Privacy Impact Assessment

for the

FEMA-Administered Disaster Case Management

DHS Reference No. DHS/FEMA/PIA-056

May 23, 2022

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA), Office of Response and Recovery (ORR), Individual Assistance (IA) Division provides FEMA-administered Disaster Case Management pursuant to Section 426 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. § 5189d (Stafford Act). Through FEMA-administered Disaster Case Management (DCM), FEMA supplements existing services provided by state and local organizations following a disaster to adequately meet the disaster-caused unmet needs of survivors. FEMA is publishing this Privacy Impact Assessment (PIA) to cover the collection, use, maintenance, retrieval, and dissemination of personally identifiable information (PII) of individuals who participate in FEMA-administered Disaster Case Management. This Privacy Impact Assessment is intended to consider the privacy risks and applicable mitigation strategies associated with FEMA-administered Disaster Case Management.

Overview

Under the Stafford Act, FEMA, or another federal agency, non-profit organization, or qualified private organization when operating on behalf of FEMA, may provide Disaster Case Management directly to survivors or through financial assistance[1] to state[2] or local government agencies, Indian tribes, or qualified private organizations. Federal award Disaster Case Management programs[3] (e.g., grant, cooperative agreement) are distinct from FEMA-administered Disaster Case Management because the state or tribe is not acting on behalf of or as an agent of FEMA. This Privacy Impact Assessment focuses on FEMA-administered Disaster Case Management.

FEMA primarily administers Disaster Case Management through experienced providers selected based on their availability and capability to perform the work. FEMA evaluates those capabilities against the size and scope of the disaster and subsequent unmet needs. A disaster-caused unmet need is an un-resourced item, support, or assistance that has been assessed and verified as necessary for a survivor to recover from a disaster. This may include food, clothing, shelter, first aid, emotional and spiritual care, household items, home repair, or rebuilding. FEMA

[1] Disaster Case Management federal awards are overseen and approved by FEMA's Individual Assistance (IA) Division, or its delegate, under the Stafford Act. FEMA may provide financial assistance through Disaster Case Management federal awards to allow for the state/tribe to administer and implement its own Disaster Case Management program in the aftermath of a presidential major disaster declaration that includes Individual Assistance and a Disaster Case Management designation (hereafter "IA declaration").
[2] "State" includes the fifty states, the territories, and the District of Columbia.
[3] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, FEDERAL EMERGENCY MANAGEMENT AGENCY, PRIVACY IMPACT ASSESSMENT FOR GRANT MANAGEMENT PROGRAMS, DHS/FEMA/PIA-002, and U.S. DEPARTMENT OF HOMELAND SECURITY, FEDERAL EMERGENCY MANAGEMENT AGENCY, PRIVACY IMPACT ASSESSMENT FOR GRANT MANAGEMENT MODERNIZATION, DHS/FEMA/PIA-013, *available at* https://www.dhs.gov/privacy-documents-fema.

determines who can best execute the mission and support the survivors and selects a provider[4] to implement Disaster Case Management on FEMA's behalf (hereafter "chosen provider"). A chosen provider to implement FEMA-administered Disaster Case Management may be:

- A federal agency that provides case management services, such as the U.S. Department of Health and Human Services, Administration for Children and Families (HHS/ACF), through a mission assignment;[5]
- A national-level voluntary agency experienced in case management, such as the American Red Cross, through an interagency reimbursable work agreement (IRWA);[6]
- A voluntary agency providing personnel experienced in case management through invitational travel[7] (to pay for travel costs); or
- A FEMA contractor experienced in providing Disaster Case Management services working through an existing or new FEMA contract.[8]

FEMA-administered Disaster Case Management supplements existing services typically provided by state and local organizations following a disaster. Without federal support, the state may be inundated and unable to address the size and scope of the needs or unable to sustain the length of time the services are needed. In most instances, this means that FEMA may need to provide services to address the immediate disaster needs while the state develops its Disaster Case Management federal award application and plan for supplementing existing services to address the needs at the most local level. At the conclusion of the FEMA-administered Disaster Case Management, cases may be transferred to a longer-term, non-federal Disaster Case Management program management entity (e.g., a state or voluntary agency active in disasters) to continue to address disaster-caused unmet needs. Some of these entities may be eligible to apply for a FEMA Disaster Case Management federal award (e.g., grant, cooperative agreement).

FEMA-administered Disaster Case Management can be a short-term program that provides limited services to disaster survivors or a longer program with a full spectrum of case management

[4] FEMA may consult a state, tribe, or territory when selecting a chosen provider that is in the best interest of the public.
[5] A mission assignment is a work order issued by FEMA that directs another federal agency to utilize its authorities and resources in support of disaster assistance, pursuant to the Stafford Act. FEMA issues mission assignments as part of a presidentially-declared emergency or major disaster pursuant to its authority under the 42 U.S.C. §§ 5170a, 5192; 44 C.F.R. sec. 206.2(a)(18)).
[6] An interagency reimbursable work agreement is an agreement between federal agencies where the services or supplies provided come from the servicing agency's own resources, and where supplies or services from a third-party contractor are either unnecessary or incidental.
[7] Invitational travel is authorized, official travel for individuals who are either not employed by the federal government or employed intermittently by the government (i.e., consultants or experts) acting in a capacity directly related to official activities of the federal government.
[8] For example, FEMA has an existing Individual Assistance support contract that includes the ability to execute an optional task order to perform Disaster Case Management services.

services that may last for up to 24 months, or longer in demanding circumstances, from the date Individual Assistance is designated on the major disaster declaration. The purpose of FEMA-administered Disaster Case Management is to address immediate to long-term disaster-caused unmet needs, including the development of individual disaster recovery plans and referrals to available resources.

The typical period of performance may range from approximately 90-180 days to address immediate unmet needs

or longer to address prolonged unmet needs. Services for survivors may generally begin as early as 14 days from the date of the Individual Assistance disaster declaration. Once implemented, case managers work one-on-one with survivors to:

- Identify resources for disaster-related unmet needs;
- Assist individuals with developing a personalized disaster recovery plan;
- Advocate for the resources needed and available to address the survivor's unmet needs;
- Schedule recurring meetings with the survivor to check on their recovery status; and
- Discuss next steps to prioritize and address continued unmet needs.

FEMA will provide a subset[9] of Individuals and Housing Program (IHP) registration data, which includes personally identifiable information, collected during Disaster Assistance Registration intake (hereafter called "focused registration data") from survivors who would benefit from case management services to the chosen provider identified by the FEMA Individual Assistance Division. Sharing this information enables the chosen provider to know which resources have been made available to survivors, prepare for the additional resources to assist survivors with their unmet needs, and proactively engage the individual and invite them to complete the necessary intake form in order to facilitate their recovery. Once the chosen provider has received the registration data, case managers take the information and manually input it into their IT system. The chosen provider will review survivor registration information to ensure that there are no duplicate case files or overlap in services. The provider will also confirm that sparse resources and services are distributed among survivors in a timely and equitable manner so that there are no gaps in federal support. The focused registration data is used to perform the following activities, some of which may be performed simultaneously:

[9] The subset includes those identified as likely to benefit from Disaster Case Management , such as those over the age of 65, those with FEMA verified loss, and those who may have an emergency need. Datasets with new groups of registrants may be shared continuously as new applicants are processed and/or new tiers of needs are identified.

- Conduct outreach to affected disaster survivors in Individual Assistance-designated areas and set up appointments for intake assessments and triage;
- Assist survivors in filling out applications for programs that provide financial assistance or services. Case managers will help the survivor to develop a financial assistance case for available federal or non-federal financial assistance programs or services. The cases managers invite survivors to complete the necessary applications for financial assistance;
- Help survivors navigate FEMA's Sequence of Delivery[10] and avoid duplication of benefits;
- Conduct intake assessments of disaster survivors and subsequently triage and tier survivor cases according to the severity of the disaster needs; and
- Ensure that seniors, individuals with disabilities, individuals with access and functional needs, and others who would not effectively be able to recover on their own in a timely manner are supported and have access to resources that address their disaster-caused unmet needs.

Beyond those registered survivors referred by FEMA, the chosen provider's case managers may connect with survivors in disaster recovery centers, shelters, and other community locations where there are individuals who have been impacted by the disaster. Also, a disaster survivor may proactively contact the chosen provider themselves (e.g., via a helpline or in-person) to obtain Disaster Case Management.

The provider's case managers will use survivors' responses to the questions in FEMA Form (FF)-104-FY-21-146, *FEMA-administered Disaster Case Management Intake Form* ("Disaster Case Management Intake Form"), to conduct an intake assessment. The Disaster Case Management Intake Form, included as Appendix A to this Privacy Impact Assessment, will lead to the collection of data elements listed in Section 2.1. Case managers will complete and use responses to the questions in the form, to assess, screen[11] and refer disaster survivors to resources that address their disaster-related needs. The order in which the chosen provider asks the questions may vary depending upon the configuration of its IT system. As the survivor responds to the questions, the case manager manually enters the responses into the provider's case management IT system. Any IT system that the chosen provider uses to implement Disaster Case Management

[10] The Sequence of Delivery establishes the order in which disaster relief agencies and organizations assist disaster survivors. *See* 44 C.F.R. § 206.191. Duplication of benefits is when an applicant receives financial assistance from multiple sources for the same purpose. *See* Section 312 of the Stafford Act, 42 U.S.C. § 5155; *see* also 44 C.F.R. § 206.110 and 206.191. *See* also Individual Assistance Program and Policy Guide 1.1 (IAPPG 1.1) located here: Individual Assistance Program and Policy Guide | FEMA.gov.

[11] "Screen" is the process needed to avoid duplication of services and ensure the survivor is eligible for disaster-related services

on behalf of FEMA must comply with FEMA cybersecurity and privacy requirements for storing personally identifiable information and sensitive personally identifiable information (SPII).

Case managers may visually inspect verification documents (e.g., driver's license) to validate the pre-disaster address of survivors and validate their identity. They only document that verification and validation took place using a checkmark or other indicator. There are two potential outcomes once an individual is found to need services. In the first outcome, a survivor satisfactorily receives a referral to resources to meet their needs, and the case is closed. In the second outcome, a survivor may opt to work with the case manager to create a personalized disaster recovery plan and meet with the case manager, as needed, to prioritize and address their disaster-caused unmet needs and identify next steps. A disaster recovery plan is a goal-oriented plan for recovery that will assist with prioritizing the unmet needs in order of urgency and provide referrals to resources to address those needs. Disaster case managers facilitate survivors' access to the large spectrum of critical resources available to address their specific needs and advise them on how best to streamline and expedite their disaster recovery.

Case managers may refer disaster survivors to groups that provide necessary resources, such as food, clothing, furniture, appliances, transportation, employment, financial assistance, health insurance, medical equipment, legal referral services, senior services, behavioral health services, and child and youth services. The case manager will triage the case to determine how often the case manager and survivor should meet to check on the progress of the disaster recovery plan, the status of their disaster-caused unmet needs, and outline any additional next steps.

When referring disaster survivors to a voluntary recovery group as part of a FEMA-administered Disaster Case Management program, the chosen provider may share applicable information —- that may include personally identifiable information —- with the voluntary recovery group. Before the information is shared the chosen provider will provide the survivor or authorized representative with FF-104-FY-21-147, *FEMA-Administered Disaster Case Management Consent Form* ("Disaster Case Management Consent Form"). Upon receipt of signature and consent, FEMA may share information about the subjects of the disaster case for unmet needs with voluntary organizations (as defined in 44 C.F.R. § 206.2(a)(27)). Once a FEMA-administered Disaster Case Management program has closed, the chosen provider may share open case files with a Disaster Case Management federal award recipient so that the survivors continue to receive Disaster Case Management.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

Under Section 426 of the Robert T. Stafford Disaster Relief and Emergency Assistance

Act, as amended, 42 U.S.C. § 5189d (Stafford Act), FEMA is authorized to "provide case management services, including financial assistance, to state or local government agencies or qualified private organizations to provide such services to victims of major disasters to identify and address unmet needs."

Pursuant to Executive Order 12148, as amended by Executive Orders 12673 and 13286, the President of the United States has delegated the authority to provide case management services to DHS.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The DHS/FEMA-016 FEMA-administered Disaster Case Management Files System of Records Notice (SORN)[12] applies to the information FEMA collects and shares to manage the FEMA-administered Disaster Case Management Program.

The DHS/FEMA-008 Disaster Recovery Assistance Files System of Records Notice (SORN)[13] applies to the information FEMA collects from and during Disaster Assistance Registration Intake.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

FEMA uses the Individual Assistance system[14] to collect and store Individuals and Household Program registration data. The FEMA Chief Information Officer granted the system Authority to Operate (ATO) on February 16, 2021.

There is currently no FEMA IT system storing Disaster Case Management intake information. Instead, chosen providers will utilize their own IT systems to collect and store Disaster Case Management intake information. FEMA will ensure that the chosen provider's system is in alignment with Homeland Security Acquisition Regulation (HSAR) Class Deviation 15-01, Safeguarding of Sensitive Information,[15] and/or security plan requirements in connection with the Authority to Operate and risk assessment. FEMA will publish an appendix (Appendix B) to this Privacy Impact Assessment lists the case management systems approved by the agency

[12] *See* DHS/FEMA-016 Disaster Case Management (DCM) Files System of Records, 87 FR 1171 (January 10, 2022), *available at* https://www.dhs.gov/system-records-notices-sorns.
[13] *See* DHS/FEMA-008 Disaster Recovery Assistance Files, 87 FR 7852 (February 10, 2022), *available at* https://www.dhs.gov/system-records-notices-sorns.
[14] See U.S. DEPARTMENT OF HOMELAND SECURITY, FEDERAL EMERGENCY MANAGEMENT AGENCY, PRIVACY ACT ASSESSMENT FOR THE INDIVIDUAL ASSISTANCE (IA) PROGRAM, DHS/FEMA/PIA-049, *available at* https://www.dhs.gov/privacy-documents-fema.
[15] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, HOMELAND SECURITY ACQUISITION REGULATION (HSAR) CLASS DEVIATION 15-01, SAFEGUARDING OF SENSITIVE INFORMATION (March 10, 2015), *available at* https://www.dhs.gov/publication/current-hsar-deviations

prior to implementation of FEMA-administered Disaster Case Management.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

In accordance with National Archives and Records Administration (NARA) Authority N1-311-86-1, Item 4C10a, records pertaining to disaster assistance will be placed in inactive storage when they are two years old and will be destroyed when they are six years and three months old.

In accordance with NARA Authority N1-311-86-1, Item 4C6a, Disaster Case Management files covering the administrative management, program, and information functions (such as mission assignments and correspondence with state and local officials) will be consolidated at appropriate regional offices upon close of the disaster field office (DFO). These files will be retired to off-site storage one year after closeout and destroyed three years after closeout.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The Disaster Case Management Intake Form (FF-104-FY-21-146) and Disaster Case Management Consent Form (FF-104-FY-21-147) were submitted to Office of Management and Budget (OMB) under OMB Control No. 1660-NW132.[16] Disaster Assistance Registration Intake information has coverage under OMB Control No. 1660-0002.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

FEMA-administered Disaster Case Management assesses disaster-caused unmet needs, such as food, clothing, shelter, first aid, emotional and spiritual care, household items, home repair, or rebuilding. To assess these unmet needs, a wide variety of information is required. Below is a snapshot of the type of information collected:

The following information is collected about the case manager:

- Full name;
- Work phone number; and

[16] Temporary OMB control numbers are assigned to new collections. OMB will assign the official OMB number once approved.

- Work location.

The following types of information will be collected from survivors[17] at the time of intake:

- Client information (name, age, gender, language, phone numbers, email addresses, FEMA registration number, Disaster Case Management identifier);
- Co-client information (relationship to applicant, reside with applicant, name, age, gender, language, phone, email, FEMA registration number, Disaster Case Management identifier);
- Household occupant information (household size, names, relationships to client, dependent status, age, gender);
- Current address (address, apartment number, type of dwelling, household size, location status, alternative living situation); and
- Damaged dwelling address (address, apartment number, type of dwelling, household size, location status, alternative living situation).

The following types of information will be collected to assess unmet needs, which may include development of individual disaster recovery plans and referrals to available resources:

- Self-reported disability or access and functional need, such as Personal Assistance Services /At-risk;
- Self-reported symptoms and feelings of distress;
- Unmet needs (self-identified);
- Behavioral health advocacy assessment;
- Childcare/Youth;[18]
- FEMA/Small Business Administration (SBA) loan;
- Clothing assessment;
- Employment assessment;
- Financial assessment;
- Food assessment;
- Furniture and appliances assessment;

[17] Survivors are termed "clients" upon completion of intake.
[18] "Youth" is generally meant to be someone too young to be left alone where families require childcare.

- Health insurance and access to health care;
- Housing assessment;
- Transportation assessment;
- Senior services assessment;
- Legal services assessment;
- Assistance animals and household pets; and
- Funeral assistance.

In addition, FEMA shares the following focused registration dataset collected from survivors during Individuals and Housing Program registration intake with Disaster Case Management chosen providers:

- Registrant Name and FEMA Registration Number;
- Disaster Number;
- Damaged County;
- Registrant Damaged Dwelling (DD) Address;
- Registrant Damaged Dwelling City of Residence;
- Registrant Damaged Dwelling Zip Code;
- Registrant Current Mailing Address (CMA) Street;
- Registrant Current Mailing Address City;
- Registrant Current Mailing Address Zip Code;
- Registrant Primary Phone Number;
- Registrant Alternate Phone Number;
- Real Property FEMA Verified Loss;
- Personal Property FEMA Verified Loss;
- Total FEMA Verified Loss;
- Self-Reported Income;
- Homeowners Insurance/Renters Insurance – Y/N;
- Flood Insurance – Y/N;

- Non-Compliant (NCOMP) with the National Flood Insurance Requirement Act of 1968, 42 U.S.C. § 4001, *et seq.;*
- Small Business Administration Status;
- Approved Housing Assistance (HA) Amount;
- Approved Other Needs Assessment (ONA) Amount;
- Approved Individuals and Households Program Amount;
- Household (HH) Size;
- Household Member Age 7 and under;
- Household Member Age 65 and older;
- Household Ages;
- Emergency Need;[19]
- Access and Functional Need;
- Personal Assistance Services[20] Y/N (e.g., for self-reported disability or access and functional need);
- Direct Housing Assistance Eligible Y/N;
- Direct Housing Assistance Received Y/N;
- Residence Type; and
- Current Location.

2.2 What are the sources of the information and how is the information collected for the project?

FEMA or its chosen provider collects both focused registration data and Disaster Case Management intake information directly from survivors on behalf of themselves or their households through interviews, either in-person or over the phone. The case manager typically inputs the information directly into an electronic case management system.

[19] Emergency needs such as food, clothing, medication, or shelter.
[20] Personal Assistance Services (PAS) are provided to individuals with disabilities to help with activities of daily living, such as grooming, eating, bathing, toileting, dressing and undressing. Personal Assistance Services also includes instrumental activities of daily living, such as taking medication and communicating and accessing programs and services. Personal Assistance Services includes a range of services that support independent living. Typically, Personal Assistance Services may be provided by home health agencies, independent contractors, Centers for Independent Living (CIL), family members, or friends.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

The project does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

Since survivors personally provide the Disaster Case Management intake information directly to a case manager, the information is presumed to be accurate. Survivors will have opportunities to review their information with the case manager for accuracy and completeness.

Survivors likewise provide registration intake information directly to the FEMA Individual Assistance Division. Refer to DHS/FEMA/PIA-049 Individual Assistance Program for more information about registration intake.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that FEMA, or its chosen provider, may collect more personal information from individual survivors than is authorized and necessary to provide Disaster Case Management.

Mitigation: This risk is mitigated. FEMA mitigates this privacy risk by limiting the information that may be collected to only the information necessary to provide Disaster Case Management. FEMA has worked with the DHS Privacy Office to ensure that only the appropriate information is collected as part of the FEMA-administered Disaster Case Management. FEMA adheres to the safeguards and notice requirements of the Privacy Act and the Paperwork Reduction Act. The chosen provider shall limit its collection of personal information to only those data elements listed in the Disaster Case Management Intake Form. Further, FEMA limits the disclosure of the Individual Assistance Division's focused registration dataset with chosen providers to only those applicants in population groups likely to benefit from Disaster Case Management. FEMA documents which data elements are shared, their authority and their purpose, through appropriate information sharing agreements.

Privacy Risk: There is a privacy risk that FEMA could maintain information about Disaster Case Management survivors that is inaccurate, incomplete, or no longer current.

Mitigation: This risk is mitigated. FEMA mitigates this privacy risk when a case manager meets with a survivor. The survivor will review their list of disaster-caused unmet needs and validate if those remain the same and/or if they need additional referrals to available resources to help meet those needs. During scheduled follow-up meetings with the survivor, the case manager will review the information provided, including contact information, with the survivor to confirm

its accuracy and update any of the inaccurate information recorded during the initial intake. In general, focused registration data is shared once with the chosen provider. However, if the client's information puts them in a different focused population eligible for programs becoming available later then the client's information could be subsequently shared, with any updates to the focused registration data being shared with the chosen provider. Clients may also request a hard copy of their information from their case manager. Moreover, clients can utilize the Disaster Case Management Consent Form to request a copy of their own Disaster Case Management case file.

Privacy Risk: There is a privacy risk that survivors could accidentally provide inaccurate contact information, resulting in FEMA, or its chosen provider, contacting a third party and giving them access to the survivor's inaccurate application information.

Mitigation: This risk is mitigated. FEMA mitigates this risk when case managers verify the individual's information by asking for clarifying information and/or a visual identification (e.g., driver's license) of the person they are speaking with to confirm that they are who they say they are and review contact information before any potential personally identifiable information might be discussed.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The purpose of the FEMA-administered Disaster Case Management is to address immediate, interim, or long-term disaster-caused unmet needs, to include development of individual disaster recovery plans and referrals to available resources. The program registration data collected from survivors is used to enable the chosen provider to proactively engage Individuals and Housing Program recipients and invite them to complete the necessary intake form in order to facilitate their recovery. FEMA, or its chosen provider, uses contact information, such as name, phone number, and email address, to determine interest in the Disaster Case Management and connect the survivor to a Disaster Case Management case manager who can help them address their unmet needs.

FEMA, or its chosen provider, uses the survivor-provided data to determine the severity[21] of the disaster-caused unmet needs and the types of referrals needed to assist the survivor with resolving those unmet needs. The tiers are used to assign a priority level to a case based on the survivor's severity of need and ability to recover. The Disaster Case Management case manager uses triage to determine the management caseloads. Clients with the highest priority level cases (tier 4), for instance, will have their needs revisited more frequently by the case manager. These survivors may have more immediate needs for food or shelter; typically, survivors who are highly dependent on social services, elderly, individuals with disabilities, or individuals with access and

[21] There are tiers (1-4) that are related to the types of survivor needs.

functional needs may need more intensive case management.

FEMA, or its chosen provider, uses contact information such as name, phone number, and email address, to connect the survivor to a Disaster Case Management case manager who will help them address their unmet needs. FEMA uses registration number and Disaster Case Management identifier to ensure individual client records are maintained in the correct files and that Individuals and Housing Program registration and Disaster Case Management intake information is not collected again.

Survivors report behavioral health information, such as names of those in distress and a brief description of symptoms or feelings of distress. The case manager will use the information to provide available resources like crisis counseling programs, community clinical providers, disaster distress helplines, counseling services, or a private counsel directory directly to the disaster survivor. The case manager does not provide any contact information to the referred source. Financial information, such as pre-disaster income and expenses and post-disaster income is used to determine potential referrals for income-based state/local assistance programs, such as Disaster Unemployment Assistance or Grant Assistance, and assist survivors in filling out applications for programs that provide financial assistance. Survivors may report information about their children to allow case managers to assess childcare and education needs and refer the survivor to community resources. The Disaster Case Management Intake Form, included as Appendix A to this Privacy Impact Assessment, will lead to the collection of data elements listed in Section 2.1.

While there is a paper collection form, the chosen providers will primarily be using the form as a reference of data elements they can collect while using their own case management database systems to guide the order in which the elements are collected. The data elements within the form are used to assess, screen, and refer disaster survivors to available resources that address their specific disaster-related unmet needs.

FEMA, or its chosen provider, collects and maintains records during Disaster Case Management implementation that will be used to provide these services and to monitor and assess the effectiveness of the FEMA-administered Disaster Case Management through the reporting of various metrics. Metrics can include reporting where the case managers are located (e.g., shelter or disaster recovery center), hiring, number of cases, open cases/closed cases, and types and numbers of referrals. Disaster Case Management responsibilities may also include making intake assessments and referrals for unmet needs; providing outreach and triage at locations such as shelters, congregate areas, and temporary disaster housing locations, or other community locations where there are individuals who have been impacted by the disaster and have unmet needs; developing and monitoring a disaster recovery plan, recovery goals referral resources, and status of survivor recovery efforts; connecting the disaster survivor to recovery resources that are locally available; and advocating for available resources to assist survivors.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

This effort does not use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or anomaly.

3.3 Are there other components with assigned roles and responsibilities within the system?

As discussed in Section 1.3, chosen providers will utilize their own IT systems to collect and store Disaster Case Management intake information. There is currently no FEMA IT system storing Disaster Case Management intake information. While chosen providers give direct support, FEMA's policy for managing the program does not require or allow other DHS components or FEMA programs to have a role in the chosen provider's system.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk that FEMA and its chosen providers receiving Disaster Case Management data about survivors could use information for purposes other than what was intended.

Mitigation: This risk is mitigated. FEMA mitigates this risk by ensuring that its chosen providers, through signed information sharing and access agreements, will be bound by the Routine Uses in the Disaster Case Management System of Records Notice. FEMA's chosen providers are required to agree to the terms and conditions and specific uses of the information.

Privacy Risk: There is a privacy risk that FEMA's chosen providers may collect personal information from disaster survivors through mission efforts separate from the FEMA-administered Disaster Case Management that could potentially be used inappropriately.

Mitigation: This risk is partially mitigated. FEMA partially mitigates this risk by ensuring that when FEMA-administered Disaster Case Management is activated, typically through a mission assignment or interagency reimbursable work agreement, FEMA and its chosen provider implement an appropriate information sharing and access agreement that will include provisions related to the unauthorized use of personally identifiable information and penalties for violations. Moreover, the written agreement with the chosen provider will specifically require the use of the Disaster Case Management Intake Form.

Privacy Risk: There a privacy risk that FEMA may share focused registration data about individuals who are not interested in or who do not need Disaster Case Management with providers.

Mitigation: This risk is partially mitigated. This risk is mitigated by limiting the disclosure of focused registration data to only those individuals who historically have needed additional assistance in effectively recovering in a timely manner. Moreover, Individuals and Housing Program registrants are provided an Individuals and Housing Program Consent Form to permit the disclosure of their information.[22]

Privacy Risk: There is a privacy risk that Disaster Case Management records may be maintained in a chosen provider's database that lacks the appropriate security and privacy controls to prevent unauthorized access, use or disclosure.

Mitigation: This risk is partially mitigated. FEMA requires that before sharing information with chosen providers, they must ensure that their database meets both FEMA and DHS standards prior to implementation of a FEMA-administered Disaster Case Management. FEMA conducts an assessment of chosen providers to ensure the contractor-owned or contractor-operated system maintains adequate controls to input, store, process, output, and/or transmit FEMA information in compliance with FEMA cybersecurity policy. This process is further outlined below in Section 8. FEMA follows all pertinent records schedules discussed in Sections 1.4 and 5.1 and will ensure that its chosen provider also follows the records schedules in accordance with the applicable written information sharing agreement. FEMA's Individual Assistance Division Records Liaison Officer (RLO) is responsible for ensuring that FEMA-administered Disaster Case Management records are not kept for longer than they are needed. FEMA information sharing agreements with chosen providers will include the records retention period of the survivor's records. The chosen provider is responsible for abiding by the terms and conditions of the information sharing agreements. In addition, the FEMA Records Branch provides instruction to inform FEMA programs and those that implement FEMA programs (e.g., chosen providers) about proper record retention, disposition requirements, records inventory training, file plan training, and file structure training to ensure that FEMA personnel are aware of all retention requirements.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

FEMA provides prior notice of its collection of information in several ways. First, FEMA will provide notice through this Privacy Impact Assessment and the Disaster Case Management System of Records Notice. Second, FEMA provides notice via Privacy Act Statements, which are

[22] *See* Authorization for the Release of Information Under the Privacy Act (FEMA Form 140-003d-1), *available at* https://www.fema.gov/sites/default/files/documents/fema_authorization-release-information-under-privacy-act-form.pdf.

included on both the Disaster Case Management Intake Form and Disaster Case Management Consent Form. FEMA staff or the chosen provider's case manager will read a Privacy Notice regarding the collection to members of the public prior to collecting any information over the telephone.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Participation in a FEMA-administered Disaster Case Management is completely voluntary. Should the survivor choose to participate, they will be given the Disaster Case Management Consent Form to sign and return to their respective case manager prior to any information being collected. Should the survivor choose to no longer participate in the program, they can contact their case manager who will ensure the survivor no longer receives referrals.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a privacy risk that individuals may not understand the purpose for FEMA collecting Disaster Case Management information and that information provided for one purpose may be collected for a different purpose.

Mitigation: This risk is mitigated. FEMA mitigates this risk by publishing the legal authority and purpose for collecting Disaster Case Management information in this Privacy Impact Assessment and the Disaster Case Management System of Records Notice. In addition, FEMA developed a standard Disaster Case Management intake form that will be used by chosen providers to conduct intake assessments with disaster survivors. Each form will adhere to Paperwork Reduction Act requirements and contain an approved Privacy Act Statement that lists the legal authority and purpose for collecting the information.

Privacy Risk: There is a privacy risk that Disaster Case Management applicants may not be aware that their chosen providers are collecting information on behalf of FEMA when they apply through a third-party provider such as the American Red Cross or HHS Administration for Children and Families.

Mitigation: This privacy risk is mitigated. FEMA provides notice by way of this Privacy Impact Assessment, the Disaster Case Management System of Records Notice, and the Privacy Act Statements or notices associated with Disaster Case Management-approved forms, and the Individual Assistance Program and Policy Guide (IAPPG).[23]

Privacy Risk: There is a privacy risk that Disaster Case Management applicants may not be aware that chosen providers will store their information in a third-party IT system, such as HHS

[23] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, FEDERAL EMERGENCY MANAGEMENT AGENCY, INDIVIDUAL ASSSISTANCE PROGRAM AND POLICY GUIDE, VERSION 1.1, *available at* https://www.fema.gov/assistance/individual/policy-guidance-and-fact-sheets

Administration for Children and Families' Electronic Case Management Record System (ECMRS) or the American Red Cross' Coordinated Assistance Network (CAN).

Mitigation: This risk is partially mitigated. This Privacy Impact Assessment serves as an additional notice regarding the way FEMA receives and manages Disaster Case Management data. Notice is also provided through the Privacy Act Statements or notices associated with Disaster Case Management -approved forms. HHS Administration for Children and Families has published a Privacy Impact Assessment for the use of their IT system for Disaster Case Management.[24]

Privacy Risk: There is a privacy risk that individuals may not be aware that FEMA proactively shares a dataset belonging to Individuals and Housing Program recipients identified to be most in need of Disaster Case Management.

Mitigation: This privacy risk is partially mitigated. FEMA provides a level of notice through the publication of this Privacy Impact Assessment, the Disaster Recovery Assistance Files System of Records Notice, and the Disaster Case Management System of Records Notice. FEMA does not limit data sharing to Individuals and Housing Program recipients who may need or want Disaster Case Management. Disaster Case Management chosen providers act on behalf of FEMA and are obligated under a formal information sharing agreement to adhere to DHS/FEMA security and privacy requirements. However, since Disaster Case Management is not a data element in the Individual Assistance system, there is a residual risk that survivors who are not interested in Disaster Case Management or do not have an unmet need may have their information shared with chosen providers. FEMA will only share with the chosen provider focused registration data that is necessary to narrow the pool of Individuals and Housing Program registrants who FEMA identifies as likely to benefit from Disaster Case Management (e.g., those over the age of 65, those with FEMA-verified loss, and those who may have an emergency need). This data includes, but is not limited to, contact information for disaster survivors. Once the chosen provider has contacted the survivor and the survivor indicates they want Disaster Case Management, the chosen provider will begin intake and create a case file for the survivor. Data for individuals who decline participation will be destroyed in accordance with the appropriate record retention schedule.

Section 5.0 Data Retention by the Project

5.1 Explain how long and for what reason the information is retained.

In accordance with NARA Authority N1-311-86-1, Item 4C6a, general FEMA-administered Disaster Case Management files covering the management, program and information functions should be consolidated at appropriate regional offices upon close of the disaster field

[24] *See* U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, OFFICE OF HUMAN SERVICES EMERGENCY PREPAREDNESS AND RESPONSE, PRIVACY IMPACT ASSESSMENT FOR THE ADMINISTRATION FOR CHILDREN AND FAMILIES, (2017), *available at* https://www.hhs.gov/sites/default/files/acf-electronic-case-management-record-system.pdf.

office (DFO). These files should retire to off-site storage one year after closeout and destroyed three years after closeout.

In accordance with NARA Authority N1-311-6-1, Item 4C10a, records pertaining to disaster assistance, which include FEMA-administered Disaster Case Management files, such as Disaster Case Management intake and referral records, should retire to inactive storage when two years old and be destroyed when six years, three months old.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that FEMA, or the chosen provider, could retain the data for a longer period than necessary and not in accordance with the NARA-approved records disposition schedules.

Mitigation: This risk is partially mitigated. FEMA follows all pertinent records schedules discussed in Sections 1.4 and 5.1 and will ensure that its chosen provider also follows the records schedules in accordance with the applicable written information sharing agreement. In addition, the FEMA Records Branch provides trainings to inform FEMA programs of proper record retention, disposition requirements, records inventory training, file plan training, and file structure training to ensure that FEMA personnel are aware of all retention requirements. FEMA's Individual Assistance Division Records Liaison Officer (RLO) is responsible for ensuring that FEMA-administered Disaster Case Management records are not kept for longer than they are needed. FEMA information sharing agreements with chosen providers will include the records retention period of the survivor's records. It is the responsibility of the chosen provider to abide by the terms and conditions of the information sharing agreements.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

FEMA shares information outside of DHS with federal, state, tribal, and local entities, voluntary organizations, or FEMA-recognized and/or state-recognized Long Term Recovery Committees and their members (Long Term Recovery Groups) for the purposes of providing case management services and referrals to resources to address disaster-caused unmet needs following a major disaster declaration by the President of the United States that includes Individual Assistance.

I. Information shared with chosen providers to operate Disaster Case Management on FEMA's behalf

FEMA shares information with chosen providers and contractors and their agents

performing FEMA-administered case management for survivors. The information is shared: (1) under contract with a non-profit organization or qualified private organization that implements Disaster Case Management on behalf of FEMA, or (2) through interagency agreement or mission assignment with a federal agency who implements Disaster Case Management on behalf of FEMA.

The information is shared with FEMA-administered Disaster Case Management providers, such as the HHS Administration for Children and Families, the American Red Cross, and other voluntary entities or contractors once they have been selected to provide Disaster Case Management on behalf of FEMA and all parties have signed an approved information sharing agreement. The information is provided by encrypted file in an email attachment—per DHS guidelines—to the appropriate points of contact listed in the information sharing agreement.

Source data will be extracted from the Individual Assistance system by the Recovery and Analytics Division (RAD) within the FEMA Office of Response and Recovery. The Recovery and Analytics Division forms the dataset into an encrypted data file and sends the encrypted file by email to the chosen provider. Alternatively, data files too large to email will be encrypted and sent via the FEMA Secure Data Sharing Community of Interest on the Homeland Security Information Network (HSIN).[25]

II. Information shared with referral resources during Disaster Case Management

FEMA or its chosen provider may, with a signed consent form, share information collected from disaster survivors with a referral resource. Referrals may include those for temporary shelter, food, clothing, and medical assistance. Generally, survivors directly submit information to referral resources, such as applications for financial assistance or services. Moreover, in the event that FEMA or its chosen provider needs to provide a subset of information to a referral resource, the survivor will have provided their consent in writing. Through the Disaster Case Management Consent Form, the survivor can acknowledge the Privacy Act notification and consent to the FEMA chosen provider sharing the survivor's data with local and other available resources to address unmet needs through case management services. FEMA does not share personally identifiable information with referral resources unless the survivor seeks Disaster Case Management.

III. Information shared with states, non-profits, and Long-Term Recovery Groups at FEMA-Administered Disaster Case Management closeout

At the end of the FEMA-administered Disaster Case Management period of performance, FEMA, or its chosen provider, may share data with states, non-profits, and Long-Term Recovery Groups either pursuant to a federal award or to ensure continuity of services in the absence of a

[25] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR HSIN 3.0 SHARED SPACES ON THE SENSITIVE BUT UNCLASSIFIED NETWORK, DHS/ALL/PIA-061, *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

federal award. FEMA, or its chosen provider may share cases that were closed due to lack of resources, pending resource availability. Pursuant to Disaster Case Management closeout procedures, a chosen provider will inform FEMA of the need to further share data. Source data will be extracted from the chosen provider's case management system. Data files too large to email will be encrypted and sent via the FEMA Secure Data Sharing Community of Interest on the Homeland Security Information Network or another DHS-approved mechanism.

The survivors, with assistance from their case managers, will complete applications for aid from Long-Term Recovery Groups. Long-Term Recovery Groups prioritize survivors based on their application information and work to obtain the resources to assist them.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The external information sharing discussed in Section 6.1 is done under Routine Uses H, I, K, and L of the Disaster Case Management System of Records Notice. These Routine Uses allows for a more effective implementation of the FEMA-administered Disaster Case Management.

Routine Use H allows FEMA to share information with contractors and their agents performing case management services to survivors under a contract with a non-profit organization or qualified private organization who implements Disaster Case Management on behalf of FEMA. It also allows sharing with a federal agency who implements Disaster Case Management on behalf of FEMA through an interagency agreement or mission assignment, and allows sharing with a state or local government or tribe who implements their own Disaster Case Management program through a grant or cooperative agreement. This sharing is compatible with the original purpose of collection because FEMA conducts these information sharing activities in order to provide case management services to survivors, assisting in their road to recovery by finding resources to address their disaster-caused unmet needs.

Routine Use I allows FEMA to share applicable information necessary with voluntary organizations or to a FEMA-recognized or state-recognized Long-Term Recovery Committees and its members (Long-Term Recovery Groups) actively involved in recovery efforts. FEMA, or its chosen provider, shares information with these organizations so that case managers can advocate for resources for their client to assist them with alleviating their disaster-caused unmet needs.

Routine Use K allows FEMA to share information with recipients of a Disaster Case Management federal award to ensure the continuity of services for each disaster survivor.

Routine Use L allows FEMA to share the name, title, and business contact information of the employee or contractor providing Disaster Case Management assistance with the FEMA-administered Disaster Case Management client. In doing so, the client will have access to their

case manager for follow-up.

6.3 Does the project place limitations on re-dissemination?

Prior to implementing FEMA-administered Disaster Case Management, FEMA enters into an agreement with the chosen provider. These agreements include Mission Assignments, interagency reimbursable work agreements, and/or contracts. The agreements with these providers outline when and how data may be shared and is reinforced with an information sharing agreement that is signed by both FEMA and the provider.

Once FEMA shares information with the chosen provider, the provider may not further share the survivor's information without a signed consent form. At the time of intake, the case manager will provide the survivor with the Disaster Case Management Consent Form for their review and signature. The Disaster Case Management Consent Form allows the survivor to determine if the provider can share their information, what information may be shared, and to whom they can share the information with.

At the end of the FEMA-administered Disaster Case Management, the provider who implemented the program may share the data originally shared by FEMA along with the data collected by the provider with the recipient of the FEMA-funded Disaster Case Management federal award (e.g., grant or cooperative agreement). Before sharing with the federal award recipient, FEMA will ensure that there is an information sharing agreement in place setting forth the terms of the sharing and limiting any further re-dissemination as well as a FEMA-State/Tribe Agreement that complies with both FEMA and DHS policy.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

FEMA routinely shares personally identifiable information outside of DHS with those entities identified in the Disaster Case Management System of Records Notice for the purposes of providing disaster assistance, meeting survivor needs, and preventing the duplication of benefits. These disclosures are memorialized through various documents, including information sharing agreements, FEMA-State/Tribe Agreements, and Routine Use letters, which are maintained by the Office of Response and Recovery.

FEMA is capable of recreating whose records within FEMA systems were transmitted to a given external entity based on the documented information sharing agreement. FEMA will ensure that its chosen providers through written agreements, such as an information sharing agreement or a memorandum of agreement (MOA), maintain an accounting of disclosures.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a privacy risk that FEMA could share more information than is

needed with a chosen provider.

Mitigation: This risk is mitigated. FEMA enters into an agreement with the chosen provider prior to implementing Disaster Case Management. These agreements include Mission Assignments, interagency reimbursable work agreements, and/or contracts. The agreements with these providers outline when and how data may be shared and is reinforced with an information sharing agreement that is signed by both FEMA and the provider. FEMA will only share focused registration data with chosen providers pursuant to Routine Use H and the sharing agreements described in Section 6.1. FEMA will review these agreements every two years or as changes are made. FEMA will review the security documents at least every three years for any newly identified risks. Any newly identified risks will be mitigated between the partnering agencies in accordance with applicable laws.

Privacy Risk: There is a privacy risk that FEMA or its chosen provider could share information with entities outside of DHS for purposes other than those outlined in Section 6.1.

Mitigation: This risk is mitigated by the review and approval of information sharing agreements with chosen providers and the assessments performed by FEMA, as covered in section 8 of this privacy impact assessment. FEMA will only share information with other entities and agencies pursuant to the sharing agreements described in Section 6.1. FEMA will review these agreements every two years or as changes are made and review appropriate security documents at least every three years for any newly identified risks. Any newly identified risks will be mitigated between the partnering agencies in accordance with applicable laws.

Prior to implementing FEMA-administered Disaster Case Management, FEMA will enter into an agreement with the chosen provider. These agreements include Mission Assignments, interagency reimbursable work agreements, and/or contracts. The agreements with these providers outline when and how data may be shared and is reinforced with an information sharing agreement that is signed by both FEMA and the provider.

Privacy Risk: There is a privacy risk that FEMA or its chosen provider could erroneously disclose information to an unauthorized party.

Mitigation: This risk is mitigated. FEMA and its chosen providers are only permitted to share information outside of DHS pursuant to the routine uses found in the Disaster Case Management System of Records Notice, and only pursuant to information agreements signed by FEMA and the external entity. Any unauthorized disclosure of personally identifiable information constitutes a privacy incident that must be reported to the FEMA privacy officer within 24 hours of suspicion, discovery, or notification, in accordance with the information sharing agreement.

The Recovery and Analytics Division will extract source data from the Individual Assistance system as an encrypted data file and send it via email to the chosen provider. Authorized State/tribe points of contact listed in the information sharing agreement receive personally

identifiable information from FEMA contained within encrypted files attached to emails, per DHS guidelines. Data files too large to email will be encrypted and sent via FEMA Secure Data Sharing community on the Homeland Security Information Network.

Privacy Risk: There is a privacy risk that more information than needed could be shared with referral resources (e.g., voluntary organizations) during Disaster Case Management.

Mitigation: This risk is mitigated. Survivors directly submit information to referral resources, such as applications for financial assistance or services, and FEMA or its chosen provider will not collect data elements within an application that is being submitted to a referral resource. Moreover, in the instance that FEMA or its chosen provider needs to provide a subset of information to a referral resource, the survivor will have provided their written consent. For example, a chosen provider may share a client's name, contact information, and information needed to perform a construction analysis where limited funds are allocated. Prior to Disaster Case Management intake, the survivor signs a consent form permitting the FEMA chosen provider to share their data with local and other available resources. Through the consent form, the survivor will acknowledge a Privacy Act notice. A different consent form may be used if the survivor wants the chosen provider to share their information with an entity not covered by the standard consent form.

Privacy Risk: There is a privacy risk that FEMA, or its chosen provider, may use a survivor's information for unauthorized purposes or share it with unauthorized parties.

Mitigation: This risk is mitigated. FEMA mitigates this risk by publishing a Disaster Case Management System of Records Notice that states the purpose of the collection and permissible routine uses for disclosure. In addition, case managers will provide a consent form to obtain the survivor's written approval for informed resource referrals and advocacy to meet their disaster-caused unmet needs. Finally, FEMA will execute information sharing agreements with third parties that requires secure access to survivor information and require written confirmation that only those with a need to use the data can access it.

FEMA considers any third-party sharing of information without the express consent of FEMA a violation of the terms of agreement. FEMA will investigate any sharing that conflicts with the terms and understandings of any contract or agreement to determine malintent or gross neglect and take steps to stop any inappropriate sharing of information, such as termination of the contract/agreement. DHS/FEMA will coordinate or consult with the appropriate law enforcement agency, such as the Department of Justice, to retrieve inappropriately shared information and to ensure any inappropriate sharing of FEMA information has ceased and FEMA information has been removed from the property of any inappropriate third-party recipient(s). Specifically, DHS/FEMA will seek to recover the personally identifiable information of survivors, as practicable. FEMA or the organization that caused the breach of personally identifiable

information will provide further remediation as needed and appropriate to include notification of individuals that have been affected by the breach.

Privacy Risk: There is a privacy risk that FEMA may receive a request from a federal award recipient to gain access to a disaster survivor's personally identifiable information generated in a FEMA-administered Disaster Case Management mission to, for instance, establish their long-term Disaster Case Management program.

Mitigation: This risk is mitigated. FEMA only shares information allowable under the Disaster Case Management System of Records Notice and as outlined in the fully executed and signed information sharing agreement. FEMA will request that the chosen provider transfer the data via email with an encrypted file to the Disaster Case Management federal award recipient point of contact or will receive the data via secure file transfer from the FEMA-administered Disaster Case Management chosen provider. FEMA also requires that chosen providers hold the information in encrypted spreadsheets until the recipient is able to receive the information, and then provide that information to the state via secure file transfer after ratifying the appropriate information sharing agreement with the requesting entity.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Once the survivor has provided their information and been assigned a case manager, the survivor will meet with their case manager at an agreed upon interval. During these meetings, the case manager and survivor will review the information provided and the survivor will have the opportunity to correct any information that may be inaccurate. Survivors may also request a hard copy of their information, including the disaster recovery plan, from their case manager. Moreover, survivors can utilize the Disaster Case Management Consent Form to request a copy of their own Disaster Case Management case file. Alternatively, individuals may submit a Freedom of Information Act (FOIA) request to the FEMA Privacy Officer.

Any individual may seek notification of and access to any FEMA record pursuant to procedures provided by Freedom of Information Act and can do so by visiting https://www.dhs.gov/dhs-foia-privacy-act-request-submission-form, or by mailing a request to:

FEMA Disclosure Branch
Federal Emergency Management Agency
Department of Homeland Security
500 C Street, SW
Washington D.C. 20742

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

In addition to the steps outlined in Section 7.1 above, individuals may submit a Privacy Act Amendment request to FEMA at the address above. For Individuals and Housing Program registrants, survivors may correct certain data that they entered inaccurately via www.disasterassistance.gov by logging into their account and making the appropriate corrections.

7.3 How does the project notify individuals about the procedures for correcting their information?

Disaster Case Management survivors are notified when they meet with their case manager to correct any inaccurate information. During intake, the case manager will remind the survivor that at each subsequent meeting they will review the accuracy of the data provided and provide the survivor with the opportunity to update anything that may be inaccurate.

Further, the Disaster Case Management System of Records Notice and Disaster Recovery Assistance Files System of Records Notice (see "Contesting Record Procedures") outlines how individuals may make a request for amendment or correction of a record of the Department about the individual by writing directly to the Department component that maintains the record, unless the record is not subject to amendment or correction. The request should identify each particular record in question, state the amendment or correction desired, and state why the individual believes that the record is not accurate, relevant, timely, or complete. The individual may submit any documentation that would be helpful. If the individual believes that the same record is in more than one system of records, the request should state that and be addressed to each component that maintains a system of records containing the record.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a privacy risk that survivors may not be aware of how to access or correct their information.

Mitigation: This risk is mitigated. FEMA, or its chosen provider, will review the survivor's information at each meeting to confirm its accuracy. Survivors may request a hard copy of their information, including the disaster recovery plan, from their case manager. Moreover, survivors can utilize the Disaster Case Management Consent Form to request a copy of their own Disaster Case Management case file. Finally, the Disaster Case Management System of Records Notice and Disaster Recovery Assistance Files System of Records Notice (see "Contesting Record Procedures") provides that individuals may make a request for amendment or correction of a record of the Department about the individual by writing directly to the Department component that maintains the record, unless the record is not subject to amendment or correction.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

As stated in this Privacy Impact Assessment, FEMA will principally utilize HHS Administration for Children and Families, through a mission assignment, and American Red Cross, through an interagency reimbursable work agreement to provide FEMA-administered Disaster Case Management. HHS Administration for Children and Families and American Red Cross will use their own proprietary systems of record to collect and store Disaster Case Management information. FEMA will ensure that the chosen provider's system is consistent with Homeland Security Acquisition Regulation (HSAR) Class Deviation 15-01, Safeguarding of Sensitive Information, and/or security plan requirements in connection with the Authority to Operate and risk assessment.

FEMA contractors and their agents will undergo a rigorous assessment to ensure the contractor-owned or contractor-operated system maintains adequate controls to input, store, process, output, and/or transmit FEMA information or data in compliance with FEMA cybersecurity policy. Contractor IT systems are self-monitored or audited to capture all user activities. FEMA IT security teams routinely conduct audits to ensure that there is no misuse of Individual Assistance data and that users are following FEMA's rules of behavior. FEMA also encrypts all applicant data while in transit and at rest.

FEMA includes privacy safeguards within an information sharing agreement to extend control of FEMA's information while used by chosen providers or other external sharing partners. FEMA is responsible for enforcing its information sharing agreements and may require partners to immediately stop sharing FEMA information if found not to be abiding by the agreement. Additionally, any FEMA Regional Office may consult the FEMA Office of Professional Responsibility (OPR), Office of the Chief Counsel (OCCC), and Office of the Chief Procurement Officer (OCPO) for other appropriate action to ensure compliance with this Privacy Impact Assessment and DHS policy for safeguarding personally identifiable information.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All FEMA employees and FEMA contractors are required to complete FEMA Office of Cybersecurity Security Awareness Training and Privacy Awareness Training annually. FEMA does not require Disaster Case Management-chosen providers to perform training beyond their own organization's requirements. FEMA standard information sharing agreements stipulate that chosen providers are responsible for ensuring that all staff are trained on the proper procedures for handling, protecting, and disposing of personally identifiable information.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

FEMA chosen providers will undergo a rigorous assessment to ensure the contractor-owned or contractor-operated system maintains adequate controls to input, store, process, output, and/or transmit FEMA information in compliance with FEMA cybersecurity policy. In general, this includes the following:

- Role-based access controls to control user rights to both data and functionality;
- Defined permissions for access to data and functions used to manipulate the data;
- Initial approval to obtain access to the IT system;
- Limited access to support troubleshooting of technical system issues; and
- Security access controls and administers users' roles and permissions based on organizational positions.

Furthermore, as stated in the appropriate information sharing agreement, any party who receives or is granted access by FEMA or its chosen provider to any personally identifiable information must agree in writing with FEMA to abide by the terms and conditions in the information sharing agreement, restrict use of survivor personally identifiable information only to the performance of Disaster Case Management, and certify in writing, upon completion of the performance of services by a contractor, that the contractor has immediately un-installed, removed, and/or destroyed all copies of FEMA survivor personally identifiable information within 30 days of the recipient's performance of services to FEMA or its chosen provider.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Any information sharing agreements, including Interconnection Security Agreements, FEMA-State Agreements, Memoranda of Agreement/Understanding (MOU/MOA), or Routine Use letters, will be reviewed by the FEMA Privacy Branch and FEMA Office of Chief Counsel. All other contractually based information sharing endeavors outside of FEMA are reviewed by the FEMA Office of Chief Counsel, each party to the agreement, the FEMA Office of the Chief Information Officer, and the FEMA Privacy Branch.

8.5 Privacy Impact Analysis: Related to the Accountability and Integrity of the Information.

Privacy Risk: There is a risk that individuals without a need to know may access FEMA personally identifiable information.

Mitigation: This risk is partially mitigated. FEMA contractors and their agents will undergo a rigorous assessment to ensure the contractor-owned or contractor-operated system maintains adequate controls to input, store, process, output, and/or transmit FEMA information or data in compliance with FEMA cybersecurity policy. FEMA includes privacy safeguards within its information sharing agreements with the chosen providers or contractors to extend control of FEMA's information while used by chosen providers or other external sharing partners.

Contact Official

Blair McDonald
Deputy Director for Individual Assistance Division (Acting)
Recovery Directorate
Federal Emergency Management Agency

Responsible Official

Tammi Hines
FEMA Privacy Officer
Office of the Chief Administrative Officer
Mission Support
Federal Emergency Management Agency

Approval Signature

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

_____

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

APPENDIX A: FEMA-ADMINISTERED DISASTER CASE MANAGEMENT INTAKE FORM

(Please note that the official form is in draft and will be supplied by FEMA to the chosen provider for implementation once approved by OMB. The current draft version of this form can be found on the DHS website on the landing page for this PIA.

APPENDIX B: APPROVED FEMA-ADMINISTERED DISASTER CASE MANAGEMENT CASE MANAGEMENT SYSTEMS

FEMA will update this appendix with a list of provider and system names once those providers and systems are identified.