Privacy Impact Assessment
for the

Contact Center Capability Modernization Program (C3MP)

DHS/FEMA/PIA-043
April 11, 2017

Contact Point
James Hayes
Recovery Technology Programs Division
Federal Emergency Management Agency
(540) 686-3772

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

Abstract

The Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA), Office of Response and Recovery (ORR), Recovery Directorate, Individual Assistance (IA) Division, Recovery Technology Programs Division (RTPD) operates the Contact Center Capability Modernization Program (C3MP) system. The C3MP is a contact center management system designed to provide high quality support services to disaster survivors requesting assistance under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act) during Presidentially-declared disasters. It also provides FEMA the capability to evaluate employee and contractor performance when responding to applicants' calls in order to provide improved customer service. FEMA is conducting this Privacy Impact Assessment (PIA) because the C3MP captures personally identifiable information (PII) about applicants to provide status updates regarding their disaster applications. The C3MP also gathers data about FEMA employees and contractors to monitor and enhance the quality of service provided by FEMA.

Overview

FEMA Office of Response and Recovery (ORR) Directorate, Individual Assistance (IA) Division's Recovery Technology Program Division (RTPD) operates the Contact Call Center Management Program (C3MP). C3MP processes applicant calls FEMA receives via the toll-free assistance numbers available to the public. Disaster applicants call FEMA for various reasons, including inquiring on the status of applications, updating their application information, or completing a customer service assessment. C3MP provides FEMA call centers the capability to: route disaster applicant calls to the appropriate destination; manage employees for calls center and auxiliary disaster duties; and manage call recording for the quality assurance of employees and training.

As part of a modernization effort of the FEMA call centers, C3MP consolidates the function of and replaces 3 existing systems:

1) Advanced Call Center Network (ACCN) - ACCN provides the intelligent routing of applicant calls to ensure quality support services to callers;
2) Electronic Work Force Management (eWFM) - The eWFM manages the call center workforce and performance by providing forecasting, scheduling, and tracking of duties to ensure the call centers are appropriately staffed; and
3) Quality Assurance Recording System (QARS) - The eWFM provides call centers a means to evaluate call center employee and contractor by recording calls and screen shots.

The C3MP platform is comprised of and uses three core components.

1. Inter-Exchange Carrier (IXC) 800 Network

IXC 800 Network is the 1-800 service and interactive voice response (IVR) component of C3MP. The IVR enables the call centers to determine applicant requirements by using touch-tone recognition. The IVR delivers automated messages to the caller and interacts with the FEMA Individual Assistance (IA) System[1] database for self-help requests that provide status information without agent interaction. The Operational Data Store (ODS)[2] is the system that updates the IA database nightly. This update provides the applicant with a current status. The IVR collects information from applicants in order to provide verification for self-help automatic status. Some examples of this information are: date of birth and Registration ID.[3]

2. Consolidated Interaction Center (CIC)

CIC desktop software applies established business rules to the call center management. These include: hours of operation; disaster specific guidelines; and expected caller delay settings. This function helps determine the best way to route the applicant's call based on: the keypad options the applicant chooses; the established business rules; and what call center has an available Human Services Specialist (HSS). HSS personnel are live call center operators who are either FEMA employees or contractors.

3. Workforce Optimizer

Workforce Optimizer provides workforce management capabilities, such as call volume forecasting, work schedule generation, and associated reports. The Workforce Management function collects information from FEMA employees and contractors, such as name, email address, and network user ID, to allow case workers or supervisors to review prior phone conversations. This allows a history to be maintained containing the identity of the agent who assisted an applicant, notes to help an agent who accepts a follow-up call, and for quality assurance reviews.

Voice and Screen Recording

C3MP records 100% of all incoming and outgoing calls to and from FEMA's designated disaster assistance helplines, customer satisfaction assessment responses, and internal lines used for HSS support by National Coordination Team Assistance Group (NCT AG). FEMA may reduce this percentage during times of extremely high call volumes. Voice recordings are initiated when:

[1] The DHS/FEMA/PIA-027 National Emergency Management Information System –Individual Assistance (NEMIS-IA) Module PIA is currently undergoing updates. The latest version of the document can be found here: https://www.dhs.gov/sites/default/files/publications/privacy_pia_fema_027_2012.pdf.
[2] For more information, please see DHS/FEMA/PIA-026 Operational Data Store (ODS) and Enterprise Data Warehouse (EDW) (June 29, 2012), found here: https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_fema_ods_edw_20120629.pdf.
[3] See Section 2.1 for a full list of data collected.

- An applicant calls FEMA's 1-800 line regarding disaster assistance;
- An applicant calls FEMA (or is called by FEMA) in response to FEMA's request for customer satisfaction assessment;
- A FEMA employee or contractor calls the Recovery Service Center (RSC) internal department for support during a transaction with a disaster assistance applicant; or
- A FEMA employee or contractor calls through designated lines in the course of the registration and case review process.

C3MP collects and maintains voice recordings and the corresponding desktop screen snapshots of the following transaction types:

- FEMA employees, contractors, and/or disaster assistance applicants to provide assistance or as part of the customer satisfaction assessment process;
- FEMA employees or contractors who assist disaster applicants;
- FEMA employees or contractors during non-call-related case review for quality assurance reviews and training purposes;
- FEMA supervisory staff, quality control specialists, or contract oversight specialists' evaluation of employee or contractor calls and case review screen transactions; and
- RSC supervisors, quality control specialists, and training specialists' evaluations to ensure alignment and consistency across the enterprise.

All employees, contractors, and applicants receive notification that their calls are being recorded.

A typical call transaction using C3MP will take place after the President of the United States declares a disaster following a particular event. Once a disaster has been declared, an applicant may call the toll-free FEMA assistance number to apply for IA. Following the initial recorded FEMA greeting that includes a notice to the caller that the call is being recorded, the caller must specify which language preference, English or Spanish. If a language option is not chosen, the applicant is routed to an HSS. The IVR provides the caller with the Uniform Record Locator (URL) for the FEMA Disaster Assistance website (http://www.disasterassistance.gov/). The applicant is asked to enter the five-digit ZIP code for the area in which the damage occurred. If the call comes outside the hours of operation or during an observed holiday, a closed message with hours of operation and the FEMA Disaster Assistance website (http://www.disasterassistance.gov/) are given, through which the applicant can apply for assistance on the FEMA website. If the call is within the hours of operation, then the main menu provides the applicant with three call-routing options: 1) apply for disaster assistance; 2) automated self-help/status check; and 3) helpline, whereby an applicant gets connected with a HSS who may

help update his or her disaster application or provide other assistance. The IVR routes the call or notifies the caller of the minimum expected delay. Below are more details on each option:

Option 1) Apply for disaster assistance: First, the C3MP connects the caller to an automated Privacy Act (PA) Notice (attached as Appendix A). The next message provides the applicant with a list of information needed to complete the registration intake interview. After the notice, C3MP routes the applicant to a queue to connect him or her to the next available HSS to perform the registration intake interview. The applicant's connection to C3MP ends once he or she is routed to the HSS queue. An applicant cannot complete a registration via telephone keypad inputs through C3MP.

Option 2) Automated self-help/status check: C3MP connects the applicant to the self-help menu. The applicant is asked to provide all of the following for verification purposes: FEMA registration ID, last four digits of the disaster applicant Social Security number (SSN); and date of birth. The applicant enters the data via keypad, which is then queried against the IA database for authentication. If any of the information provided by the applicant does not match information in the IA database, the IVR responds with an error message. Following several failed validation attempts, the applicant is then transferred to a queue to then connect to the next available live HSS. The HSS will verify the applicant's identity by asking for a combination of: first and last name, last 4 of the social security number, address, phone number and date of birth. These questions are used to verify the information that was given to FEMA during the applicant's initial intake.[4] On the other hand, if the information entered is correctly, the entered data is authenticated against the IA database, and the applicant receives an automated status update. C3MP does not provide any PII in the automated status update. Once the applicant has completed self-help, the applicant may hang up or opt to be transferred to a queue to speak with a HSS.

Option 3) Helpline: C3MP connects the applicant to a queue, which then connects to a HSS to assist with the disaster application updates and/or questions. In this case, the HSS provides the Privacy Act statement (attached in Appendix A) to the applicant before requesting any additional information from the applicant.

The call recording starts once the caller and FEMA employee or contractor are connected on FEMA designated disaster assistance help lines. Calls placed to and from non-designated disaster assistance help lines are not recorded in C3MP. FEMA provides notice of recording to callers via a pre-recorded Privacy Act Statement while callers wait in queue to speak with a FEMA employee or contractor. FEMA employees and contractors who speak with applicants read a

[4] This verification process falls outside the scope of C3MP and will be discussed more fully in a forthcoming Individual Assistance PIA.

scripted Privacy Notice. Employees and contractors are informed during training that their calls and screenshots will be recorded and monitored for quality assurance.

FEMA employee or contractor desktop computer screens may also be recorded to accompany the voice transaction. If a call also includes desktop screen captures the screen recording begins simultaneously with the voice recording. Recording the desktop screens during voice transactions allows the quality control specialist or supervisor to observe the FEMA employee or contractor's disaster assistance data entry and case review accuracy.

Desktop Screen Recording Not Related to a Telephone Call

In addition to answering telephone calls, FEMA employees and contractors process disaster assistance applications by reviewing the applicant's case file maintained in the IA system to determine eligibility. During this case review and processing, C3MP records a random percentage of desktop computer screen shots based on the FEMA employee or contractor's identification or particular work assignment.

A portion of the recorded screen shots are evaluated in C3MP, archived, and held for six years to allow time to resolve any personnel matters that may arise from the use of C3MP data for employee or contractor performance evaluations or to determine qualifications for continued employment. Recordings for evaluation can be selected randomly and assigned to quality control staff for review. Supervisors can also select recordings of their team members and perform evaluations for quality. FEMA purges the screen shots that are not used in an evaluation of a FEMA employee or contractor within 45 days.

Quality Evaluation

The supervisor, quality control specialist, contract specialist, or training specialist performs evaluations that are maintained in C3MP. FEMA sets targets for the percentage of RSC transactions to be evaluated in C3MP based on factors including: call volumes, special project initiatives (e.g., a recertification project), and training objectives. C3MP recordings are selected randomly or targeted for evaluation of the quality of service delivered to the disaster assistance applicant. The evaluator uses the appropriate FEMA-approved QARS evaluation form to assess the employee or contractor's quality of work along with a system-generated result. These results are generated by weighing various evaluation criteria. Supervisors grade the employees' quality of interactions with members of the public, FEMA employees, and contractors that are included in the results. C3MP then assigns scores to each criterion. The tabulation is based on the combination of these scores and weights. C3MP stores the result and the supervisor retrieves it using the employee or contractor's name and user identification number for subsequent review and evaluation. C3MP quality evaluations are typically made available to the employee or contractor for review and possible discussion.

FEMA also determines training opportunities for its employees and contractors based on the evaluations stemming from the C3MP recordings. Contact staff calls are evaluated by FEMA supervisory, quality control, or contract oversight staff according to the contract provisions between FEMA and the contracting entity. Calibration sessions are conducted in which representatives from each RSC perform evaluations on recorded transactions, compare results, and establish consensus on the quality management process to ensure calls are evaluated in a consistent manner across the RSCs.

C3MP recordings can be played back at the discretion of the supervisor or quality control reviewer. C3MP records are used as training tools for employees and contractors during their quality control evaluation process. Through C3MP, RSC HSS supervisors and Special Processing Unit (SPU) staff are able to assess the quality of service provided to applicants. Customer Survey & Analysis (CSA) supervisory staff ensures delivery of quality service by those performing customer satisfaction assessments of both IA and Public Assistance (PA) recipients. The program assists the Training Department and NCT AG by providing consistent guidance and training recommendations based on findings from the recordings. C3MP provides Individual Assistance Contract Management Section (IA-CMS) with insight to measure the level of quality and performance provided by contract staff both within the RSC or providing support remotely, such as language translation services.

FEMA Employee and Contractor Desktop Software Usage

Supervisory and performance management staff use C3MP to analyze the performance of employees or contractors. To do so, they document how the employees and contractors navigate through the various software applications used to provide customer service to applicants. Application usage is logged by C3MP and used to assess current processes and employee performance to optimize efficiency within the RSCs by providing data related to the length of time spent in systems or applications throughout the day. The primary privacy risk with C3MP is that information collected from applicants can be used in a manner inconsistent with the purpose of collection.

FEMA mitigates this risk by implementing the following controls: 1) C3MP does not retain the PII that the applicant inputs via the telephone keypad; 2) FEMA has limited the PII requested from the applicant to only what is necessary to match the applicant and the disaster registration requested; and 3) all information within audio recordings and screen captures is collected to evaluate employee and contractor performance. Voice recordings are held for six years. Those portions of the screen-only recordings that are reviewed for workforce quality assessment are archived and held for six years to allow time to resolve any personnel matters that may arise from the use of quality assessment data for employee or contractor performance evaluations or to determine qualifications for continued employment. FEMA purges screen-only recordings that are not used in an evaluation of a FEMA employee or contractor within 45 days.

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?

C3MP is authorized to collect information in order to properly administer the programs that are authorized and described in this PIA. C3MP collects, uses, and maintains the records within this system under the authority of:

- Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. § 5174 (Stafford Act). Section 408 of the Stafford Act authorizes FEMA, as the designee of the President of the United States, to provide federal assistance to individuals and households. The same section mandates the creation of a system of records to identify recipients, of which C3MP is a part.
- E-Government Act of 2002, 44 U.S.C. § 101, requires enhancements to improve the performance of Government in collaborating on the use of information technology to improve the delivery of Government information and services. C3MP uses technology to improve the delivery of disaster assistance.
- 5 U.S.C. § 4302. The establishment of performance appraisal systems is required by the DHS regulation. C3MP implements part of the performance appraisal system for Call Center operators.
- 6 U.S.C. § 795. The establishment of controls to prevent fraud, waste, and abuse is required by DHS. C3MP facilitates the intake of information used to determine eligibility and implements part of the control for the prevention of fraud, waste, and abuse.
- Executive Orders 13571 and 13411. These Executive Orders require streamlining service delivery and customer service and improvement of assistance to disaster survivors. C3MP serves to improve customer service functions at the FEMA Call Center used by disaster survivors.
- The authority to collect SSN during the process of disbursing Federal disaster assistance is conferred under 31 U.S.C. § 7701(c)(1) and Executive Order 9397, as amended by Executive Order 13478.
- 5 C.F.R. § 430.102. The DHS regulations on Performance Management require the Agency to create a systematic process by which an agency involves its employees, as individuals and members of a group, in improving organizational effectiveness in the accomplishment of agency mission and goals. C3MP functions to implement personnel management processes.

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

The information in C3MP is covered by the following SORNs:

- DHS/FEMA-008 Disaster Recovery Assistance Files System of Records, which covers the collection of disaster applicant and applicant information.[5]
- DHS/ALL-004 General Information Technology Access Account Records System of Records, which covers the collection of registration information from FEMA employees and contractors requiring access to C3MP.[6]
- OPM/GOVT-1 General Personnel Records System of Records, which allows coverage for personnel records used in the Workforce Management function.[7]
- DHS/FEMA-002 Quality Assurance Recording System, which covers the collection of call recordings and screen shots for the purpose of quality assurance and training.[8]

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

C3MP is currently in development. It is a DHS requirement that the system comply with DHS Management Directive 4300A at a security level of Moderate as defined in Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems. A System Security Plan, maintained to reflect the current state of the system during its overall implementation period, describes how that directive and associated standards will be met. The tentative date for the ATO is March 2017.

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

The C3MP uses the same approved schedules as its predecessors (ACCN and QARS). Records and reports related to and regarding call recordings when an agent was evaluated by FEMA's quality control staff are maintained by FEMA for 3 years and then transferred to the FRC, which will destroy after 6 years (N1-311-08-1, Item 1). Records and reports related to and regarding unevaluated call recordings are maintained for 45 days after the date of recording (N1-311-08-1, Item 2).

[5] DHS/FEMA-008 Disaster Recovery Assistance Files, 78 Fed. Reg. 25,282 (April 30, 2013).
[6] DHS/ALL-004 General Information Technology/Access Account Records System (GITAARS), 77 Fed. Reg. 70,792 (November 27, 2012).
[7] OPM/GOVT-1 General Personnel Records, 77 Fed. Reg. 73,694 (December 11, 2012).
[8] DHS/FEMA-002 Quality Assurance Recording System, 79 Fed. Reg. 35,366 (June 20, 2014).

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 following forms are used by the system:

- OMB No. 1660-0002 includes the FEMA Form 009-0-1, "Application /Registration for Disaster Assistance."
- OMB No. 1660-0128, "Federal Emergency Management Agency Applicant Assistance Program Effectiveness & Recovery Survey"
- OMB No. 1660-0129, "Federal Emergency Management Agency Applicant Assistance Follow-Up Program Effectiveness & Recovery"
- OMB No. 1660-0107, "Public Assistance Customer Satisfaction Survey"
- OMB No. 1660-0036, "Federal Emergency Management Agency (FEMA) Applicant Assistance Customer Satisfaction Surveys"

Section 2.0 Characterization of the Information

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

The following information is collected from FEMA employees and contractors to support the Workforce Management function:

- First and last name;
- Email address;
- Network user ID;
- Customer Interaction Center ID (CIC) ID[9];
- Seniority date; and
- Effective hire date.

The IVR collects the following from disaster applicants for verification for self-help automatic status:

[9] CIC ID is identification provided to employees and contractors used to log into the phones.

- Date of Birth;
- Zip Code;
- Registration ID; and
- Phone number – Call back function only.

The following information from disaster applicants may be included, as provided, on audio and/or screen recordings captured for quality assurance purposes:

- Applicant's name;
- SSN
- Home address;
- Current phone numbers (home, cell, etc.);
- Current mailing address;
- Email address; and
- Personal financial information including the disaster applicant's bank name, bank account information, insurance information, applicant or household income, number of occupants and dependents, and dollar amount of their losses.

FEMA generates the following data from audio recordings and screen captures:

- Contact ID (a unique identification assigned to each recorded contact in C3MP);
- Performance and Quality Results Reports; and
- A "quality result" about the FEMA employee/contractor who conducts the phone transaction/case review involving an applicant or public disaster assistance applicant's file or request for internal assistance.

C3MP receives daily statistical information from the Enterprise Data Warehouse (EDW) and Document Management and Records Tracking System (DMARTS)[10] to display employee or contractor performance data within C3MP.

Data received from DMARTS includes:

- FEMA Agent ID;

[10] For more information, please see DHS/FEMA/PIA-009 Document Management and Records Tracking System (DMARTS), (May 15, 2013) found here: https://www.dhs.gov/sites/default/files/publications/privacy_pia_fema_009a_2013.pdf.

- Action denoted in DMARTS (for example Reprocess, Archive, and Add date, time (hours, minutes, and seconds).
- Date
- Time (hours, minutes, seconds)

EDW (IA Timestamp Report):

- FEMA Agent Name (First & Last);
- Action (e.g. route, cancel, hold);
- Date;
- Process (e.g., applicant inquiry, applicant update);
- Time (hours, minutes, seconds);
- FEMA employee or contractor; and
- User Name.

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

The information sources for C3MP come directly from the IA disaster applicants. Applicant disaster applicants call the FEMA call center and input the necessary information to verify identity when requesting an automated status update. FEMA employees and contractors provide their identifying information while providing customer service to disaster applicants, conducting processing review of a disaster applicant's file, providing support to internal departments, or performing customer satisfaction assessments.

C3MP also receives information from other FEMA IT systems, namely IA, DMARTS, ODS, and EDW.

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

No. C3MP does not use publicly available data or information from commercial sources.

2.4 Discuss how accuracy of the data is ensured.

C3MP assumes the initial accuracy of the information provided by the caller to the IVR. During a typical call transaction, an applicant may verify the accuracy of the data used for

identification purposes by entering the information at the prompts. After several retries, if the data entered does not match data within the database, the applicant will connect to an HSS, who has the ability to verbally verify the data with the applicant. The disaster applicant can also reach an HSS at the end of the self-help option in order to make adjustments to the data. The data is verbally verified by the HSS as it is modified or updated.

The call recordings and screen captures in C3MP provide a snapshot of applicant customer service transactions. They are not retrievable by applicant name. The way information is collected/maintained in C3MP has no impact on a disaster applicant's ability to obtain FEMA assistance. If, during the review of a recorded transaction, an evaluator notices an inconsistency of information about an applicant between a recording and a screen capture, the evaluator reports the inconsistency to FEMA personnel who can update the record in the C3MP.

Periodic system audits ensure employee/contractor data remains current and accurate and provides an opportunity to correct erroneous data.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: A privacy risk associated with this system includes FEMA collecting erroneous information from the IA disaster applicant via C3MP during the authentication process for self-help status update. IA disaster applicants who manually enter their information via the telephone keypad can cause this error.

Mitigation: This privacy risk is mitigated by providing IA disaster applicants with the option of speaking to an HSS. This allows them to verify and update any information during the call. In addition, FEMA automatically routes applicants to an HSS after the applicant makes several incorrect/invalid authentication attempts via the self-help functionality. Lastly, data received in the database from the ODS is refreshed every six hours. The refresh action ensures the most current data is available.

Privacy Risk: A privacy risk associated with this system is that more information is collected from the disaster applicant than is necessary.

Mitigation: C3MP only prompts the applicant to provide the minimal amount of PII necessary to retrieve their file and find a status. In the event that an applicant needs to apply for assistance, C3MP will connect the caller with the appropriate intake personnel but then will disconnect the call. C3MP will not collect that information from callers.

Privacy Risk: A privacy risk associated with this system is that individuals may not know their Registration ID, and therefore may not be able to use the automated system to receive a status update.

Mitigation: FEMA mitigates this risk by offering individuals the opportunity to speak with a live representative. Limited non-PII is provided in the automated status update, and individuals can get the same information, or more, by speaking with an HSS.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The applicant information in the system (name, registration ID, SSN (last 4 digits), and ZIP code) is used to provide automated status updates to applicants via the IVR. Since it is possible that an applicant may have applied for FEMA survivor disaster assistance for multiple Presidentially-declared disasters, the combination of these data elements will ensure that the applicant is receiving the correct information for the specific disaster assistance. The last four digits of the SSN are used as the primary identifier for each applicant. Additional identifiers such as name and registration ID are used to ensure an applicant is uniquely identified. IA disaster applicant data entered via phone (keypad inputs) is matched with the data in the IA database to provide status to the applicants. The IA database receives its data from the ODS.

FEMA uses identifying information provided by employees and contractors in direct contact with disaster applicants, including CIC ID. This identifying information is used to perform assessments of the performance of FEMA's employees and contractors and to improve the quality of responses to disaster assistance applicants. This information, together with audio recordings and screen captures are used by to assess the performance quality of call center employees and contractors including language translation providers and temporary call center agents. The information is also used to assess the quality of services delivered, and to guide training plans and other needed improvements. Supervisors use the employee or contractor identifying information to assist in coaching, mentoring, counseling, and to otherwise enable RSC employees and contractors to better assist disaster assistance applicants.

RSCs may also use employee and contractor identifying information to identify call trend information needed to enhance the level of support provided to disaster applicants.

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.

No. The project does not use technology to conduct electronic searches, queries, or analyses of electronic databases to discover or locate a predictive pattern or anomalous data concerning a disaster assistance applicant.

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

No, there are no other DHS components with assigned roles within the system.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information could be used in a manner inconsistent with the purpose of collection.

Mitigation: FEMA mitigates this risk by implementing the following controls: 1) C3MP does not retain the PII that the applicant inputs via the telephone keypad; 2) FEMA has limited the PII requested from the applicant to only that which is necessary to distinguish with specificity both the applicant and the particular disaster registration for which the status is requested; and 3) all information within audio recordings and screen captures is collected to evaluate employee and contractor performance. Those portions of the screen-only recordings that are reviewed for workforce quality assessment are archived and held for six years to allow time to resolve any personnel matters that may arise from the use of quality assessment data for employee or contractor performance evaluations or to determine qualifications for continued employment. While PII and could be displayed in a screenshot of the casework being performed, the PII is not stored as individual date that can be extracted from the system. FEMA purges recordings that are not used in an evaluation of a FEMA employee or contractor within 45 days. Finally, C3MP does not contain accessible applicant data.

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.

Prior to the IA disaster applicant providing any information, FEMA provides notice about C3MP's collection of information through a recorded, automated Privacy Act Statement provided at the time the applicant's call is connected via C3MP. In addition, IA disaster applicants who need to apply for disaster assistance receive an automated message prior to connecting to a live HSS. Furthermore, in the event an HSS receives a call in which there is more than one applicant on the same call, the HSS will give notice to all subsequent applicants on the same line. Employees and contractors receive notification that their calls may be monitored by C3MP.

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

At the beginning of each call, IA disaster applicants are presented the automated Privacy Act Statement. If not in agreement, the IA disaster applicant may refuse to continue and opt-out of the C3MP system by ending the call. In addition, the applicant may also choose to opt-out at any time after being connected to a FEMA HSS by informing the HSS.

Applicants may opt-out of the recording by choosing to decline to participate in the customer service assessments when they are called back by the RSC personnel.

FEMA employees/contractors working in specific positions subject to recording in C3MP cannot opt-out of audio recording and screen captures as the recording is a requirement of their position.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a privacy risk that applicants may be unaware of the C3MP use for employee and contractor performance management and evaluation.

Mitigation: FEMA manages this risk by providing notice through the DHS/FEMA-002 Quality Assurance Recording System SORN and this PIA. FEMA also provides notice to its employees and contractors upon initial training for their position and through user system guides and resources. In addition, FEMA provides notice of call monitoring and recording via an automated message when IA disaster assistance applicants call FEMA's Recovery Service Centers via the toll-free number. FEMA employees and contractors who call IA and PA applicants read a scripted privacy notice during the introduction of the call after verifying that the individual is the applicant, co-applicant, or official designated to discuss the matter of the call. Lastly, the DisasterAssistance.gov website includes a Privacy Act Statement that will serve notice to disaster assistance applicants applying online that their information may be used for quality assurance purposes.

Section 5.0 Data Retention by the project

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

C3MP uses the same approved schedules as its predecessors (ACCN and QARS). Records and reports related to and regarding call recordings when an agent was evaluated by FEMA's quality control staff are maintained by FEMA for 3 years and then transferred to the FRC, will destroy after 6 years (N1-311-08-1, Item 1). Records and reports related to and regarding

unevaluated call recordings, including screen captures, are maintained for 45 days after the date of recording (N1-311-08-1, Item 2).

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: A privacy risk associated with this system is that the C3MP retains the information in the IVR database longer than is necessary.

Mitigation: FEMA also uses NARA-approved retention schedules to retain and eventually dispose of the data. In addition, FEMA leverages training and documentation, such as standard operating procedures, to inform FEMA users of proper record retention standards.

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 does not routinely share C3MP information with any organization outside of FEMA. In the rare instance that audio recording information is shared outside of DHS, FEMA only shares audio recording information pursuant to the routine uses in the DHS/FEMA-002 Quality Assurance Recording System SORN, and only when compatible with the purposes for collection. FEMA electronically transmits the information in encrypted, password-protected files via secure electronic transmission.

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

As per 6.1 above, FEMA does not routinely share the information in C3MP outside of DHS as part of normal business processes of the agency. Routine uses within the DHS/FEMA-002 Quality Assurance Recording System SORN covers the limited instances in which information in C3MP may be shared outside of DHS. Prior to sharing C3MP, FEMA ensures that the sharing is compatible with the purpose for which the information was collected.

6.3 Does the project place limitations on re-dissemination?

Yes. FEMA shares information only if a routine use outlined in the SORN listed under Section 6.2 above permits disclosure and there is a demonstrated “need to know” the information. FEMA also advises the receiving party that the information is sensitive and should not be shared further.

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

Requests for survivor disaster assistance records within C3MP are made to the DHS/FEMA Disclosure Office, which maintains the accounting of what records were disclosed and to whom.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: A privacy risk associated with this system is that the information in C3MP could be erroneously disclosed or shared with unauthorized recipients.

Mitigation: This privacy risk is mitigated because FEMA only shares the information in C3MP outside of DHS pursuant to the routine uses found in the DHS/FEMA-008 Disaster Recovery Assistance Files System of Records, DHS/FEMA-002 Quality Assurance Recording System SORN,or only pursuant to a written request submitted to the FEMA Disclosure Office.

FEMA also manages this risk through training. System-specific privacy awareness training is required for all C3MP users. Users are trained to ensure that the information in C3MP is only shared or disclosed in a manner consistent with the purpose of the collection of the information and consistent with the applicable SORNs covering the specific information that is to be shared or disclosed.

Section 7.0 Redress

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

An applicant may call and connect directly to a live HSS who can verify and update the applicant's information. This process is not within the scope of the C3MP system; however, the HSS will use the IA system for these updates. IA disaster applicants may also consult the SORNs listed in Section 1.2 for additional information regarding how to access their respective IA disaster application files via a Privacy Act or Freedom of Information Act (FOIA) request.

DHS employees and contractors may seek access to their information by submitting a Privacy Act or Freedom of Information Act (FOIA) request to the Disclosure Officer, DHS/FEMA, Records Management Division, 500 C Street, SW, Washington, DC 20472.

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

C3MP automatically routes applicants to a live HSS if all information that the applicant enters cannot be matched by the IVR database to a record in the IA database. Once connected to an HSS, the applicant information must be verified and FEMA can correct or update the applicant's

information. The HSS will verify the applicant's identity by asking for a combination of: first and last name, last 4 of the social security number, address, phone number and date of birth. These questions are used to verify the information that was given to FEMA during the applicant's initial intake.[11] An applicant's information can only be updated with a live HSS and not through the automated system. IA disaster applicants may also consult the SORNs listed in Section 1.2 for additional information regarding how to access their respective information.

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

Applicants are notified of the procedures for correcting their information through this PIA as well as through the SORNs listed in Section 1.2. An HSS may be reached via the toll-free number to provide notice to applicants regarding correcting their information. In addition, all notification, record access, and record correction procedures for are addressed, outlined, and described the SORNs listed in Section 1.2.

Furthermore, FEMA employees and contractors may request copies of their recordings.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: A privacy risk associated with this system is that IA disaster applicants using C3MP will be unaware of the redress process.

Mitigation: This privacy risk is mitigated because C3MP automatically routes applicants to a live HSS to verify their information if the information they enter does not return a status record from the ODS via the self-help option. In addition, this PIA and the SORNs listed in Section 1.2 provide notification of the redress process.

Privacy Risk: There is a risk that the FEMA employees and contractors do not have adequate redress opportunities to correct, amend, or access their information in C3MP.

Mitigation: FEMA employees and contractors whose information is in C3MP are informed of the appropriate redress mechanisms through the required C3MP user training. For example an employee would notify his or her supervisor if he or she found that C3MP contained any erroneous PII about him or her. In addition, this PIA and the SORNs listed in Section 1.2 provide notification on redress.

[11] This verification process falls outside the scope of C3MP and will be discussed more fully in a forthcoming Individual Assistance PIA.

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?

Access to the system is role-based; therefore, FEMA users have access only to the portion of the data required to perform their official duties. FEMA ensures that the practices stated in this PIA are followed by leveraging training, policies, rules of behavior, and auditing and accountability.

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

All FEMA employees and contractors are required to complete initial and annual privacy awareness training. Authorized users of C3MP are also trained according to their access rights. All users are required to meet the system-specific privacy awareness training that is administered in a designated training environment.

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

In instances in which the personal information of applicants stored in C3MP is viewable, it may only be viewed by authorized personnel with the appropriate user roles and training and a relevant "need to know." Authorized personnel are determined by supervisor appointment. This process ensures that privacy and information safeguarding requirements are met by limiting access to sensitive information to only those users whose operational role and mission warrants such access. The information within the system is further protected by the use of identification and authentication controls, access control lists, and physical access controls to the IA disaster application. Also, there are standard operating procedures (SOP) for reference and an information system security officer (ISSO) who provides security guidance over the project. Contractors working for FEMA must undergo the suitable clearance process prior to being authorized access to FEMA IT systems.

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?

Currently, the C3MP does not require information sharing agreements or MOUs, however, the project has a process to review such agreements as necessary. This process involves program stakeholders, information system security officers, the Office of Chief Counsel, and the FEMA

Privacy Officer. Similarly, C3MP will leverage its stakeholders in the process of reviewing and approving any new uses for the project. If new uses are contemplated for the C3MP platform or its information, FEMA will update the required privacy compliance documentation.

Responsible Officials

William H. Holzerland
Senior Director for Information Management
Department of Homeland Security

Approval Signature

_____

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

Appendix A

Privacy Notice Delivered Via Phone:

We are required to provide you with the following Privacy Act Statement. The Privacy Act of 1974 protects your rights as to how FEMA uses and shares your information. The Stafford Act and other authorities allow FEMA to collect this information to determine eligibility and administer financial assistance as a result of an emergency or Presidentially-declared disaster. FEMA may share your information outside of FEMA with entities such as with states, tribes, local governments, voluntary organizations, and other organizations in accordance with published routine uses. FEMA shares this information to enable you to receive additional disaster assistance and as necessary to prevent a duplication of benefits and to prevent future disaster losses. FEMA may record phone calls for internal quality assurance purposes. Furnishing your SSN and other requested information is voluntary; however, failure to produce may delay or prevent you from receiving assistance. If you knowingly make false statements to obtain disaster aid, it is a violation of federal and state laws. To apply for disaster assistance, you will need the following: pen and paper; the date your disaster damages occurred; your Social Security number; address and phone numbers where you can be reached; your family's gross income; and your insurance information. The interviewed will take 20 to 30 minutes and is authorized by the Office of Management and Budget under Control Number 1660-0002. Please hold for the next available agent. This call may be monitored and recorded for quality assurance purposes.