019, DHS and FEMA determined that another major privacy incident occurred when FEMA took part in the unauthorized sharing of disaster survivors' PII with a non-governmental partner that conducts disaster response services. This incident was considered "major" as it also impacted more than 100,000 individuals' PII.

Since both of these major privacy incidents were the result of poor information sharing practices, the PCR's primary objective was to review internal FEMA guidance meant to ensure that individuals' privacy is adequately protected in information sharing and safeguarding activities. The DHS Privacy Office employs PCRs as a means of identifying and remediating privacy issues and promoting structural improvements in a cooperative, collaborative, and constructive manner. This report sets forth the DHS Privacy Office's findings and provides recommendations to protect privacy within FEMA's information sharing practices, particularly with how they relate to the major privacy incidents, as well as compliance with DHS Privacy Policy.

II. Scope and Methodology

Pursuant to Section 222(b) of the Homeland Security Act, the DHS Chief Privacy Officer (CPO) has the authority to investigate departmental programs and operations as they relate to privacy.[4] The DHS Privacy Office conducted this PCR to determine ways to improve FEMA's information sharing and safeguarding activities, while adequately protecting individuals'

---

[1] *See* DHS Instruction 047-01-004 for Privacy Compliance Reviews (January 2017), *available at* https://www.dhs.gov/publication/dhs-privacy-policy-instruction-047-01-004-privacy-compliance-reviews.
[2] A "major incident" is any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people as defined in OMB Memorandum M-19-02, *available at* https://www.whitehouse.gov/wp-content/uploads/2018/10/M-19-02.pdf.
[3] 44 U.S.C. § 3554(b)(7)(C)(iii)(III)(bb).
[4] *See* Homeland Security Act of 2002, Pub L. 107-296, 116 Stat. 2135 (November 25, 2002), as amended, *available at* https://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf.

privacy. To achieve that objective, the DHS Privacy Office reviewed FEMA's compliance with DHS information sharing policy and compliance with terms in the information sharing agreements associated with the two recent major privacy incidents from FY19. The primary focus for this PCR was on FEMA's adherence to privacy requirements set forth in:

1. DHS Information Sharing and Safeguarding Directive 262-05;
2. Privacy Policy Directive 140-06/The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security;[5]
3. Privacy Policy Guidance Memorandum 2017-01, DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information;[6]
4. DHS Directive 047-01 Privacy Policy and Compliance,[7] and DHS Instruction 047-01-001 Privacy Policy and Compliance;[8]
5. DHS Instruction 047-01-007, Handbook for Safeguarding Sensitive PII;[9] and
6. DHS Instruction 047-01-005 for Component Privacy Officers.[10]

As a threshold matter, the DHS Privacy Office recognizes FEMA's issuance of *FEMA Directive #262-1: Data Sharing* (FEMA Data Sharing Directive) and Implementation Plan that identifies privacy of a survivor's sensitive PII (SPII)[11] as a paramount principle.[12] Acting Administrator Gaynor's All Hands Memorandum of July 16, 2019, presents the FEMA Data Sharing Directive as complementary to other FEMA management policies that support a consistent, agency-wide process to what, when, and how FEMA shares data. The FEMA Data Sharing Directive and the associated Implementation Plan signify a commitment to rectifying gaps that put PII at risk by providing clear roles, responsibilities, and timelines for improvements to FEMA's information sharing processes. The findings and recommendations in this PCR complement and support FEMA's identified path forward.

---

[5] *See* Privacy Policy Directive: 140-06 (December 2008), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.
[6] *See* Privacy Policy Guidance Memorandum: 2017-01 (April 2017), *available at* https://www.dhs.gov/sites/default/files/publications/PPGM%202017-01%20Signed_0.pdf.
[7] *See* DHS Directive: 047-01 (July 2011), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-directive-047-01_0.pdf.
[8] *See* DHS Instruction: 047-01-001 (July 2011), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-instruction-047-01-001_0.pdf.
[9] *See* DHS Instruction: 047-01-007 (December 2017), *available at* https://www.dhs.gov/sites/default/files/publications/dhs%20policy%20directive%20047-01-007%20handbook%20for%20safeguarding%20sensitive%20PII%2012-4-2017.pdf.
[10] *See* DHS Instruction: 047-01-005 (February 2017), *available at* https://www.dhs.gov/sites/default/files/publications/dhs%20policy%20instruction%20047-01-005%20Component%20Privacy%20Officer%20Privacy.pdf.
[11] SPII is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. *See* DHS Instruction: 047-01-007 (December 2017), *available at* https://www.dhs.gov/sites/default/files/publications/dhs%20policy%20directive%20047-01-007%20handbook%20for%20safeguarding%20sensitive%20PII%2012-4-2017.pdf.
[12] FEMA Directive #262-1: Data Sharing on file with the DHS Privacy Office.

In conducting the PCR, the DHS Privacy Office developed and submitted an extensive questionnaire designed to seek information and documentation about FEMA-issued information sharing policies and practices, to determine how they align with the Department policies cited above, as well as verify privacy safeguards described in relevant Privacy Impact Assessments (PIA). The DHS Privacy Office reviewed FEMA's responses including all supporting documentation and received briefings and demonstrations from FEMA subject matter experts.

The DHS Privacy Office conducted this PCR in coordination with personnel from FEMA's Privacy Branch, Office of Response and Recovery (ORR), Texas Regional Office, and the Office of Chief Counsel (OCC). The findings detailed in this report reflect conclusions reached by the DHS Privacy Office based on an assessment of FEMA-related information sharing agreements, privacy compliance documentation, exchanges with FEMA personnel, and an analysis of documents, responses, discussions, and other information received in response to this PCR.

In conducting this PCR, the DHS Privacy Office:

- Reviewed existing information sharing agreements and information sharing agreement templates;
- Reviewed FEMA Privacy compliance and policy documentation, with particular attention paid to:
  - DHS/FEMA/PIA-049 Individual Assistance (IA) Program;[13]
  - DHS/FEMA-008 Disaster Recovery Assistance Files System of Records Notice;[14]
  - Acting Administrator Gaynor's All Hands Memorandum "Data Sharing Directive and Implementation Plan"; and
  - FEMA Directive #262-1: Data Sharing, July 16, 2019.
- Developed and distributed an initial questionnaire (April 2019);
- Reviewed initial FEMA responses, requested records, audit logs, policies and procedures, training manuals, and other supporting documentation (May 2019);
- Met with subject matter experts from FEMA's Privacy Branch, Recovery Office, Office of Response and Recovery – IA Division, and the OCC (May-June 2019);
- Met with FEMA to receive a basic overview of the sequence of delivery within the FEMA Recovery Office (May 2019);
- Conferenced with FEMA Region 6 – Texas Recovery Office (July 2019);
- Drafted an initial PCR Report for FEMA comments (September 2019);
- Responded to FEMA comments (October 2019); and
- Drafted and published this final PCR Report (October 2019).

[13] *See* DHS/FEMA/PIA-049 Individual Assistance Program PIA, *available at* www.dhs.gov/privacy.
[14] DHS/FEMA-008 Disaster Recovery Assistance Files, 78 FR 25282 (April 30, 2013).

III. Findings

Summary
The DHS Privacy Office provides the following recommendations to improve FEMA's implementation of information sharing and safeguarding activities that adequately protect individuals' privacy:

> *Recommendation 1:* FEMA OCC should standardize information sharing agreement templates. FEMA OCC should develop information sharing agreements for on-going information sharing partners.
>
> *Recommendation 2:* FEMA should ensure it adequately involves the FEMA Privacy Branch nationwide and, in all information sharing activities to implement DHS Privacy and Information Sharing Policy.
>
> *Recommendation 3:* FEMA leadership should reorganize the FEMA Privacy Branch's reporting structure to comply with *Privacy Policy Instruction 047-01-005 for Component Privacy Officers*.[15]
>
> *Recommendation 4:* The FEMA Privacy Branch should overhaul the delivery and oversight of mandatory privacy training in accordance with *DHS Instruction 047-01-005 for Component Privacy Officers*.
>
> *Recommendation 5:* The FEMA Privacy Branch should update privacy compliance documents to comport with Office of Management and Budget (OMB) Memorandum M-17-12.[16]
>
> *Recommendation 6:* The FEMA Privacy Branch should develop a Continuity of Operations Plan to ensure privacy operations continue during emergencies.

Below is a discussion of how the DHS Privacy Office reviewed the program for compliance, our findings, and when necessary, specific recommendations to FEMA in response to these findings.

---

[15] *See* DHS Instruction 047-01-005 for Component Privacy Officers (February 2017), *available at* https://www.dhs.gov/sites/default/files/publications/dhs%20policy%20instruction%20047-01-005%20Component%20Privacy%20Officer%20Privacy.pdf.
[16] *See* OMB Memorandum M-17-12 Preparing for and Responding to a Breach of Personally Identifiable Information, *available at* https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf.

A. Process and Oversight

Finding: FEMA lacks a standard administrative process for determining which type of information sharing agreement to use to address privacy protections in information-sharing programs.

FEMA documents the sharing of PII and SPII with external entities by using a variety of different types of agreements. At the time of publication of this PCR, FEMA uses the following tools to document external information sharing:

- Information Sharing and Access Agreements (ISAA),[17]
- Routine Use Letters,
- Written Consent,[18]
- Computer Matching Agreements (CMA),[19]
- FEMA-State Agreements (FSA),[20]
- Subpoena Response Letters,[21]
- Intergovernmental Service Agreements (IGSA),[22]
- Interconnection Security Agreements (ISA),[23]
- Service Level Agreements (SLA),[24] and

[17] DHS May 2017 Lexicon defines ISAA as an "agreement that is used to facilitate the exchange of information between the Department (or any element or entity within the Department) and one or more outside parties."
[18] Written consent forms are used by FEMA when the individual whose PII is being disclosed by FEMA completes a documented consent form for a one time sharing. There is no formal guidance for Written Consent forms. Written Consent forms do not fully conform to the Fair Information Practice Principles and lack a discussion of retention, auditing, and access controls. The DHS Privacy Office was told that these agreements, once signed by the Volunteer Agency Liaison (VAL), are stored at the Joint Field Office (JFO) within a locked cabinet.
[19] Pursuant to 5 U.S.C. § 552a(o) of the Privacy Act of 1974, as amended by the Computer Matching and Privacy Protection Act of 1988, any record contained in a system of records may only be disclosed to a recipient agency or non-federal agency for use in a computer matching program pursuant to a Computer Matching Agreement between the source agency and the recipient agency or non-federal agency. The Department requires Computer Matching Agreements to be developed and approved for any matching program as defined by the statute.
[20] A FEMA-State Agreement is a formal legal document stating the understandings, commitments, and binding conditions for assistance applicable as the result of a major disaster or emergency declared by the President. *FEMA Recovery Policy 9420.1 Secure Data Sharing* states that FEMA-State Agreements are between FEMA and a state, tribe, territory, or commonwealth that provide the understandings, commitments, and conditions under which FEMA disaster assistance shall be provided.
[21] Subpoena Response Letters are a special form of Routine Use Letters invoked by a court order (e.g., subpoena). A Subpoena Response Letter is used when an individual seeks records with a subpoena, court order, or other court demand and the matter is subject to third-party litigation.
[22] FEMA uses Intergovernmental Service Agreements to establish an agreement between FEMA and the State for the provision of direct housing assistance, under section 408 of the Stafford Act. There is no formal, departmental guidance for IGSAs.
[23] FEMA uses Interconnection Security Agreements to document security protections on interconnected systems to ensure only acceptable transactions are permitted.
[24] FEMA Directive #262-1: Data Sharing defines SLA as a contract or MOA between a services customer and services supplier that specifies, usually in measurable terms, what services the service provider will furnish.

- Memorandum of Understanding/Agreement (MOU/A).[25]

The most common tools used at FEMA Regional Offices to provide external entities FEMA data are the ISAA and the Routine Use Letter.

DHS Directive 047-01, and *DHS Instruction 047-01-001*, define an ISAA as an agreement that defines the terms and conditions of information/data exchanges between two or more parties. The term ISAA encompasses agreements in any form including MOU, MOA, Letters of Intent, etc.[26]

The ISAA documents the terms and conditions of the information sharing or exchange to include privacy protections and limitations on further disclosure of the information. ISAAs at FEMA are signed by the Federal Coordinating Officer (FCO) or Regional Administrator (RA) (or designee) and the Sharing Partner Executive. FEMA currently uses one ISAA template for sharing with a Federal entity and another ISAA template for sharing with a non-Federal entity.

The threshold for use of a FEMA ISAA template is not documented. FEMA Office of Response and Recovery is participating in an intra-agency initiative to establish an agency-wide business process and developing a FEMA Reference Guide for Sharing PII/SPII that suggests an ISAA template is used when the requestor includes multiple entities and there is sharing over 100 records or when repeat sharing is intended.

Departmental practice established that an ISAA should document the mission-based objectives it will accomplish. Clearly defining the ISAA objectives is critical in scoping each information sharing initiative. In addition, ensuring the initiative clearly expresses the intended objectives in the ISAA will enable greater accountability and easier evaluation of the initiative's success. The current FEMA ISAA template drafted by OCC is not standardized, has incomplete terms, lacks provision for federal privacy protections under the Privacy Act and DHS Privacy Policy requirements, and often does not consider the information sharing partner's responsibilities. The Federal Insurance and Mitigation Administration (FIMA) uses a completely different template.

The FEMA Privacy Branch defines Routine Use Letters as written statements outlining the terms and conditions for data sharing under a Routine Use of the Privacy Act. Routine Uses are defined in System of Records Notices.[27] The FEMA Reference Guide for IA Data Sharing Process Flow

---

[25] FEMA Directive #262-1: Data Sharing defines MOU as a document that describes the general area of understanding between parties, explaining the concepts of mutual understanding, goals, and plans shared by the parties.

[26] DHS Information Sharing Environment Instruction 262-05-001 defines ISAA as any memorandum of understanding, memorandum of agreement, letter of intent, or any other form of agreement that is used to facilitate the repeated, continuing, or enduring exchange of or access to information, including for limited periods of time (e.g., as part of a pilot initiative) between the Department (or any element or entity within the Department) and one or more outside parties (including domestic or foreign entities in the private or public sector and government agencies at the Federal, State, or local level).

[27] 5 U.S.C. § 552a(a)(7) defines "routine use" as, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.

further defines Routine Use Letters as a unique tool for FEMA information sharing. FEMA uses Routine Use Letters when there is a single entity requestor who has requested fewer than 1,000 records shared for a one-time use. A Routine Use Letter is signed by the FCO or RA (or designee) and the Sharing Partner Executive.

FEMA lacks a clear policy or guidance to distinguish when the most appropriate vehicle to use is an ISAA or a Routine Use Letter. The FEMA Privacy Branch and OCC Information Law Branch (ILB) currently provide ad hoc guidance upon request. Conversely, a Region 6 Texas Recovery Office (TRO) Regional Counsel created a useful information sharing standard operating procedure (SOP) to establish a consistent standard in Region 6 for reviewing and processing requests for information retained by FEMA Region 6 in a System of Records. The Region 6 Texas Recovery SOP, as well as other ad-hoc documents that have not been formalized, suggest that if FEMA will be engaging in repeated bulk data transfers,[28] then FEMA should execute an ISAA. If FEMA will be engaging in one-time sharing of PII, then a Routine Use Letter should be used according to the SOP. The DHS Privacy Office recommends that FEMA develop an agency-wide SOP to better document and standardize the information sharing FEMA undertakes.

As part of the FEMA Data Sharing Directive and Implementation Plan, FEMA has begun to put together a business process to include how to document information sharing and when to use which information sharing vehicle. This process, at a minimum, should implement existing departmental information sharing and privacy policy, while addressing FEMA's unique information sharing needs. Regardless of which information sharing vehicle is chosen, until a repeatable process is formalized in policy there will continue to be privacy risks in all FEMA information sharing activities. To FEMA's credit, the Data Sharing Directive Implementation Timeline states that FEMA will propose external data sharing agreement templates and associated business processes to the FEMA Data Governance Council (DGC)[29] between July and September 2019. FEMA, with Mission Support as the lead, will produce a plan for developing the repository of formal data sharing agreements and publish formal data sharing agreement templates and associated business processes between October and December 2019.[30]

---

[28] DHS Instruction IA 1000 Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines (January 2017), *available at* https://www.dhs.gov/sites/default/files/publications/office-of-intelligence-and-analysis-intelligence-oversight-program-and-guidelines.pdf, defines "Bulk Data Transfer" as transfer of large quantities of data that, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.). FEMA has no standard definition for bulk data, which introduces a further challenge for providing consistent guidance on information sharing requirements.

[29] FEMA's DGC, led by the Office of Program and Policy Analysis (OPPA), plays a role in overseeing the sharing of PII with partners. Currently, the FEMA DGC is drafting an official charter for the council. The purpose of the DGC is to strengthen FEMA's management of data to support effective and efficient mission delivery, advance integrated analytics capabilities, and facilitate data-driven decision making. The DGC facilitates the collaborative efforts across FEMA to develop, adjudicate, and deliver guidance, policies, and standards related to data management, to include data sharing policies and instructions. FEMA's DGC provides the FEMA Privacy Branch a forum for outreach, collaboration, and coordination that can continue to address privacy shortcomings and implement external information sharing best practices.

[30] As of October 2019, OPPA has taken the lead on developing a repository for formal data sharing agreements, due to the nature of its responsibilities to mature data management. The DHS Privacy Office recommends OPPA, Mission Support, and other stakeholder offices within FEMA collaborate on the repository moving forward.

Recommendation 1: FEMA OCC should standardize information sharing agreement templates. FEMA OCC should develop information sharing agreements for on-going information sharing partners.

Finding: FEMA does not have a standard agency approach or process for clearing, auditing, and ensuring compliance with terms set forth in ISAAs. This lack of a standard process has led to poor oversight of suspected and confirmed privacy incidents.

In response to PCR inquiries, the DHS Privacy Office found that FEMA does not have a process to ensure third parties adhere to ISAA terms and does not conduct compliance audits. At the front end, FEMA ISAAs set the parameters for use and state whether further sharing of the information with trusted partners is allowed or prohibited, yet there is no subsequent follow up or reporting requirements to confirm these parameters are followed. While FEMA states it includes language requiring partners to employ appropriate safeguards to ensure data is protected and to report any loss or compromise of the information FEMA shared with it, recent incidents demonstrate that these are not always put into practice. At the back end, FEMA does not follow up once the ISAA is signed to ensure compliance with its terms and does not conduct audits of ISAAs, as it does not have a formalized audit process nor adequate resources for these purposes.

Due to the absence of a disciplined process, many ISAAs are handled at the local level (e.g., at the Joint Field Office (JFO) or Regional Office) and drafted by the local OCC. At that point, the FCO at the JFO or RA at the Regional Office may sign off on the ISAA, with inconsistent FEMA Privacy Branch oversight. Other times, the data sharing request will go to the FEMA Headquarters Recovery Analytics Division (RAD), which will initiate the ISAA drafting process in coordination with HQ OCC. At that time, the FEMA Privacy Branch may, but not always have an opportunity to review. However, the final signatories are more often the FCO and RA.

There is currently no central repository in FEMA for approved ISAAs and no process exists for circulating cleared ISAAs internally or externally. The FEMA Data Sharing Directive assigns responsibility to the Office of Policy and Program Analysis (OPPA) to gather requirements for and coordinate the establishment of a centralized repository for all approved FEMA data sharing agreements and associated review requirements. This centralized repository and OPPA's oversight promote transparency, the potential to leverage agreements across the Agency, and the ability for other FEMA information sharing needs to be fulfilled under existing, appropriately approved, agreements. The DHS Privacy Office found that the document and agreement management issues contributed to the unauthorized sharing of PII with the non-governmental partner, which compromised the PII of disaster survivors in a privacy incident that was eventually remedied.[31]

[31] While this incident was remedied (through individual notification, credit monitoring, and call center services for the impacted individuals), and the incident has since been closed, the DHS Privacy Office Director of Incidents concluded that a formalized process that defines operations for storing and circulating the Information Sharing and Access Agreements would have simplified the investigation into this major incident.

The DHS Privacy Office notes that this issue is actively being pursued by the ORR in coordination with the FEMA Privacy Branch, as part of the FEMA Data Sharing Directive and Implementation Plan. The FEMA Data Sharing Directive sets the expectations that FEMA will be transparent with data to support the agency's mission, while articulating the steps required to protect and secure data. The FEMA Data Sharing Directive requires all FEMA Program Offices to document all data sharing agreements with external partners and describe the sharing purpose; the nature of the data; the frequency of exchange; requirements for how the data should be protected, transferred, stored, and used; as well as stipulations for allocating and managing risk.

Finding: The FEMA Privacy Branch lacks adequate oversight of, or participation in, the development and implementation of FEMA's Information Sharing and Access Agreements, resulting in gaps in privacy protections and safeguards.

At the time of this PCR, the FEMA Privacy Branch is not sufficiently involved in the development, review, or monitoring of FEMA ISAAs. Based on privacy compliance documents reviewed by the DHS Privacy Office, the FEMA Privacy Branch's awareness or privacy oversight of ISAAs appears limited to cross checking existing System of Records Notices (SORN) that may allow for a routine use to share the information, but not assessing the privacy impact of the sharing nor ensuring the ISAA appropriately provides provisions for the protections of the information being shared. While having the legal authority to share information is required, that is simply the baseline of compliance. Proactively applying appropriate governance mechanisms in the development of ISAAs, ensuring all agreements have been reviewed by the FEMA Privacy Branch and include all necessary privacy and information safeguarding standards, and completing all required privacy compliance documents, better aligns with departmental policy on information sharing and safeguarding requirements. Sufficient ISAA governance ensures that when personally identifiable information is shared, privacy safeguards follow the information to agencies it is being distributed to, and any further dissemination that may occur.

Recently, the FEMA Data Sharing Directive assigns the Information Management Division (IMD) responsibility for ensuring FEMA Program Offices compliance with appropriate privacy requirements, consistent with DHS Privacy Policy for information sharing agreements. The Directive also requires that external sharing activities follow DHS privacy policy and standards as appropriate. IMD should fully implement and promote the FEMA Data Sharing Directive.

DHS Directive No. 262-05: Information Sharing and Safeguarding,[32] outlines the responsibilities of the DHS Chief Privacy Officer to ensure that departmental information sharing and safeguarding activities comply with applicable laws and provide adequate protections for individuals' privacy. As the DHS Privacy Office's main point of contact at FEMA, the FEMA Privacy Officer should be an active participant in the discussion, construction, and implementation of all FEMA ISAAs that involve PII. As outlined in the DHS Information

[32] *See* DHS Information Sharing and Safeguarding Directive: 262-05 (September 2014).

Sharing and Safeguarding Strategy,[33] Components should support and sustain the capacity and capability to share and safeguard mission-essential information in support of the DHS mission. As the primary steward of information privacy protection for FEMA, this responsibility falls largely on the FEMA Privacy Branch.

In addition, as directed in *DHS Instruction 047-01-005 for Component Privacy Officers*, each Component Privacy Officer is to provide privacy oversight of information, including PII, as well as communicate privacy initiatives on Component programs with internal and external stakeholders in coordination with the DHS Privacy Office. To implement DHS Directive No. 262-05, FEMA should also ensure that the DHS Privacy Office reviews and approves all ISAAs templates, as appropriate, to determine if they comply with applicable privacy law and adequately protect individuals' privacy.

FEMA Instruction 109-2-1 FEMA Privacy Program[34] implements Privacy Policy Instruction 047-01-005 at FEMA and assigns responsibility to the Privacy Branch to review FEMA ISAAs for privacy issues. However, in practice, the FEMA Privacy Branch is not formally included in the ISAA review process. *FEMA Instruction 109-2-1 FEMA Privacy Program* requires that FEMA has a Routine Use in an applicable SORN or identifies an exception under 5 U.S.C. § 552a(b) that authorizes information sharing with external entities. FEMA is currently working on an Office of Response and Recovery Data Sharing Process Flow (Routine Use and ISAA) that may better operationalize the FEMA Privacy Branch's role. However, the DHS Privacy Office remains concerned that the "Process Flow" is done in a silo within the Office of Response and Recovery, and there is a lack of consistency in the process across different offices within FEMA In the May 24, 2019 draft version shared with the DHS Privacy Office, the "Process Flow" aligns with FEMA Instruction 109-2-1 in that FEMA OCC must coordinate with the FEMA Privacy Branch to conduct legal and privacy policy review. The FEMA Privacy Branch can then provide its concurrence, non-concurrence, or edits back to the FEMA Program point of contact.

FEMA's Individual Assistance (IA) Program PIA[35] broadly covers the collection, use, maintenance, retrieval, and dissemination of PII of applicants for implementing the FEMA IA programs. The PIA states that FEMA memorializes external information sharing through a number of documents, including CMAs, ISAAs, FEMA-State Agreements, and Routine Use letters. FEMA provides the receiving entity with the security requirements to ensure that the data is protected from third-party disclosure, and that survivor PII is protected according to industry-

---

[33] *See* DHS Information Sharing and Safeguarding Strategy (January 2013), *available at:* https://www.dhs.gov/sites/default/files/publications/12-4466-dhs-information-sharing-and-safeguarding-strategy-01-30-13--fina%20%20%20_0.pdf.

[34] FEMA Instruction 109-2-1 FEMA Privacy Program provides guidelines and procedures to establish, manage, and operate the Agency's privacy program. It expands on the concepts, definitions, and governance outlined in FEMA Directive 109-2 FEMA Privacy Program. The Instruction incorporates by reference all DHS Directives, Instructions, Privacy Policy Guidance Memoranda/Privacy Policy Directives, and other guidance documents issued by the DHS Chief Privacy Officer in their entirety. To the extent conflict exists between DHS and Agency policy documents, the Departmental policy or policies are controlling.

[35] *See* DHS/FEMA/PIA-049 Individual Assistance (IA) Program*, available at* www.dhs.gov/privacy.

standard security practices. CMAs are reviewed by FEMA's OCC, FEMA's Information Management Division (including the Privacy Branch), the Deputy Administrator of FEMA, and the DHS Data Integrity Board.[36] All other contractually-based information sharing endeavors outside of FEMA are reviewed by FEMA's OCC (by each party to the agreement), the Office of the Chief Information Officer, and the FEMA Privacy Branch for consistency with the Disaster Recovery Assistance Files SORN.[37]

However, FEMA's Privacy Branch does not review all ISAAs, nor does FEMA's Privacy Branch complete privacy threshold analysis' (PTA) or PIAs for ISAAs. A sample review of FEMA PTAs held by the DHS Privacy Office confirmed several instances in which systems operated by FEMA share information, including PII, outside of the Department. The FEMA Privacy Branch states that agreements on an ad-hoc basis also warrant their review, but most are not reflected in PTAs. As PTAs are designed to determine whether a Department program or system has privacy implications and warrants additional privacy compliance documentation, the lack of PTA coverage for ad hoc arrangements puts the Agency at risk.

Based on historical interactions with the DHS Privacy Office, the FEMA Privacy Branch demonstrates a lack of proactive management and oversight of the generation, review, and submission of privacy compliance documentation for ISAAs that is required through DHS privacy policy. The Department uses PTAs and PIAs as the mechanisms to assess privacy risks in Departmental information sharing activities. This absence of privacy compliance documentation points to FEMA Privacy Branch's inability to forge a privacy-focused culture within the organization that ensures the consideration of privacy risks during development of information sharing initiatives. During this PCR, the FEMA Privacy Branch made assurances it would draft PTAs or PIAs to discuss the privacy risks of and mitigations to FEMA's information sharing practices.

Finding: FEMA does not adhere to Departmental policies/instructions/requirements around information sharing.

FEMA Privacy Branch developed a Privacy Policy and Compliance Directive that provides direction on the collection, use, maintenance, disclosure, deletion, and destruction of PII. Upon review, however, it is almost verbatim to *DHS Instruction 047-01-001*, without addressing FEMA-specific issues, nor placing any additional substantive requirements on FEMA personnel.

Per *DHS Directive 047-01 Privacy Policy and Compliance*, Component Heads are responsible for implementing DHS privacy policy and procedures as established by the DHS Chief Privacy Officer. Under *DHS Directive 047-01 Privacy Policy and Compliance,* Component Privacy Officers are responsible for overseeing the implementation of DHS privacy policies, including all guidance documents and memoranda, at the Component level. If the FEMA Privacy Branch

[36] CMAs are subject to a robust oversight process dictated by the Privacy Act of 1974, as amended. For more information about the DHS Data Integrity Board, *see* https://www.dhs.gov/sites/default/files/publications/computer-match-directive-262-01_0.pdf.
[37] DHS/FEMA-008 Disaster Recovery Assistance Files, 78 FR 25282 (April 30, 2013).

determines that Instruction 047-01-001 is specific enough to meet the needs of the Component, particularly as it relates to ISAAs, then efforts should be focused on implementing said policy, and raising awareness and compliance among FEMA personnel. If, however, the FEMA Privacy Branch found any gaps after analyzing existing DHS policies, steps should be taken to fill those gaps by creating and promoting customized policies.

Rather than generating duplicative policies and instructions, FEMA should focus its efforts on understanding and implementing standing DHS privacy policies, directives, and instructions. This will ensure that all FEMA personnel, programs, and systems are handling personally identifiable information in a manner consistent with departmental standards. If FEMA does not believe that current Department-wide policies are adequately addressing its needs, a thorough and thoughtful analysis could be conducted to identify gaps or issues, as well as ways in which they might be addressed through the development of more specific component level policy.

To assist FEMA in complying with *DHS Directive No. 262-05: Information Sharing and Safeguarding,*[38] the DHS Privacy Office provided FEMA comments and edits on draft ISAA templates, to ensure that templates included all necessary privacy and information sharing safeguards. However, the recommendations were not incorporated into the ISAAs templates and no explanation was provided for their exclusion. The template recommendations provided were derived from Departmental information sharing policy and guidance that is based on the Fair Information Practice Principles (FIPPs). The FIPPs are a set of eight principles that are rooted in the tenets of the Privacy Act of 1974. The Chief Privacy Officer's authority to use these principles as the framework for privacy policy at DHS is based upon Sections 222 (a)(1) and (a)(2) of the Homeland Security Act of 2002, as amended, which authorize the Chief Privacy Officer to assume primary responsibility for DHS privacy policy, including (1) assuring that the use of technologies sustains and does not erode, privacy protections relating to the use, collection, and disclosure of personal information; and (2) assuring that personal information contained in DHS Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act. FEMA has not been consistent in the application of the FIPPs through its information sharing process.

The FIPPs form the basis of the Department's privacy compliance policies and procedures governing the use of PII. These principles are: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing. The FIPPs provide the foundation of all privacy policy development and implementation at the Department and must be considered whenever a DHS program or activity raises privacy concerns or involves the collection of personally identifiable information from individuals, regardless of their status.

The type of information sharing agreement called the Written Consent Form inherently involves the participation of individuals, and by default their consent for the collection and use of the PII

[38] The DHS Information Sharing and Safeguarding Directive 262-05; establishes the policy and governance framework for information sharing and safeguarding both within the Department and between the Department and its federal, state, local, tribal, territorial, private sector, and international partners.

that they provide. FEMA receives and shares registration and assistance records, as well as Temporary Housing Assistance Eligibility Determinations via Written Consent forms. While the Written Consent Form acknowledges participation from the survivor, these forms lack a discussion of retention, auditing, and access controls.

As required under the Privacy Act of 1974,[39] the Department must maintain accurate records. Failing to do so, as noted in *DHS Privacy Policy Guidance Memorandum 2017-01*,[40] could undermine efficient decision making and create the risk of errors. A privacy risk of the Individual Assistance program is that inaccurate information could be maintained about disaster assistance applicants, particularly when the data is collected from other federal agencies if the applicant applies with the U.S. Department of Housing and Urban Development (HUD) or U.S. Small Business Administration (SBA) first. FEMA mitigates this privacy risk by verifying any applicant data received from other federal agencies against the applicant's Social Security number (SSN), and if inaccuracies are found in the received data, FEMA supplies the correct data from the applicant's FEMA file, which will automatically update HUD and SBA's files via the CMAs.

FEMA employs a number of effective safeguards in order to protect the information collected under the Individual Assistance program from inappropriate access or use by terms within the ISAAs. Information collected via the Individual Assistance program is maintained within the Disaster Assistance Improvement Program (DAIP), National Emergency Management Information System-Individual Assistance (NEMIS-IA), Virginia Systems Repository (VSR), and Disaster Management and Support Environment (DMSE) Cloud Environment (CE).[41] These systems comply with all aspects of the FISMA,[42] and each have a current Authority to Operate (ATO).[43] These systems employ all applicable rules and policies, including all DHS automated systems security requirements to safeguard information. Access to information within the system is limited to those individuals who have an operational need to know, as well as a verified official duty and appropriate background level.

The FEMA ISAA template contains language that requires partners who receive information from FEMA apply the appropriate technical, physical, and administrative safeguards to secure any and all FEMA survivor/registrant PII shared under the provisions of the ISAA. The FEMA ISAA templates include language to ensure that each IT system that stores, analyzes, processes, or uses FEMA PII, regardless of configuration or location, has as System Security Plan and undergoes routine cybersecurity scans. The partners are also required to retain such plans and

---

[39] *See* 5 U.S.C. § 552a, *available at* https://www.gpo.gov/fdsys/pkg/USCODE-2010-title5/pdf/USCODE-2010-title5-partI-chap5-subchapII-sec552a.pdf.
[40] *See* DHS Privacy Policy Guidance Memorandum 2017-01 "DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information", at IV. A. vi. (April 27, 2017), *available at* https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01.
[41] *See* DHS/FEMA/PIA-049 Individual Assistance (IA) Program, *available at* www.dhs.gov/privacy.
[42] *See* Public Law 113-283, 128 Stat. 3073 (December 18, 2014), *available at* https://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf.
[43] *See* Security Authorization Process Guide (March 16, 2015), *available at* https://www.dhs.gov/sites/default/files/publications/Security%20Authorization%20Process%20Guide_v11_1.pdf.

records of such scan results, producing them as necessary to comply with audit requests. Lastly, the FEMA templates require that personnel with access to any FEMA survivor/registrant PII provided under the ISAA have completed privacy and security training and understand survivor PII protection responsibilities.

However, FEMA's current ISAA templates lack a discussion on retention, redress, auditing, or reporting. ISAAs should address the retention period for the recipient. Individuals whose information is shared should know how to correct their data if inaccurate or seek redress if a decision is made based on inaccurate data. If FEMA is entering into a long-term agreement, ISAAs usually require regular reporting on implementation of the agreement. If FEMA is entering into a one-time, or short-term arrangement, ISAAs usually require reporting within 90 days of the completion of the sharing. The reports help to ensure accountability for adhering to the standards of the agreement and helps the Department understand when sharing is or is not successful/beneficial. Metrics for the reporting are flexible, as is the format, but reporting is usually required. The FEMA Privacy Branch can implement *DHS Directive No. 262-05: Information Sharing and Safeguarding* and Privacy Policy Directive 140-06 by more fully contributing to the ISAA development and review process.

The DHS Privacy Office believes that FEMA can fully comply with Department information sharing policy just as it successfully complies with the CMA process. FEMA should replicate the CMA process for other external information sharing. The Department requires CMAs be developed and approved for any matching program as defined by the Privacy Act. *DHS Directive 262-01* and *Instruction 262-01-001 Computer Matching Agreements and the Data Integrity Board* effectuates policies for engaging in and approving the use of CMAs, which are reiterated by *FEMA Recovery Policy 9420.1 Secure Data Sharing* and *FEMA Instruction 109-2-1: FEMA Privacy Program*. The FEMA Instruction clarifies that the FEMA Privacy Branch is responsible for reviewing FEMA CMAs for completion and providing comments and edits as appropriate. The FEMA Privacy Branch works with the program office and system owner to address questions and coordinates review within FEMA, including OCC and responsible FEMA program officials, and with the DHS Privacy Office.

> **Recommendation 2:** FEMA should ensure it adequately involves the FEMA Privacy Branch nationwide and, in all information sharing activities to implement DHS Privacy and Information Sharing Policy.

B. Organization/Structure/Authority

Finding: The position of the Privacy Branch's location within the FEMA organizational structure, does not allow for a holistic approach to information sharing that considers privacy policy and legal requirements.

The PCR made clear that the current organizational placement of the FEMA Privacy Branch is insufficient to provide the level of oversight and direction necessary to sufficiently oversee the privacy impact of the organization's information sharing activities.

OMB Circular No. A-130[44] identifies the Senior Agency Official for Privacy (SAOP) as the senior official, designated by the head of an agency, who has overall agency-wide responsibility for information privacy. Under the OMB Memorandum for the Heads of Executive Departments and Agencies, Memorandum M-16-24,[45] the SAOP manages privacy risks associated with any agency activities that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems. As the DHS SAOP, the DHS Chief Privacy Officer formalized DHS privacy policy requiring DHS Components to appoint a Privacy Officer within their Component to oversee privacy compliance, policy, and oversight activities in coordination with the DHS Chief Privacy Officer. Through this directive, the Component Privacy Officer serves as an extension of the DHS Chief Privacy Officer to facilitate the successful accomplishment of OMB Circular No. A-130 requirements at the Component level. To facilitate the effective function of Component Privacy Officers,[46] the Department issued instructions that outline Component Privacy Officer responsibilities, as well as requirements for the collection, use, maintenance, disclosure, deletion, and destruction of PII.[47]

To efficiently and effectively identify, mitigate, and reconcile privacy issues related to FEMA information technology systems and programs, the FEMA Privacy Branch must be strategically positioned in a location within the Component's hierarchy that affords it both the authority required, as well as the ability to coordinate with senior leadership as needed. In May 2007, DHS Secretary Chertoff issued *DHS Memorandum for Designation of Component Level Privacy Officers* requiring the designation of officials to serve as full-time Components Privacy Officers at operational components, to include FEMA. In June 2009, DHS Deputy Secretary Lute issued *DHS Memorandum for the Designation of Component Privacy Officers* directing ten DHS components, including FEMA, to each designate a senior-level federal employee as a full-time Privacy Officer reporting to the Component Head. The DHS Deputy Secretary's memo was formalized in February 2017 via the DHS Instruction 047-01-005, which requires that the Component Privacy Officer report directly to the Component Head, must be a senior level federal employee with significant privacy experience, and be provided the appropriate levels of staff support and resources.

At this time, the FEMA Privacy Branch is not advantageously situated to provide the FEMA Privacy Officer with the level of visibility, access, or influence necessary to fulfill its mission.

---

[44] *See* OMB Circular No. A-130: Managing Information as a Strategic Resource (July 2016), *available at* https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource.

[45] *See* OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy (September 2016), *available at* https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m_16_24_0.pdf.

[46] *See* DHS Privacy Policy Instruction Number: 047-01-005 (February 2017), *available at* https://www.dhs.gov/sites/default/files/publications/dhs%20policy%20instruction%20047-01-005%20Component%20Privacy%20Officer%20Privacy.pdf.

[47] *See* DHS Instruction Privacy Policy Directive: 047-01-007 (December 2017), *available at* https://www.dhs.gov/sites/default/files/publications/dhs%20policy%20directive%20047-01-007%20handbook%20for%20safeguarding%20sensitive%20PII%2012-4-2017.pdf.

The Senior Director for Information Management serves as the FEMA Privacy Officer and is responsible for making privacy policy decisions in consultation with the DHS Chief Privacy Officer and implementing responsibilities defined in DHS Instruction 047-01-005. To address the FEMA Administrator, the FEMA Privacy Officer's current chain of command includes the Office of the Chief Administrative Officer (OCAO) and Mission Support (MS Privacy responsibilities at FEMA are separated across various levels of responsibility. As currently situated, the FEMA Privacy Officer is responsible for day-to-day privacy compliance and oversight. This means that the officer with privacy responsibilities is not on equal footing with the heads of other FEMA offices that he oversees, including the U.S. Fire Administration, Regions I-X, Resilience, and the Office of Response and Recovery, as required by DHS Privacy Policy. The DHS Privacy Office recommends realignment so that the FEMA Privacy Officer can oversee implementation of DHS privacy policies within the Component and report directly to the FEMA Administrator, as required.

As previously noted, DHS Directive 262-05[48] establishes the policy and governance framework for information sharing and safeguarding both within the Department and between the Department and its federal, state, local, tribal, territorial, private sector, and international partners. Under this Directive, the General Counsel and the Chief Privacy Officer (consistent with the Component designees) are required to ensure that departmental information sharing and safeguarding activities comply with applicable law and adequately protect individuals' privacy, respectively. This PCR found that FEMA is not structured to ensure that the FEMA Privacy Officer can inform information sharing activities throughout the Agency and ensure compliance with the Directive.

To address current systemic and programmatic privacy gaps and risks, FEMA leadership should promptly reorganize its reporting structure to comply with the DHS Deputy Secretary's Memo and DHS Instruction 047-01-005, resulting in a direct line of reporting from the Privacy Officer to the FEMA Administrator. To implement resource and financial provisions of DHS Directive 047-01,[49] FEMA should also provide the level of material support necessary to appropriately staff the Privacy Branch in a way that will allow it to properly attend to information sharing assessments and the development of necessary information sharing compliance documentation.

In addition to privacy responsibilities, the Senior Director for Information Management (also the FEMA Privacy Officer) is also responsible for records management, the FEMA disclosure program, and Paperwork Reduction Act compliance. This runs contrary to the DHS Deputy Secretary's Memo and DHS Instruction 047-01-005, which requires the designation of a full-time Privacy Officer with significant privacy experience. The FEMA Privacy Branch stated that there are thirty-seven available positions supporting the FEMA Information Management Division, yet only six are tasked with privacy related responsibilities. Additionally, all current

[48] *See* DHS Information Sharing and Safeguarding Directive: 262-05 (September 2014).
[49] *See* IV.B.5, *available at* https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-directive-047-01_0.pdf.

FEMA privacy employees can be mandatorily deployed in the aftermath of a disaster, leaving even fewer resources specifically to manage privacy responsibilities.

A strong privacy office is an integral part of a modern information-focused organization,[50] especially one with varied operational missions and dispersed management. Every aspect of information sharing is replete with privacy risks (as revealed through recent FEMA privacy incidents), and a strong privacy office can guide FEMA in implementing a structure that ensures adequate resources are in place to fulfill information sharing and safeguarding requirements in FEMA's information sharing activities, even when operational deployments of staff are necessary.

The DHS Privacy Office recognizes FEMA Privacy Branch efforts during this PCR to address issues and make changes that would quickly improve the Agency's privacy posture. The DHS Privacy Office agrees with FEMA Privacy Branch concerns that it may lack sufficient staff and resources to oversee compliance with information sharing and privacy compliance requirements and recognizes this may be a significant issue to implement DHS Instruction No. 047-01-005.

> **Recommendation 3:** FEMA leadership should reorganize the FEMA Privacy Branch's reporting structure to comply with *Privacy Policy Instruction 047-01-005 for Component Privacy Officers*.

C. Training

Finding: The FEMA Privacy Branch does not deliver privacy training to improve organizational awareness for the handling and safeguarding of personally identifiable information; privacy incident handling, reporting, and mitigation practices; and compliance documentation requirements.

The provision of privacy-specific training is key to establishing a fundamental understanding among all employees of the need to protect and safeguard personally identifiable information. It is not only necessary to provide this training upon the onboarding of new employees and contractors, but also as an ongoing effort to account for the changes in policy and legislation that govern the protection of sensitive information and raise awareness on a continuing basis. The FEMA Privacy Branch does not currently effectively track the completion of mandatory privacy training or enforce training requirements.

As outlined in the OMB Circular A-108,[51] all federal agencies are required to establish sufficient training mechanisms to provide their personnel with an understanding of the Privacy Act, OMB guidance, the agency's implementing regulations and policies, and any job-specific requirement

---

[50] *See* OMB Circular A-130: Managing Information as a Strategic Resource (July 2016), Appendix 1, at pp. A-1 – A-2., *available at* https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf.
[51] *See* OMB Circular A-108: Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act (December 2016), *available at* https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A108/omb_circular_a-108.pdf.

related to privacy. Under OMB Circular A-130, each SAOP must assess and address the training and professional development needs of his/her agency with respect to privacy. As such, agencies shall develop, maintain, and implement mandatory agency-wide privacy awareness and training programs that are consistent with applicable OMB, National Institute of Standards and Technology (NIST), and Office of Personnel Management (OPM) policies, standards, and guidelines for all personnel. This training should include foundational information, as well as more advanced, role-based privacy training to information system users, managers, senior executives, and contractors. Per the *DHS Privacy Office Guide to Implementing Privacy*,[52] the DHS Privacy Office developed a training course, *Privacy at DHS: Protecting Personal Information*, which is to be completed annually by all DHS employees and contractors. The course expands on basic privacy concepts to build an understanding among DHS personnel of the Privacy Act and E-Government Act, as well as the proper use and protection of PII. Supplemental training offered by the DHS Privacy Office to Component personnel includes instruction on privacy basics, as well as the drafting and development of privacy compliance documents such as PTAs, PIAs, and SORNs. Advanced, role-based privacy training, however, is best created and delivered by the Component Privacy Office given its awareness of the Component's mission and culture. Additionally, to facilitate auditing and accountability, the FEMA Privacy Branch should track the provision and completion of all privacy-related training to employees and contractors.

Privacy incidents, whether accidental or malicious, can pose specific risks to individuals, because there is an increasing recognition that personal information, such as Social Security numbers, financial account information, health information, and biometric data, is valuable and can be reverse engineered with a potential for great public harm. Therefore, it is crucial that DHS personnel be able to identify and report a suspected or confirmed privacy incident.[53] This is a difficult task if employees do not receive training and guidance on properly handling PII and identifying privacy incidents.

This PCR found that the FEMA Privacy Branch provides minimal outreach and training on what constitutes a privacy incident and what should be done when a privacy incident occurs. During this PCR, the DHS Privacy Office Director of Incidents reviewed the types of incidents occurring at FEMA and the degree of assistance provided by the FEMA Privacy Branch to resolve reported incidents. The total number of reported incidents was low during the time frame covered by the PCR but included two major incidents. Without additional insight from the FEMA Privacy Branch, it is difficult to know whether the incident numbers are low due to careful handling of PII or due to a lack of training, understanding, and ability to identify privacy incidents.

The DHS Privacy Office recommends the FEMA Privacy Branch assign a staff member to lead training, awareness, investigations, and remediation activities on future FEMA privacy incidents.

---

[52] *See* DHS Privacy Office Guide to Implementing Privacy (June 2010), *available at* https://www.dhs.gov/xlibrary/assets/privacy/dhsprivacyoffice-guidetoimplementingprivacy.pdf.
[53] *See* DHS Instruction 047-01-008 Privacy Incident Handling Guidance (December 2017), *available at* https://www.dhs.gov/sites/default/files/publications/047-01-008%20PIHG%20FINAL%2012-4-2017_0.pdf.

The FEMA staff lead for incidents should be someone other than the FEMA Privacy Officer given the workload already handled by the FEMA Privacy Officer, as such a designation will fail to produce the attention and response time needed to mitigate incidents. For the FEMA Privacy Branch to become more fully invested in incident management, the FEMA staff lead will need to obtain access to the Enterprise Cyber Operations Portal (ECOP) to have the ability to directly assess reported suspected or confirmed incidents. Additionally, a dedicated incident staff member could provide the requisite outreach and training for FEMA personnel.

As part of effective information sharing management, the FEMA Privacy Branch should also develop and provide privacy training to the VAL to better inform voluntary agencies who request DHS-data on how to appropriately handle DHS-data. Furthermore, individualized training covering how to protect FEMA data should be provided to each Emergency Management Partner, including but not limited to other federal agencies, state and tribal governments, local and voluntary organizations, utility companies, hospitals and health care providers, and private sector businesses that employ disaster survivors. All training should establish a formal process for determining with whom to trust Agency data.

> **Recommendation 4:** The FEMA Privacy Branch should overhaul the delivery and oversight of mandatory privacy training in accordance with *DHS Instruction 047-01-005 for Component Privacy Officers*.

D. Incident and Privacy Compliance

Finding: FEMA does not adhere to Office of Management and Budget (OMB) Memorandum M-17-12.

The DHS Privacy Office assessed FEMA's compliance with OMB guidance to determine if information sharing and safeguarding activities associated with the two major incidents[54] and similar activities adequately protect individuals' privacy. The DHS Chief Privacy Officer, pursuant to Section 222 of the Homeland Security Act and as the Department's SAOP under OMB Memorandum M-17-12,[55] must determine any potential impacts a privacy incident may have on individuals' privacy.

The SAOP has agency-wide responsibility and accountability for the agency's privacy program and is responsible for overseeing, coordinating, and facilitating the agency's privacy compliance

---

[54] DHS defines a privacy incident or breach as: "The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (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."

[55] OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3 2017), *available at* https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf.

efforts, including those related to the Privacy Act of 1974.[56] Further, under OMB Memorandum M-17-12, the SAOP shall ensure that all agency Privacy Act SORNs include routine uses for the disclosure of information necessary to respond to a breach either of the agency's PII or, as appropriate, to assist another agency in its response to a breach.[57]

While OMB Memorandum M-17-12 was issued in 2017, the FEMA Privacy Branch has updated only one FEMA Privacy Act SORN routine uses to comply with OMB Memorandum M-17-12.[58] Updated SORNs with updated incident-related routine uses will help identify what information was potentially compromised, the population of individuals potentially affected, the purpose for which the information had originally been collected, the permitted uses and disclosures of the information, and other information that may be useful when developing the agency's incident response.

> **Recommendation 5:** The FEMA Privacy Branch should update privacy compliance documents to comport with Office of Management and Budget (OMB) Memorandum M-17-12.

Finding: The FEMA Privacy Branch has not made alternate arrangements should an incident require the deployment of the FEMA Privacy Branch staff in response to a catastrophic disaster. The lack of guidance after deployment has led to ineffective privacy compliance with DHS policies and instructions.

The Stafford Act[59] allows the President to authorize FEMA to provide financial assistance to individuals and households in a state where, as a direct result of a major disaster, survivors incur necessary expenses and have serious needs that they are unable to meet through other means.[60] The Act[61] allows the President to form emergency support teams of federal personnel to be deployed in an area affected by a major disaster or emergency. By policy, any FEMA employee can be called to serve on these emergency support teams. The FEMA Privacy Branch has not made alternate arrangements should a major disaster or emergency require the deployment of the FEMA Privacy Branch staff in response to a catastrophic disaster. All employees within the FEMA Privacy Branch are subject to deployment. While the absence of privacy staff is a core

---

[56] OMB Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy* (Sept. 15, 2016), *available at* https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m_16_24_0.pdf.
[57] 5 U.S.C. § 552a(b)(3). The publication of appropriate routine uses is required under the Privacy Act and thus would be necessary in order to disclose information for the purpose of executing an agency's obligations to effectively manage and report a breach under FISMA. Disclosures pursuant to a routine use are permissive, not mandatory. *See* Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28,948 (July 9, 1975), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/implementation_guidelines.pdf.
[58] FEMA Privacy Branch submitted a draft of the DHS/FEMA-008 Disaster Recovery Assistance Files SORN, with the correct routine uses, to the DHS Privacy Office on July 5, 2019, *see* DHS/FEMA-008 Disaster Recovery Assistance Files, 78 FR 25282 (April 30, 2013).
[59] 42 U.S.C. §§ 5121-5207.
[60] 42 U.S.C. § 5174; 44 CFR §§206.110-119.
[61] 42 U.S.C. § 5144.

issue, the absence of procedures to address privacy issues while these staff are deployed is of greater concern.[62]

Indeed, FEMA's FISMA[63] compliance score decreased from 95 percent for PIAs in August 2017, to 89 percent in November 2017 in the aftermath of Hurricane Harvey.[64] The FEMA Privacy Branch should have a Continuity of Operations Plan to ensure all Agency operations continue to incorporate privacy protections, preserve the privacy of individuals, and are compliant with relevant privacy laws and policy frameworks.

During a disaster, the FEMA Privacy Branch is still responsible for the development of policies; ensuring privacy compliance; responding to privacy incidents, inquiries, and investigations; and conducting privacy training and education throughout FEMA. The current lack of guidance has led to ineffective privacy compliance with DHS policies and instructions during disasters.

> **Recommendation 6:** The FEMA Privacy Branch should develop a Continuity of Operations Plan to ensure privacy operations continue during emergencies.

IV. Conclusion

The DHS Privacy Office found that the FEMA Privacy Branch requires additional staff and resources so that it may accomplish the full breadth of its mission efficiently, even during national emergencies. FEMA should develop an effective approach to protecting privacy in its information sharing that incorporates robust oversight, collaboration, outreach, training, compliance, and incident mitigation. A first step would be for FEMA to implement the six recommendations noted in this PCR. To that end, the DHS Privacy Office requests that the FEMA Privacy Branch:

- Monitor the implementation of this PCR's recommendations and update, as needed, relevant FEMA privacy compliance documentation to reflect the findings and/or outcomes of this PCR; and

- Provide a written report on the implementation status with supporting documentation as appropriate of all recommendations within 12 months of this PCR's publication date. For any recommendations that FEMA has not implemented or has chosen not to implement in that timeframe, we request that FEMA explain why the recommendations were not implemented.

---

[62] The FEMA Privacy Officer notes that privacy staff have been declared unavailable for deployments on a continuous basis since November 2017.
[63] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283 (2014), requires each Component to track adherence to the comprehensive framework required under the FISMA, which is designed to protect government information, operations, and assets.
[64] Since August 2018, FEMA's FISMA compliance has continuously maintained at 100 percent for PIAs.

The DHS Privacy Office thanks FEMA for their assistance in conducting this PCR and for being responsive to our inquiries throughout the PCR process. We look forward to working with FEMA in the future to provide any and all support needed to assist in implementing the recommendations of this PCR.

V. Privacy Compliance Review Approval

Responsible Official

Peter T. Gaynor
Acting Administrator
Federal Emergency Management Agency

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

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