Privacy Impact Assessment
for the

Deployment Tracking System
Beta Test

DHS/FEMA/PIA-040

March 20, 2015

Contact Point
Allyson Koncke-Fernandez
Incident Workforce Management Division
Response Directorate
Office of Response and Recovery
(202) 735-7159

Reviewing Official
Karen L. Neuman
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), Response Directorate, Incident Workforce Management Division (IWMD) coordinates deployment programs under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act). The IWMD Deployment Branch operates the FEMA Deployment Tracking System (DTS) to assign and track the deployment of disaster response and recovery personnel. FEMA is conducting this Privacy Impact Assessment (PIA) because FEMA collects uses, maintains, retrieves and disseminates personally identifiable information (PII) through DTS to coordinate and manage emergency and disaster deployments of personnel.

Overview

Upon a Presidentially-declared emergency or disaster under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act),[1] FEMA may deploy emergency and disaster response and recovery personnel to provide aid and assistance. Disaster response and recovery personnel may include permanent and temporary full-time FEMA employees, reservists, Cadre of On-call Response and Recovery Employees (CORE), FEMA Corps volunteers, and DHS Surge Capacity Force members. Under FEMA's "Every Employee is an Emergency Manager" initiative, FEMA trains, qualifies, and assigns regular and recurring emergency management duties to all full-time (permanent, temporary, and CORE) and reservist employees. CORE employees are appointed for two to four years to perform disaster preparedness, response, recovery, and mitigation-related activities under the Stafford Act. FEMA Corps is a partnership between FEMA and the Corporation for National and Community Service (CNCS) that enhances FEMA's disaster response and recovery personnel with trained 18-24 year olds devoted solely to FEMA emergency and disaster response and recovery efforts. The DHS Surge Capacity Force members are non-FEMA DHS employees who volunteer to supplement FEMA's emergency and disaster response and recovery personnel.

The IWMD Deployment Branch operates the FEMA Deployment Tracking System (DTS) to assign and track the deployment of disaster response and recovery personnel. The Automated Deployment Database (ADD) previously served as FEMA's emergency and disaster personnel deployment coordination and management system,[2] and the Availability Reporting System (ARS) collected and maintained personnel deployment availability status. DTS enables FEMA to effectively manage emergency and disaster personnel deployments simultaneously via a web-based user interface. DTS also facilitates disaster responder accountability through a

[1] Pub. L. No. 93-288, and codified at 42 U.S.C. §§ 5144, 5149, 5170 and 5197.
[2] *See* the DHS/FEMA/032 - Deployment Programs PIA *available at* https://edit.dhs.gov/sites/default/files/publications/privacy-pia-fema-deployment-programs-20130816.pdf.

number of dashboards, reports, search and mapping utilities, and automatic status notifications functions.

DTS Beta Test

In May 2014, the IWMD Deployment Branch launched a Beta Test for DTS to test the software for "real-world" scenarios and preview the final release of the more comprehensive version of DTS. The forthcoming PIA for the operational phase of DTS will discuss an analysis of the Beta Test and evaluation. The DTS Beta test identifies, maintains, and archives a FEMA employee's deployment status, job positions, proficiencies, skills, language, and deployment history. The DTS Beta test also stores position qualifications to enhance deployment decisions (e.g., matching personnel who have specific language skills to an area in which such language proficiency is required).

The DTS Beta test consists of two user interfaces; the "Deployer" and the "Responder Portal." Users assigned to the "Deployer" interface create, issue, and process deployment orders and manage supporting data (i.e., personnel, qualifications, events, duty stations, and emergency contact information). The Deployers communicate regularly with FEMA's deployed workforce, prompting them to check-in with daily deployment status and location in order to maintain workforce accountability. The Responder Portal is used by all field-deployable FEMA employees. Deployable personnel review and accept deployment orders through the Responder Portal, which also manages responders' availability, contact preferences, and contact details.

Initial Data Entry and Employment Verification

DTS receives a small subset of specified historical employee PII, from the ADD System (FEMA's previous deployment system) to initiate the DTS Beta test. This upload includes the employee's first name, last name, middle initial, email address, phone numbers (home, work, and cell), home address, emergency contact information (name, relationship, and phone number), hire date, skills and proficiency levels, employee type (i.e., permanent and temporary full-time employee, CORE, or reservist), job type (FEMA component or office), region, organization information, supervisor, position type or official position title, program area, pay type, grade, step, and series. FEMA needs to collect this specific salary information to properly determine the cost of deploying personnel.

This upload does not include any Social Security Numbers (SSNs), as DTS does not store SSNs for FEMA personnel;[3] instead, DTS assigns a personnel identification number (PID) to each FEMA employee. This allows FEMA to track and monitor new assignments and to associate all user actions (i.e., availability, deployment history, deployment status,

[3] Prior to the upload into DTS, an IWMD Deployment Branch Reports Specialist exports a database file from ADD comprised of the data elements described above. Although the initial ADD export includes the SSN, the Specialist encrypts the SSN and makes it unrecoverable by applying a shift cipher and hashing it with an SHA 512 hash. Simultaneously, the Specialist creates a DTS Identification Code. FEMA neither transmits the SSN nor stores it in DTS.

acknowledgement of deployment notification, actions taken on a deployment, and daily accountability for accepted deployment requests) with specific personnel. DTS maintains an auditable log of all uploads and the resulting record creations or inactivation, according to the National Archives and Records Administration (NARA)-approved retention schedule, which is in progress with the FEMA Records Management Division (RMD).

Deployment Orders

Under FEMA's "Every Employee is an Emergency Manager" initiative, every new FEMA employee must accept the terms of employment, including requirements for participation in deployment programs. An employee's refusal to deploy without authorization from his or her leadership may be cause for disciplinary action. When FEMA leadership determines that a particular disaster or emergency event requires additional staff support, the IWMD Deployment Branch and regional staffing points of contact (SPOCs) create a deployment order in the DTS Beta test to request the deployment of available FEMA response personnel. These deployment orders may call for specific positions, specialized teams, pre-configured "force packages" to meet certain "force structures,"[4] or individual resources via a Name Deployment Order. FEMA employee responders receive official deployment request notifications on their choice of government email, personal email, text message, or automated voice recording. Employees sign on to the Responder Portal to receive the details after they get a deployment request. FEMA employee responders are required to update their availability status and accept, delay, or decline deployment requests via the Responder Portal, where they can also update their contact preferences and details. The FEMA employee responders use the Responder Portal to check-in, change lodging or duty station, provide daily accountability, check-out, and demobilize once deployed.[5]

Risks and Mitigations

The primary risk associated with DTS is that manual data entry results in the storage of erroneous data in DTS. To mitigate this risk, FEMA goes directly to the source at the US Department of Agriculture (USDA)/National Finance Center (NFC), rather than DHS Office of the Chief Human Capital Officer, because FEMA handles payroll directly through the NFC. FEMA uses a regular biweekly USDA NFC Database upload. In addition, the IWMD Deployment Branch regularly reviews records for accuracy. Following the NFC Database

[4] Deployment orders known as "force packages" specify the need for individual positions or teams with the capability of meeting certain "force structures." These individuals or teams must have reached certain proficiencies and must be trained and prepared to fill a specified position and respond to particular types and levels of incidents.
[5] Note that the requirements for FEMA reservists are slightly different. Up to 60 days of pre-approved leave is permitted per year for FEMA reservists. When a reservist is on leave he or she is not listed as "available" in DTS, which makes the individual unavailable for deployment rotations. A reservist who is listed as "available" is required to be deployable within 24 hours. If a reservist declines a deployment request while "available," the action is documented in the employee's personnel file. If a reservist declines three deployment requests within a year his or her employment may be terminated. FEMA reservists have the same requirement as a full-time employee of consenting to these terms of employment when they accept a position with FEMA.

upload, if the IWMD Deployment Branch finds a discrepancy regarding PII, the Deployment Branch verifies the information with the respective individual to ensure accuracy. In addition, in the event of an employee non-match, Deployment Branch staff may choose to either confirm that the employee is valid and add that record to DTS, or if warranted, the staffer may choose to deactivate the DTS personnel record.

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?

FEMA collects, uses, maintains, retrieves and disseminates PII of disaster response and recovery personnel pursuant to its authorities and obligations under Sections 503, 504, and 507 of the Homeland Security Act of 2002,[6] Sections 303, 306, 403, 502, and 621 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act),[7] *as amended*, and the Post-Katrina Emergency Management Reform Act (PKEMRA).[8] FEMA collects Social Security numbers (SSN) from FEMA employees and other personnel pursuant to Executive Orders on the Numbering System for Federal Accounts Relating to Individual Persons[9] and Federal Agency Use of Social Security Numbers.[10]

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

The information associated with FEMA's deployment programs is covered by the following SORNs:

- DHS/ALL-004 Department of Homeland Security General Information Technology Access Account Records System (GITAARS) System of Records[11] allows FEMA to collect and maintain account information, including PII, for the purpose of providing authorized individuals with access to DHS IT systems;
- DHS/ALL-014 Department of Homeland Security Emergency Personnel Location System of Records[12] covers the information needed to contact DHS personnel to respond to all hazards emergencies or to participate in exercises;

[6] 6 U.S.C. §§ 313, 314, 317, 320 and 711.
[7] Pub. L. No. 93-288, and codified at 42 U.S.C. §§ 5144, 5149, 5170b, 5192 and 5197.
[8] Pub. L. No. 109-295.
[9] Exec. Order No. 9397, "Numbering System For Federal Accounts Relating to Individual Persons."
[10] Exec. Order No. 13478, "Amendments to Executive Order 9397 Relating To Federal Agency Use of Social Security Numbers."
[11] DHS/ALL-004 Department of Homeland Security General Information Technology Access Account Records System (GITAARS) System of Records, 77 FR 70792 (November 27, 2014), *available at* http://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm.
[12] DHS/ALL-014 Department of Homeland Security Emergency Personnel Location System of Records, 73 FR 61888 (October 17, 2008), *available at*, http://www.gpo.gov/fdsys/pkg/FR-2008-10-17/html/E8-24807.htm.

- DHS/ALL-019 Department of Homeland Security Payroll, Personnel, and Time and Attendance Records[13] allows FEMA to ensure proper payment of salary and benefits to DHS personnel and to track time worked for reporting and compliance purposes; and
- OPM/GOVT-001 General Personnel Records System of Records[14] allows FEMA to collect pertinent workforce information on FEMA employees for use in national or homeland security emergency/disaster response.

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

The FEMA Office of the Chief Information Officer approved a system security plan and a one-year Authority to Operate on September 29, 2014.

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

FEMA's RMD is collaborating with partner agencies and NARA to establish an approved retention and disposal schedule for its deployment qualification records and deployment records that is consistent with the above referenced SORNs and the mission-driven needs of the agency. In the meantime, DTS retains the data. All retained data will be disposed of (including retroactive disposal of some information) once NARA approves this retention and disposal schedule.

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 PRA is not applicable to the DTS Best test because the DTS Beta test only collects and uses information about existing FEMA employees. The PRA package for DTS collection forms relating to the subsequent broader DTS rollout is in the approval process.

Section 2.0 Characterization of the Information

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

Data from Existing FEMA Employees Included in Initial Upload from ADD into DTS:

- Full Name (first, middle initial, and last);
- SSN securely stored as an unrecoverable salted hash;[15]

[13] DHS/ALL-019 Department of Homeland Security Payroll, Personnel, and Time and Attendance Records, 73 FR 63172 (October 23, 2008), *available at* http://www.gpo.gov/fdsys/pkg/FR-2008-10-23/html/E8-24993.htm.
[14] OPM/GOVT-001 General Personnel Records System of Records, 77 FR 73694 (December 11, 2012), *available at*, http://www.gpo.gov/fdsys/pkg/FR-2012-12-11/html/2012-29777.htm.

- Primary Home Address;
- Primary Email Address;
- Primary Telephone Numbers (home, work, and cell);
- Hire Date;
- Employee Type (i.e., permanent and temporary full-time employee, CORE, or reservist);
- Region;
- Supervisor;
- Organization;
- Skills;
- Languages spoken;
- Job Type (FEMA component or office);
- Program Area (i.e., Public Assistance or Individual Assistance);
- Position Type (Official Position Title, i.e., Public Assistance Project Specialist or Private Sector Specialist);
- Proficiency Level (i.e., Trainee, Qualified, or Coach/Evaluator);
- Pay Type;
- Grade;
- Step;
- Series;
- Government Credit Card Holder (Y/N); and
- Emergency Contact Information (name, relationship, and phone number).

DTS Generated Information

- Personal Identification Number (PID).[16]

Data Entered into a Deployment Order by IWMD or Regional SPOCs:

- Event;
- Employee Type, Job Type, and Program Area Requested;
- Job Title, Skills, Language, Minimum Proficiency, and Number Requested;
- Duty Station Name, Type, and Location (if applicable);

[15] A Reports Specialist from IWMD's Deployment Branch conducts an ADD export comprised of the data elements described above prior to the upload into DTS. In addition, the Reports Specialist creates a DTS Identification Code by applying a shift cipher to the SSN to encrypt the product, then hashes the encryption using an SHA 512 hash even though the initial ADD export includes the SSN. FEMA does not store the SSN, which is unrecoverable in DTS.

[16] The PID allows FEMA to track and monitor new assignments and to associate all user actions (i.e., availability, deployment history, deployment status, acknowledgement of deployment notification, actions taken on a deployment, and daily accountability for accepted deployment requests) with specific personnel.

- Targeted Arrival Date;
- Latest Possible Deployment Arrival Date;
- Expected Duration;
- Concur Travel Authorization Code;
- Rental Vehicle Allowed (Y/N);
- POC Name, Phone Number, and Position;
- Force Package (contains position and proficiency);
- Designated Team Name;
- Specified Name(s) Requested (for Name Deployment Order Only);
- Name of Cadre Manager Requesting Specific Employee(s);
- SPOC Name;
- Per Diem Authorized (Y/N);
- Proximity to Incident Required (Y/N); and
- Number of Miles Proximity (if Yes to Proximity Requirement).

Data Entered by FEMA Employee Responders on the Responder Portal:

- Email Addresses;
- Phone Numbers (home, work, and cell);
- Emergency Contact Information (name, relationship, and phone number);
- Dates of Availability;
- Accept, Delay or Decline Deployment Requests;
- Reason for Declining Deployment Request
- Check-In Date;
- Request Leave (for FEMA Reservists only in order to indicate dates and leave types, i.e., military or pre-approved non-availability);
- Check-Out Date and Reason for Check-Out;
- Demobilization Date;
- Deployed Information (lodging, lodging phone, and phone while deployed); and
- Rental Car Information (rental agency, make, model, and license plate number).

Biweekly Export from USDA NFC:

- Full Name (first, middle initial, and last);
- Home Address;
- Supervisor Code (indicates whether or not the individual is a supervisor);
- FEMA_HR_ID. (NFC personal identifier);
- Current Employment Status (active or inactive);
- FEMA and NFC Organization Codes;
- Employee Type;

- Position Title;
- Pay Type, Grade, Step, Series;
- Hire Date; and
- DTS Identification Code, which is used to match existing records during subsequent NFC uploads (Identification Code is determined by encrypting and hashing the SSN; SSN becomes unrecoverable).

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

FEMA collects the deployment program information stored in the DTS Beta through an initial upload of historical data from ADD, data extracts from the USDA/NFC Database, and employee personal information and availability updates through the Responder Portal. The sources of information for FEMA's deployment programs and DTS include: 1) FEMA employees who are participating in FEMA's deployment programs; 2) ADD (historical data); 3) USDA/NFC Database; and 4) DTS itself, which creates a PID for each individual in the system.

FEMA may collect information directly from the individual through the Responder Portal; or in the case of the NFC Database, FEMA may collect information via an extract from a supporting IT system.

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.

2.4 Discuss how accuracy of the data is ensured.

FEMA ensures the accuracy of the data it collects by obtaining the information directly from individual deployment program participants when possible. Most information stored in DTS is not collected directly from individual deployment program participants. FEMA relies on the official employee information maintained by the Office of Personnel Management (OPM) and USDA/NFC to ensure accuracy of payroll and personnel data in DTS. OPM and USDA/NFC are the systems of record and data stewards for all government personnel data.

In addition, the IWMD Deployment Branch employs a number of safeguards to ensure the accuracy of the employee data. DTS imports the organizational abstracts and employee files from the NFC Database via a manual upload of a redacted file in order to reconcile the USDA/NFC Database records with DTS employee records. The Deployment Branch verifies the information with the respective individuals or POCs if the NFC Database import results in two names corresponding with the same hashed SSN or the same name corresponding with two different hashed SSNs. The data extracts from the USDA/NFC Database assist FEMA in

ensuring the accuracy of its information. In addition, FEMA program managers are responsible for reviewing the records of employee responders and may contact the Deployment Branch to correct discrepancies. The Deployment Branch also monitors the database records daily provides reports to management, and forwards concerns or suspected inaccuracies to the Deployment Branch or the employee's manager.

Finally, all FEMA employee responders included in the DTS Beta may verify their information through the Responder Portal. The Responder Portal provides FEMA employee responders with the ability to access their information, including employment, skills and deployment details as well as update their availability, personal contact information, and emergency contact information. To update other PII fields within the DTS Beta, an employee must contact IWMD Deployment Branch personnel, who manually enter authorized changes or correct employment information.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that FEMA collects more information than is necessary to accomplish the employee deployment tracking purpose.

Mitigation: FEMA mitigates this risk by collecting only that information which is necessary to fulfill the purpose of deployment tracking and accountability for emergency response and recovery personnel. This mission includes tracking deployments and maintains information regarding training, eligibility, and performance to provide an overall picture of the deployment readiness of the FEMA workforce.

To mitigate the risk of over collection and to promote data quality and integrity, DTS Beta Test imports information directly from the USDA/NFC, as the data steward for pay and personnel data for FEMA. The USDA/NFC import is the most accurate and timely source for personnel and employment information verification. The USDA/NFC import prevents the need for FEMA to collect unnecessary data from other sources.

Privacy Risk: There is a risk that FEMA collects erroneous or inaccurate information on FEMA employees.

Mitigation: FEMA manages this risk by requiring regular reviews of the data for accuracy by the IWMD Deployment Branch. Additionally, the regular USDA/NFC Database import verifies the employee's information. Employees of the Deployment Branch monitor the database records daily and forward any noted discrepancies to the Deployment Branch or the employee's manager for immediate verification with the respective individual, in order to ensure accuracy following each import. Additionally, FEMA program managers verify the names of the team members upon deployment to ensure accuracy. Finally, all FEMA employee responders included in the DTS Beta can verify their information through the Responder Portal at any time.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

FEMA uses the information in the DTS Beta to determine deployment assignments. The following personnel support the DTS application and system users in the operational environment: FEMA employee responders, ORR's IWMD Deployment Branch staff members, Regional SPOC, FEMA HQ staff, cadre managers, database administrators, system administrators, and the DTS Information Systems Security Officer (ISSO). FEMA assigns all user roles and associated privileges commensurate with their job descriptions. IWMD's Deployment Branch houses the primary users responsible for maintaining the DTS Beta.

FEMA qualifies its employees who hold FEMA Qualification System (FQS) disaster titles under its Deployment Qualifications Program. These employees include permanent and temporary full-time employees, COREs, and reservists. The DTS Beta holds incident workforce members' position qualification records, attained specialties, and training information in order to qualify these individuals.

The DTS Beta collects and maintains pertinent information, such as the full name, email address, home address, phone numbers, emergency contact information, hire date, employee type and organization information, skills, proficiencies, pay type, grade, step, and series. DTS assigns a PID to each employee record, which allows the system to avoid storing SSNs or other sensitive PII. FEMA initially collects the SSN but then protects the information by storing it as an unrecoverable salted hash. The DTS Beta also protects privacy by using role-based access and by granting an employee access to the system only if his or her program leadership approves an access request on a "need to know" basis. DTS prevents the inappropriate use of the information collected by granting access to information that is pertinent to the respective user's role. During and following the Beta test, when FEMA terminates its employees or restricts them from involvement in deployment programs for reasons other than termination, the NFC export upload updates the individual's record in DTS, and the approved Program Official notifies the IWMD Deployment Branch to update the employee information in the system. The Deployment Branch is currently working with FEMA RMD and NARA to finalize a suitable approved retention schedule for DTS prior to implementation of the full DTS System.

The DTS Beta shares statistical information with FEMA's WebEOC Crisis Management System (CMS), for situational awareness purposes only. WebEOC CMS, a web-enabled, invitation-only crisis information management system, provides secure real-time situational awareness and information sharing to help emergency managers promptly make sound, informed decisions. A browser within WebEOC pulls the information for use during a specific browser session when FEMA leadership requests specified data. WebEOC does not retrieve any PII from DTS and does not store or integrate DTS data.

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.

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

No.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that FEMA uses the information in DTS for purposes other than that for which it was originally collected.

Mitigation: FEMA manages this risk by limiting the collection and use of information to that which is necessary to contact individuals, manage and coordinate their deployments, and monitor their location and work activities. In addition, FEMA limits access to the information and the DTS Beta to those individuals with a "need to know" the information for performance of their official duties. FEMA also limits the sharing of the information within DTS to "read only" access by the IWMD Deployment Branch and limits the sharing to the occasions in which FEMA Regional Office personnel or FEMA HC personnel at JFOs may run DTS reports. Only FEMA personnel who are authenticated and granted a password by the IWMD Deployment Branch or DTS's ISSO may edit information in DTS.

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.

The DTS Beta provides the requisite notice of FEMA's information collection to facilitate its deployment programs through many different media. FEMA provides notice through a Privacy Notice to FEMA employees prior to granting access to the system (Appendix A). In addition, this PIA and DHS/ALL-014 Department of Homeland Security Emergency Personnel Location System of Records provide notice to disaster response and recovery personnel regarding FEMA's collection of information. Lastly, DHS/ALL-004 Department of Homeland Security General Information Technology Access Account Records System of Records provides notice of FEMA's collection of information to grant DTS access to FEMA employees.

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

Under FEMA's "Every Employee is an Emergency Manager" initiative every new FEMA employee accepts the terms of employment, which include requirements for participation in deployment programs once he or she accepts a FEMA position. Failure to provide their information may directly impact their qualifications for employment. As such, FEMA employees cannot opt-out of DTS but are aware of these requirements when they accept an offer of employment from FEMA.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not receive notice that FEMA is collecting, maintaining, and using their information for the purpose of deployment coordination and accountability.

Mitigation: FEMA mitigates this privacy risk by providing notice of its collection of information through a Privacy Notice prior to accessing DTS (see Appendix A). In addition, this PIA and DHS/ALL-014 Department of Homeland Security Emergency Personnel Location System of Records provide notice of FEMA's collection of information for deployment. The DHS/ALL-004 Department of Homeland Security General Information Technology Access Account Records System of Records provides notice of FEMA's collection of information to grant DTS access to FEMA employees.

Section 5.0 Data Retention by the project

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

FEMA RMD is collaborating with NARA to establish an approved retention and disposal schedule for its deployment programs that is consistent with the above referenced SORNs and FEMA's mission. All retained data will be disposed of (including retroactive disposal of some information) once NARA approves this retention and disposal schedule, all data will be retained and disposed of, including some data retroactively, in accordance with the NARA-approved schedule

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that DTS retains information longer than necessary and relevant.

Mitigation: FEMA mitigates this privacy risk by establishing a NARA-approved retention and disposal schedule for the DTS Beta and subsequently, the broader DTS version, in order to minimize the time the Agency keeps data in line with the mission of its deployment programs. In addition, FEMA leverages training and documentation, such as the FEMA Privacy

Directive, the FEMA Privacy Program Manual, and standard operation procedures (SOP), 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 shares information collected and entered into the DTS Beta test with USDA/NFC in order to verify information regarding FEMA employees. FEMA only shares the information within the DTS Beta outside of FEMA in accordance with the routine uses published in DHS/ALL-019 Department of Homeland Security Payroll, Personnel, and Time and Attendance Records. Responsible program and project managers review all Memorandum of Understanding (MOU) and Information Sharing Access Agreements (ISAA) between FEMA and its partners. The agreements are also reviewed by FEMA Privacy Officers, the FEMA Chief Information Security Officer (CISO), FEMA Chief Counsel, and FEMA Operations Center (FOC) Director, and then FEMA forwards the documents to DHS for formal review and approval. FEMA shares information related to DTS access in accordance with the routine uses in the DHS/ALL-004 Department of Homeland Security General Information Technology Access Account Records System of Records.

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

FEMA shares deployment-related information in the DTS Beta for a limited purpose in accordance with the Privacy Act and the routine uses prescribed in DHS/ALL-019 Department of Homeland Security Payroll, Personnel, and Time and Attendance Records. DHS/ALL-019 Department of Homeland Security Payroll, Personnel, and Time and Attendance Records allows FEMA to ensure proper payment of salary and benefits to DHS personnel and to track time worked for reporting and compliance purposes.

FEMA only shares DTS Beta test data with USDA/NFC to verify personnel information about FEMA employees to ensure that FEMA is able to base deployment decisions on accurate information about the status of its workforce. This information sharing is consistent with Routine Use (L), "to the other Federal agencies who provide payroll personnel processing services under a cross-servicing agreement for purposes relating to the conversion of DHS employee payroll and personnel processing services; the issuance of paychecks to employees and distribution of wages; and the distribution of allotments and deductions to financial and other institutions, some through electronic funds transfer."

6.3 Does the project place limitations on re-dissemination?

Yes, FEMA shares information only pursuant to routine uses outlined in the SORNs listed under Section 6.2 above or through an approved MOU or ISAA, such as the sharing described in Section 6.1. In addition, FEMA re-disseminates information only in accordance with the Privacy Act.

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

As identified in the SORNs listed under Section 6.2 above, requests for records from the DTS Beta should be made to the Response Directorate or the FEMA Disclosure Office Branch Chief, who maintain an account of what records are disclosed and to whom.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a privacy risk associated with the system that information in DTS Beta could be shared outside of the Department for a purpose that is inconsistent with the original collection of data.

Mitigation: For the DTS Beta test, FEMA only shares DTS Beta test data with USDA/NFC to verify personnel information about FEMA employees to ensure that FEMA is able to base deployment decisions on accurate information about the status of its workforce. This information sharing is consistent with Routine Use (L), "to the other Federal agencies who provide payroll personnel processing services under a cross-servicing agreement for purposes relating to the conversion of DHS employee payroll and personnel processing services; the issuance of paychecks to employees and distribution of wages; and the distribution of allotments and deductions to financial and other institutions, some through electronic funds transfer."

FEMA further restricts the sharing by requiring a "need to know" for the specific data. Information may be shared with other federal, state, or local government agencies as well as with non-profit organizations with mission-specific ties to FEMA and may be shared only through encrypted, password-protected, flat files, or automated transfers. FEMA also mitigates this privacy risk by requiring orientation and training of all individuals with access to the DTS Beta to ensure the proper use and handling of data.

Section 7.0 Redress

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

The information within the Beta version of DTS is part of the DHS/ALL-014 Department of Homeland Security Emergency Personnel Location System of Records. Individuals may access their information via a Privacy Act or Freedom of Information Act (FOIA) request to the

DHS HQ Chief FOIA Officer or FEMA Disclosure Office Branch Chief. Additionally, within the DTS Beta, the IWMD Deployment Branch may access the information regarding FEMA employees. All FEMA employee responders participating in the Beta test may use the Responder Portal to access a limited amount of their individual information. Information related to access to the DTS IT system is part of the DHS/ALL-004 Department of Homeland Security General Information Technology Access Account Records System of Records., Individuals may access their information via a Privacy Act or FOIA request to the DHS HQ Chief FOIA Officer or FEMA Disclosure Office Branch Chief.

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

The information within the Beta version of DTS is part of the DHS/ALL-014 Department of Homeland Security Emergency Personnel Location System of Records. Individuals may access their information via a Privacy Act or FOIA request to the DHS HQ Chief FOIA Officer or the FEMA Disclosure Office Branch Chief. Additionally, all FEMA employee responders included in the DTS Beta can access their individual information through the Responder Portal. Information related to access to the DTS IT system are part of the DHS/ALL-004 Department of Homeland Security General Information Technology Access Account Records System of Records. Individuals may access their information via a Privacy Act or FOIA request to the FEMA Disclosure Office Branch Chief.

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

This PIA (along with the aforementioned SORNs in Section 1.2) informs employees how to correct their information in the Beta version of DTS. In addition, FEMA provides notice of redress in DTS directly to FEMA employees during their initial disaster responder orientation as well as subsequent training courses. FEMA explains the redress process to employees' supervisors and program managers either via email, verbally, or by telephone.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals whose information appears in the Beta version of DTS will seek redress from FEMA for inaccurate data maintained by USDA/NFC.

Mitigation: FEMA mitigates this risk by providing notice of redress in DTS directly to FEMA employee responders, their POCs, team leaders, and program managers during their initial training and during subsequent training courses, as noted above in Section 7.3. FEMA describes the redress process to supervisors and program managers, either via email, verbally, or telephone. These POCs and team leaders, in turn, describe the redress process to their respective participants. In addition, when accessing the Responder Portal, FEMA notifies its employee

responders that they can update their information in the DTS Beta directly. FEMA responders are instructed to contact his or her supervisor on the record or cadre manager when errors occur within the responder's profile that cannot be updated directly in DTS. The manager will work with IWMD to correct the USDA/NFC information if necessary. Furthermore, DTS Beta provides users with a privacy notice, which includes redress information, prior to entry into the DTS system. Finally, this PIA, the DTS User Manual, and the DHS/ALL-014 Department of Homeland Security Emergency Personnel Location System of Records offer notice of redress.

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?

The IWMD Deployment Branch ensures that FEMA follows the practices stated in this PIA by complying with internal FEMA policies, including the FEMA Privacy Program Directive, the FEMA Privacy Program Manual, standard SOPs, orientation and 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.

FEMA requires all users of the DTS Beta version to successfully meet annual privacy awareness and information security orientation and training requirements according the FEMA training guidelines, as well as program-specific DTS system training. Moreover, the IWMD Deployment Branch trains DTS Beta users on the system and how to safeguard PII.

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 establishes SOPs and guidelines about how to use the Beta version of DTS. Designated IWMD Deployment Branch personnel determine which FEMA employees need access to DTS. Once IWMD confirms a new user's need for access with the appropriate HQ or regional manager, personnel administrators manually enter the user's information into the DTS Beta and assign all users within DTS a series of roles that govern their ability to access and interact with various portions of the system. IWMD assigns most roles to users via the personnel page. Upon approval as a DTS user, FEMA grants role-based access limiting the individual to only DTS information pertinent to his or her particular role or function.

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?

FEMA maintains an MOU and ISAA with the USDA/NFC to verify information relating to FEMA employees for the DTS Beta and subsequent operational phases. The FEMA Privacy Officer, FEMA CISO, the DTS program manager, FEMA Chief Counsel and FOC Director review all FEMA MOUs and ISAAs. FEMA then forwards the agreement to DHS for formal review and approval.

Responsible Officials

Eric M. Leckey
Privacy Officer
Federal Emergency Management Agency
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

Appendix A: Deployment Tracking System IT System Privacy Notice

FEMA collects your information to grant you access to the Deployment Tracking System (DTS) for the purposes of disaster deployment tracking and accountability, pursuant to 44 U.S.C. §§ 3101 and 3534. FEMA may disclose your information as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974, as amended. This includes sharing your information as necessary and authorized by the routine uses published in DHS/ALL-004 General Information Technology Access Account Records System of Records, 77 FR 70792 (November 27, 2012), and upon written request, by agreement or as required by law. Disclosing your information on this form is voluntary. However, not providing the requested information could delay or prevent FEMA from granting you access to DTS.