Privacy Impact Assessment
for the

Deployment Tracking System (DTS)

DHS/FEMA/PIA-040(a)

July 19, 2017

Contact Point
Justin Shoemate
Section Chief, Systems Integration and Reports
Deployment and Analysis Branch
Workforce Management Division
Federal Emergency Management Agency
(202) 412-5042

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), Field Operations Directorate, Workforce Management Division (WMD) coordinates personnel deployment programs under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act).[1] The WMD Deployment and Analysis Branch operates the 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) in DTS to coordinate and manage the deployment of federal emergency response and recovery personnel to federally-declared emergencies and disasters. This PIA updates and supersedes the previously published Deployment Tracking System Beta Test PIA.[2]

Overview

The WMD Deployment and Analysis Branch operates DTS to assign and track the deployment of disaster response and recovery personnel. DTS supercedes the Automated Deployment Database (ADD) and the Availability Reporting System, which were FEMA's previous emergency and disaster personnel deployment coordination and management systems.[3] DTS enables FEMA to centrally and effectively manage emergency and disaster personnel deployments via a web-based user interface. DTS also facilitates disaster responder accountability through a number of dashboards, reports, search and mapping utilities, and automatic status notification functions.

When the President declares an emergency or disaster under the Stafford Act,[4] FEMA may deploy emergency, disaster response, and recovery personnel to provide aid and assistance. Disaster response and recovery personnel may include permanent and temporary full-time FEMA employees, FEMA reservists, FEMA Cadre of On-call Response and Recovery Employees (CORE) (collectively "FEMA Personnel"), in addition to FEMA Corps Members, DHS Surge Capacity Force (SCF) members, state and local first responders, and employees of other federal agencies ("Non-FEMA Personnel").

Under FEMA's "Every Employee is an Emergency Manager" initiative,[5] FEMA trains, qualifies, and assigns regular and recurring emergency management duties to all full-time

[1] 42 U.S.C. § 5121.
[2] DHS/FEMA/PIA-040 Deployment Tracking System Beta Test (March 20, 2015), *available at* https://www.dhs.gov/compliance.
[3] DHS/FEMA/PIA-032 Deployment Programs (August 16, 2013), *available at* https://www.dhs.gov/compliance.
[4] 42 U.S.C. §§ 5144, 5149, 5170, and 5197.
[5] The "Every Employee is an Emergency Manager" intiative is a disaster workforce-centric program designed to promote FEMA employee preparedeness, training, and emergency management engagement. *See*

(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.[6] DHS SCF members are non-FEMA DHS employees who volunteer to supplement FEMA's emergency and disaster response and recovery personnel during major events. FEMA Corps Members are National Service Members undertaking a year of service through the FEMA Corps program, which is jointly operated by the Corporation for National and Community Service (CNCS) and FEMA.[7] FEMA also deploys employees and contractors from DHS Headquarters; DHS Components; non-FEMA partners from other federal agencies (typically from the Small Business Administration (SBA) and the Department of Housing and Urban Development (HUD)); state, local, and tribal governments; and voluntary agencies through Mission Assignments. A Mission Assignment is a FEMA work order, with or without reimbursement, that directs another federal agency to use its authorities and the resources granted to it under federal law in support of state, local, tribal, and territorial government assistance.[8]

FEMA uses DTS to track and monitor all deployed personnel for safety and security purposes, as well as to conduct historical staffing analyses to improve the efficacy of its disaster response efforts. DTS allows FEMA to track and monitor new assignments and to associate all user actions with specific personnel. DTS enables FEMA to maintain and archive FEMA Personnel availability dates for deployment, as well as track responders' deployment history, deployment status, deployment notifications and timely responses, actions taken during a deployment, job positions, proficiencies and qualifications, skills, langauges, and trainings. DTS also enables all deployed personnel to provide safety and security accountability daily for accepted deployment requests. DTS also stores position qualifications, specialties, certifications, and training histories to enhance deployment decisions (e.g., matching personnel who have specific language skills to an area in which such language proficiency is required).

To ensure FEMA maintains a workforce with a diverse set of disaster recovery and response skills, all personnel hold FEMA Qualification System (FQS)[9] disaster titles. In accordance with the FEMA Administrator's aforementioned vision of every employee being an emergency manager, every FEMA employee will be assigned to one of four position categories: Incident Management, Incident Support, Ancillary Support, or Mission Essential. These position categories are defined as:

https://www.fema.gov/blog/2012-02-06/every-employee-emergency-manager-and-femas-workforce-transformation.

[6] 42 U.S.C. § 5121.

[7] FEMA Corps is a unit of 1,600 service corps members dedicated to disaster preparedness, response, and recovery. The program is a partnership between FEMA and CNCS that enhances FEMA's disaster response and recovery personnel with young adults, ages 18-24, who are devoted solely to FEMA emergency and disaster response efforts. *See* https://careers.fema.gov/fema-corps.

[8] 42 U.S.C. §§ 5170(a) and 5192; 44 CFR 206.2(a)(18).

[9] DHS/FEMA/PIA-033 Deployment Qualifications Program (August 16, 2013), *available at* https://www.dhs.gov/compliance.

- Incident Management (IM) – disaster field operations staff
- Incident Support (IS) – National or Regional Response Coordination Center staff
- Ancillary Support (AS) – staff deployed in place at normal duty stations to support disaster operations (may be deployed as the mission dictates)
- Mission Essential (ME) – staff required to maintain mission-essential functions

As of October 1, 2015, FEMA Personnel use DTS to manage qualifications for these FQS positions. DTS maintains basic deployment experience, training, qualification, and certification data for personnel. The FEMA DTS Data Management team uploads training course information and completion date(s) to DTS. This team receives training information from various training systems, including the FEMA Emergency Management Institute (EMI),[10] FEMA Employee Knowledge Center (FEKC), FEMA Independent Study Database (ISDB),[11] and FEMA National Emergency Management Training Center (NETC).

DTS requires the collection and maintenance of PII to perform its functions. DTS collects PII from FEMA Personnel; personnel from DHS Components that participate in the DHS SCF initiative; FEMA Corps Members; federal contractors; representatives from non-profit organizations; and state, local, and tribal government agencies who are deployed during a disaster and serve as FEMA partners in the field. FEMA uses this PII to contact responders, disseminate deployment orders, and track the location and safety of personnel while on deployment. FEMA also uses this PII to identify the capabilities of personnel for deployment-related assignments, track personnel availablity for deployment during a disaster, and ensure FEMA has the personnel required to provide an effective response in the event of a disaster declaration. User profiles are created to enable users to supply their contact information, request new position titles, request attendance at FQS-required training course offerings, and manage their languages, specialties, and certifications. This ensures FEMA can track the skillsets of all responders, contact the proper individuals for specific deployment requests in the event of a disaster declaration, and subsequently deploy available personnel to meet the needs of particular disaster situations. Both FEMA Personnel and Non-FEMA Personnel have access to edit, update, and correct their own PII while their respective profiles are active in DTS.

Initial Data Entry and Employment Verification

FEMA Employees

During FEMA's hiring and onboarding process, FEMA imports each employee's information into DTS and creates a profile on behalf of all FEMA Personnel (permanent full time,

[10] DHS/FEMA/PIA-022 Student Training/Exercise Application and Registation Records (March 29, 2012), *available at* https://www.dhs.gov/compliance.
[11] *Id.*

temporary full time, CORE, and reservist). A subset of this data comes directly from the United States Department of Agriculture, National Finance Center (NFC).

Should a FEMA employee need to correct data imported from NFC in DTS, he or she may do so. However, information in DTS will be overwritten/updated by each subsequent NFC import. To remedy any discrepancies, FEMA employees may use the MyEPP[12] site or work with FEMA's Office of the Chief Component Human Capital Officer (OCCHCO) to make corrections to NFC directly. Other data is collected directly from the individual through his or her onboarding paperwork. However, a formal Paperwork Reduction Act package has neither been completed, nor submitted to the Office of Management and Budget (OMB). FEMA's OCCHCO is working to complete this paperwork.

FEMA Corps and SCF

DTS receives a small subset of specified responder PII from FEMA Corps and SCF to create responder records for FEMA Corps and SCF volunteers. The upload for FEMA Corps includes the employee's first name, last name, email address, phone number, hire date, primary position, personnel status, organization, team, team position, team captain indicator, expected release date, and a unique identifier assigned by National Civilian Community Corps (NCCC). This unique identifier is a National Service Participant ID number (NSPID).[13] The upload for SCF includes first name, last name, email address, job series, status, hire date, organization, city, state, supervisor email, emergency contact name, and phone number.

FEMA Corps Member profiles are created from a roster provided by the AmeriCorps NCCC. For SCF volunteers, DHS Components provide profile information to SCF Management staff, who then manually enter it into DTS to create user profiles. Information for state, local, tribal, and territorial (SLTT) personnel is manually entered into the system at the field level, as needed.

Other Non-FEMA Partners

Human Resources personnel at the Joint Field Office (JFO)[14] manually enter the requisite information from other federal (non-DHS) agency employees and contractors who are not members of the SCF, such as SBA and HUD; state, local, and tribal government employees; or non-profit organizations who may collaborate with FEMA, on an as-needed basis, during disaster response and recovery operations into DTS. The information required to create a profile for these responders is first name, last name, email address, hire date, and organization/agency.

[12] MyEPP is the federal employee portal where individuals can manage their payroll and tax information. *See* https://www.nfc.usda.gov/EPPS/index.aspx?ReturnUrl=%2fepps%2f.

[13] The National Service Participant Identification (NSPID) number is a unique identifier assigned sequentially to each new national service member by CNCS. CNCS administers the AmeriCorps program. Each time a new member begins a term of service with any AmeriCorps program, that individual is assigned an NSPID number. CNCS shares the NSPID number with FEMA in the export the NCCC program office provides to FEMA Corps Management staff in place of Social Security numbers.

[14] https://www.fema.gov/pdf/emergency/nims/jfo_sop.pdf.

Day-to-Day System Use

FEMA's Deployment Tracking System (DTS) encompasses two different portals, DTS Deployer[15] and DTS Responder.[16] The Deployer portal is where new user profiles are created, deployment requests are issued, personnel deployments are managed, tranings are scheduled and curated, and personnel titles and qualifications are issued and managed. The DTS Responder portal is the set of pages that the end user sees and functions as a management site for the information related to each individual (both FEMA Personnel and Non-FEMA Personnel). It is the site that is used to accept or decline deployment or training requests, request new position titles or taskbooks, manage and correct contact information, take workflow actions, and request availability changes.

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. When FEMA leadership determines that a particular disaster or emergency event requires additional staff support, the WMD Deployment and Analysis Branch and regional staffing points of contact (SPOC) create deployment requests in DTS to initiate the identification and deployment of available FEMA Personnel. Deployment orders to an individual are based on the specific program area, position, and qualification needs of a particular disaster; a given responder's FQS title; and FEMA's Deployment Directive.[17] All FEMA Personnel, SCF Members, and FEMA Corps members receive official deployment request notifications to their preference of official (work) email, personal email, text message, or automated voice recording. Personnel who receive a deployment request from DTS must sign in to the DTS Responder portal within 24 hours in order to view the request's details and either accept or decline it. For FEMA Corps Members, Team Leaders (pre-identified FEMA Corps Members) accept or decline the requests for their respective teams in bulk. Responders are also required to update their availability status, as well as to accept or decline deployment requests via the DTS Responder portal. All deployed FEMA Personnel, FEMA Corps Members, and SCF Members use DTS to check-in to assigned duty stations, provide daily accountability in order to monitor employee safety and security, make changes to their lodging or assigned duty station, and demobilize once deployment has been completed. For all other personnel, field HR managers simply note in the system the event and duty station to which the individual is deployed, along with expected and actual arrival and demobilization dates. No daily daily accountability, account maintenance, or other system actions are required from these users.

Messaging

DTS contains a messaging module that allows supervisors, event managers, and DTS System Messaging Managers to send messages to the users' Responder portal page in DTS. Once users receive a message through the above-described methods, they can acknowledge/confirm the

[15] https://www.femadts.net.
[16] https://www.femaresponder.net.
[17] FEMA FD 010-8 (Revised) FEMA Incident Workforce Deployment, (Oct. 16, 2014). *No publically available link.*

message as well as comment on the message. These messages are generally all-hands messaging directed to a large subsections of the workforce, or event management staff informing responders of a safety or security incident. FEMA tracks when personnel respond to the messages, which FEMA Personnel are generally required to do within 24 hours.

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?

DTS is authorized to collect the PII described in Section 2.2 under the following authorities and Executive Orders:

- The Homeland Security Act of 2002, 6 U.S.C. §§ 313, 314, 317, 320, and 711 – providing authority to set up response capabilities for various types of disasters, including credentialing resources and arranging deployment of assets.
- Robert T. Stafford Disaster Relief and Emergency Assistance Act, *as amended*, 42 U.S.C. §§ 5144, 5149, 5170b, 5192, and 5197 – providing authority of the President to provide personnel for response to various disasters.
- 44 U.S.C. §§ 3101, and 3534 – making the head of an agency responsible for information collected and maintained by the agency as well as the security for systems in which that information is contained.
- Executive Order 9397 – Numbering Sytem for Federal Accounts Relating to Individual Persons,[18] as amended by Executive Order 13478 – Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers;[19] (allowing a federal agency to use personnel Social Security numbers when assigning some sort of identification number to personnel).

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:

[18] Executive Order 9397, "Numbering System for Federal Accounts Relating to Individual Persons." 8 FR 16095 (November 30, 1943).

[19] Executive Order 13478 "Amendments to Executive Order 9397 Relating To Federal Agency Use of Social Security Numbers." 73 FR 70239 (November 20, 2008).

- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) System of Records,[20] which 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 Personnel Emergency Contact Information System of Records,[21] which covers the information needed to contact DHS personnel to respond to all hazards emergencies or to participate in exercises; and
- OPM/GOVT-1 General Personnel Records System of Records,[22] which allows FEMA to collect pertinent workforce information on federal personnel for data accuracy purposes.

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 will approve the system security plan and issue an updated Authority to Operate (ATO) when this PIA is published.

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

The FEMA Records Management Branch is currently assessing input records for applicable schedules. If found, those records without schedules will be held as permanent until FEMA can work with NARA and write and approve a schedule. Information about DTS itself, and possible outputs, will be treated as permanent until such time as FEMA and NARA have written and approved a schedule for the system.

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 package for deployment collection forms is in the approval process. This PIA will be updated when those forms have official OMB numbers.

[20] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) System of Records, 77 FR 70792 (November 27, 2012), *available at* https://www.dhs.gov/compliance.

[21] DHS/ALL-014 Personnel Emergency Contact Information System of Records, 81 FR 48832 (August 25, 2016), *available at* https://www.dhs.gov/compliance.

[22] OPM/GOVT-1 General Personnel Records System of Records, 77 FR 73694 (December 11, 2012), *available at* https://www.dhs.gov/compliance.

Section 2.0 Characterization of the Information

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

Automatically Generated by DTS about all personnel in the system:

- Personnel ID number

From FEMA Employees: (denotes fields required for NETC class admissions)**[23]

- First Name
- Last Name
- Middle Initial
- Nickname
- Personnel Type
- Hire Date
- Termination Date
- Street Address
- Street Address 2
- City
- State
- Zip code
- Zip Extension
- Home Address Latitude
- Home Address Longitude
- FEMA Organization Code
- Agency
- Social Security number (SSN) (Encrypted Identification Code)
- Region
- Supervisor of Record
- Possess Government Travel Card
- FEMA Student ID
- Annuitant
- Phone Number Area Code
- Phone Number
- Phone Number Extension
- Phone Type (Personal-Home, Personal-Cell, Work-Desk, Work-Cell, FEMA-Desk,

[23] Per FEMA form 119-25-1. *Available at* https://www.usfa.fema.gov/downloads/pdf/ff_119_25_1_75_5.pdf.

FEMA-Cell)

- Email Address
- Email Address Type (Work, Personal)
- Emergency Contact First Name
- Emergency Contact Last Name
- Emergency Contact Phone Number
- Specialty
- Language
- Assigned Position Job Type
- Assigned Position Program Area
- Assigned Position
- Assigned Position Proficiency
- Is the Assigned Position Primary or Subordinate?
- Training Class Registration Course Description**
- Training Class Registration Course Date**
- Training Class Registration Course Location**
- Training Class Registration Date of Birth**
- Training Class Registration U.S. Citizen**
- Training Class Registration Not U.S. Citizen City of Birth**
- Training Class Registration Not U.S. Citizen State of Birth**
- Training Class Registration Gender Identification**
- Training Class Registration Race (only used if necessary to identify deployed personnel who are injured or die in the line of duty)**
- Training Class Registration Ethnicity (only used if necessary to identify deployed personnel who are injured or die in the line of duty)**
- Training Class Registration Home Street Address**
- Training Class Registration Home Street Address 2**
- Training Class Registration Home City**
- Training Class Registration Home State**
- Training Class Registration Home Zip Code**
- Training Class Registration Reasonable Accommodation**
- Training Class Registration Reasonable Accommodation Comment**
- Training Class Attended Course Code
- Training Class Attended Description
- Training Class Attended Date
- Training Class Attended Awarded By
- Training Class Attended Award Date

- Training Class Attended Location
- Training Class Comment
- Training Class Document
- Certification Description
- Certification Awarded By
- Certification Credited
- Certification Expiration Date
- Certification Awarded Date
- Certification Comment
- Certification Document
- User Logon Session Length
- User Logon Last Logon
- User Logon Failed Attempt
- User Logon Remote IP
- User Logon User Agent
- User Logon Authentication Type (User Name/Password or PIV)
- User Logon Authentication Source (Responder Portal or Deployer)
- NFC Organization Code
- Pay type
- Grade
- Step
- Series
- Salary
- Pay Period
- Empower HR ID[24]

<u>From all Deployed Personnel:</u>

- Deployed Event
- Deployed Duty Station with Duty Station Address
- Lodging Name
- Lodging Address
- Lodging Phone Number
- Lodging Room Number
- Rental Car Information
- Deployed Supervisor of Record

[24] The Empower HR ID is a unique identifier from an NFC file that exists for each individual in FEMA's FedHR system.

- Deployed Position Job Type
- Deployed Position Program Area
- Deployed Position
- Deployed Position Proficiency
- Deployed Per Diem Authorized
- Deployed Rental Car Authorized
- Deployed Daily Accountability Check Completed (From FEMA Employees, SCF, and FEMA Corps Only)

From SCF Personnel: (denotes fields required for NETC class admissions)**

- First Name
- Last Name
- Middle Initial
- Nickname
- Personnel Type
- Hire Date
- Termination Date
- Street Address
- Street Address 2
- City
- State
- Zip code
- Zip Extension
- Home Address Latitude
- Home Address Longitude
- Agency
- Supervisor of Record
- FEMA Student ID
- Phone Number Area Code
- Phone Number
- Phone Number Extension
- Phone Type (Personal-Home, Personal-Cell, Work-Desk, Work-Cell, FEMA-Desk, FEMA-Cell)
- Email Address
- Email Address Type (Work, Personal)
- Emergency Contact First Name
- Emergency Contact Last Name

- Emergency Contact Phone Number
- Specialty
- Language
- Assigned Position Job Type
- Assigned Position Program Area
- Assigned Position
- Assigned Position Proficiency
- Is the Assigned Position Primary or Subordinate?
- Training Class Registration Course Code
- Training Class Registration Course Description**
- Training Class Registration Course Date**
- Training Class Registration Course Location**
- Training Class Registration Date of Birth**
- Training Class Registration U.S. Citizen**
- Training Class Registration Not U.S. Citizen City of Birth**
- Training Class Registration Not U.S. Citizen State of Birth**
- Training Class Registration Gender Identification**
- Training Class Registration Race (only used if necessary to identify deployed personnel who are injured or die in the line of duty)**
- Training Class Registration Ethnicity (only used if necessary to identify deployed personnel who are injured or die in the line of duty)**
- Training Class Registration Home Street Address**
- Training Class Registration Home Street Address 2**
- Training Class Registration Home City**
- Training Class Registration Home State**
- Training Class Registration Home Zip Code**
- Training Class Registration Reasonable Accommodation**
- Training Class Registration Reasonable Accommodation Comment**
- Training Class Attended Course Code
- Training Class Attended Description
- Training Class Attended Date
- Training Class Attended Awarded By
- Training Class Attended Award Date
- Training Class Attended Location
- Training Class Comment
- Training Class Document
- Certification Description

- Certification Awarded By
- Certification Credited
- Certification Expiration Date
- Certification Awarded Date
- Certification Comment
- Certification Document
- User Logon Session Length
- User Logon Last Logon
- User Logon Failed Attempt
- User Logon Remote IP
- User Logon User Agent
- User Logon Authentication Type (User Name/Password or PIV)
- User Logon Authentication Source (Responder Portal or Deployer)

From FEMA Corps: (* denotes information collected by CNCS;[25] ** denotes fields required for NETC class admissions)

- First Name
- Last Name
- Middle Initial
- Nickname
- Personnel Type
- Hire Date
- Termination Date
- Street Address*
- Street Address 2*
- City*
- State*
- Zip code*
- Zip Extension*
- Agency
- Supervisor of Record
- FEMA Student ID
- Phone Number Area Code
- Phone Number
- Phone Number Extension
- Phone Type (Personal-Home, Personal-Cell, Work-Desk, Work-Cell, FEMA-Desk,

[25] Field exists in DTS, but data is not captured or generated when creating new personnel records.

FEMA-Cell)

- Email Address
- Email Address Type (Work, Personal)
- Emergency Contact First Name
- Emergency Contact Last Name
- Emergency Contact Phone Number
- Specialty
- Language
- Assigned Position Job Type
- Assigned Position Program Area
- Assigned Position
- Assigned Position Proficiency
- Is the Assigned Position Primary or Subordinate
- Training Class Registration Course Description**
- Training Class Registration Course Date**
- Training Class Registration Course Location**
- Training Class Registration Date of Birth**
- Training Class Registration U.S. Citizen**
- Training Class Registration Not U.S. Citizen City of Birth**
- Training Class Registration Not U.S. Citizen State of Birth**
- Training Class Registration Gender Identification**
- Training Class Registration Race (only used if necessary to identify deployed personnel who are injured or die in the line of duty)**
- Training Class Registration Ethnicity (only used if necessary to identify deployed personnel who are injured or die in the line of duty)**
- Training Class Registration Home Street Address**
- Training Class Registration Home Street Address 2**
- Training Class Registration Home City**
- Training Class Registration Home State**
- Training Class Registration Home Zip Code**
- Training Class Registration Reasonable Accommodation**
- Training Class Registration Reasonable Accommodation Comment**
- Training Class Attended Course Code
- Training Class Attended Description
- Training Class Attended Date
- Training Class Attended Awarded By
- Training Class Attended Award Date

- Training Class Attended Location
- Training Class Comment
- Training Class Document
- Certification Description
- Certification Awarded By
- Certification Credited
- Certification Expiration Date
- Certification Awarded Date
- Certification Comment
- Certification Document
- User Logon Session Length
- User Logon Last Logon
- User Logon Failed Attempt
- User Logon Remote IP
- User Logon User Agent
- User Logon Authentication Type (User Name/Password or PIV)
- User Logon Authentication Source (Responder Portal or Deployer)

<u>From State/Local, Contractors, or Employees of Other Federal Agencies ONLY When Deployed:</u>

- First Name
- Last Name
- Middle Initial
- Nickname
- Personnel Type
- Hire Date
- Termination Date
- Street Address
- Street Address 2
- City
- State
- Zip code
- Zip Extension
- Agency
- Home Address Latitude
- Home Address Longitude
- Phone Number Area Code

- Phone Number
- Phone Number Extension
- Phone Type (Personal-Home, Personal-Cell, Work-Desk, Work-Cell, FEMA-Desk, FEMA-Cell)
- Email Address
- Email Address Type (Work, Personal)
- Emergency Contact First Name
- Emergency Contact Last Name
- Emergency Contact Phone Number
- Deployed Event
- Deployed Duty Station with Address
- Lodging Name
- Lodging Address
- Lodging Phone Number
- Lodging Room Number
- Rental Car Information
- Deployed Supervisor of Record
- Deployed Position Job Type
- Deployed Position Program Area
- Deployed Position
- Deployed Position Proficiency
- Deployed Per Diem Authorized
- Deployed Rental Car Authorized

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

The responders' PII that is entered into DTS comes from multiple sources. The sources and collection methods are as follows:

Directly from the Employee: During the onboarding process, FEMA collects PII from onboarding employees as part of their OCCHCO package. This PII is manually entered into DTS, in order to create the employee's account.

***NFC File Upload*:** The NFC file upload process entails a data extraction performed by the OCCHCO Information System's Branch. Once the extraction occurs, the file is saved on a secured file server within the FEMA Enterprise Network (FEN). The WMD Deployment Section imports the extracted file into a DTS processing utility that converts the SSN from the file into an encrypted, salted hash.[26] The encrypted file is uploaded into DTS for the processing of additions (new employees), updates, and deletions (terminated employees). The following data fields come from NFC, and cannot be edited by FEMA employees using DTS:

- First Name
- Middle Initial
- Last name
- Address 1
- Address 2
- City
- State
- Zip Code + Plus 4
- Employee Type
- Date of Birth
- Gender
- Unknown
- SSN (immediately encrypted upon upload/processing)
- FEMA Organization Code
- NFC Organization Code
- Pay type
- Grade
- Step
- Series
- Salary
- Pay Period
- Enter on Duty Date
- Status (Active/Terminated)
- Hired Job Title
- Organization Supervisor Code
- Empower HR ID

Password-Protected FEMA Corps File: The FEMA Corps roster file is generated by CNCS and uploaded by a FEMA Corps program manager. DTS will process the file and make the necessary additions, updates, and deletions.

[26] FEMA uses the encrypted SSN to verify FEMA employees' identities from the NFC file import, and to validate and update FEMA employees' employment status as necessary. The encrypted SSN is also used to create a Personnel ID for the responder. DTS does not store raw SSNs.

Password-Protect SCF File: The SCF file is generated by the organization's SCF liaison. The liaison emails the password-protected file to the WMD/Workforce Generation Branch/SCF Section. Once reviewed for accuracy by the SCF Section, the password is removed and the file is uploaded into DTS for the processing of additions, updates, and deletions.

Independent Study (IS) Database File: The IS database file is exported from the Independent Study system. The exported file is placed on a secure file server within the FEN. A DTS data manager processes the most current file through DTS and awards credit for training course completions.

NETC Database File: The NETC database file is exported from the NETC admissions system. The exported file is placed on a secure file server within the FEN. The DTS Data Management team processes the most current file through DTS and generates new or updated records for scheduled or cancelled training courses.

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, DTS does not use information from commercial sources or publicly available data.

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, whenever possible. In the case of FEMA Corps Members, accuracy is ensured via receipt of roster information directly from CNCS and imported by a FEMA Corps program manager. For SCF members, the data is collected directly from the individuals and uploaded by SCF program managers. FEMA also relies on official employee information maintained by the NFC to ensure the accuracy of payroll and FEMA Personnel data in DTS. All personnel with a DTS account have access to correct and verify the accuracy of their own data within DTS. Moreover, all active FEMA employees have access to correct and verify the accuracy of their own data that is stored in NFC through MyEPP, or through the FEMA OCCHCO.[27]

Data is scheduled to be refreshed from the NFC on a bi-weekly basis to ensure the most current and accurate information is reflected in DTS. At times, this process is delayed because of process overloads, or the NFC file may be corrupted based on the data extraction. If the NFC file cannot be repaired, the NFC file may be skipped for a given pay period until the file repair can be completed.

[27] https://www.fema.gov/mission-support.

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 PII based on the personnel type of each individual responder, as well as whether the individual is deployed. While the fields exist to store the information for all personnel, FEMA has created highly-tailored business rules to appropriately scale (lessen) the amount of PII typically collected from state and local individuals when they are deployed to a specific disaster site, in addition to the amount of PII captured for SCF or FEMA Corps Members. Once deployed to a disaster site, additional PII may be necessary to guarantee the safety of the responders and contact their emergency contacts in the event of a personal emergency.

Privacy Risk: There is a risk that FEMA may misenter or collect erroneous information about FEMA Personnel.

Mitigation: All personnel with a DTS account have access to correct their own data within DTS. Additionally, all active FEMA employees have access to correct their own data that is stored in NFC through MyEPP, or through the FEMA OCCHCO.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

FEMA uses the information in DTS to issue deployment requests, determine deployment assignments, and track responders for safety, security, and accountability purposes.

FEMA uses the encrypted SSN to verify FEMA employees' identities from the NFC file import. DTS does not store raw SSNs. The SSN is encrypted immediately upon a FEMA employee's profile being created in DTS; this encrypted value is used to validate and update FEMA employees' employment status as necessary. Prior to the NFC file being uploaded, it is encrypted and securely stored on FEMA's Enterprise Network (FEN).

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?

Yes. Employees of other DHS Components may have access to DTS as users if they are members of SCF and subject to deployment. These SCF members only have access to their own account information. Employees of other DHS Components do not have administrative roles or rights within the system.

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 restricts access to the DTS data to DTS users and DTS support personnel. Support personnel have access to DTS data on a need-to-know basis, and any user found to be misusing DTS data will be subject to discipline, up to and including loss of employment or loss of security clearance.

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.

DTS provides the requisite notice of FEMA's information collection to facilitate its deployment programs through many different media. Given the possibility of a non-U.S. citizen being deployed, FEMA provides notice through a Privacy Notice to all users prior to granting access to the system. The text of this Privacy Notice is included as an appendix to this PIA.[28] In addition, the DHS/ALL-014 Personnel Emergency Contact Information SORN provides notice to disaster response and recovery personnel regarding FEMA's collection of information. Lastly, the DHS/ALL-004 General Information Technology Access Account Records System of Records Notice, the OPM/GOVT-1 General Personnel Records System of Records Notice, and this PIA provide notice of FEMA's collection of information in order to grant FEMA personnel DTS access.

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 required

[28] Appendix A: Deployment Tracking System IT System Privacy Notice.

information may directly impact an individual's 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.

For SCF, FEMA Corps, state/local personnel, contractors, or employees of other federal agencies, the data maintained about these personnel while deployed is necessary in order to ensure the safety and maintain the accountability of all personnel for which FEMA is responsible. In most cases, these individuals voluntarily provide this information, with the exception of data that is automatically imported from NFC and from FEMA Corps. In addition, non-FEMA responders are informed when they sign up for potential emergency deployment that limited information will be securely shared with the relevant FEMA deployment management personnel.

The FEMA WMD is working to develop literature to better inform deployed personnel what information about them is collected, maintained, stored, and disseminated, as well as the purpose for this collection. This PIA serves as the guidelines for the WMD's collection and use of PII through a memorialized signature on an OMB-approved form.

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 purposes of deployment coordination and accountability.

Mitigation: FEMA provides notice of its collection of information through a Privacy Notice prior to users accessing DTS (see Appendix A). In addition, FEMA makes new employees aware of information that will be required upon their acceptance of a FEMA position. This risk is further mitigated by FEMA's WMD Deployment Branch, which also gives employees an opportunity to provide consent prior to information collection through a memorialized signature on an OMB-approved form. In addition, this PIA and the SORNs listed in Section 4.1 above provide notice of FEMA's collection of information to grant DTS access to system users.

Section 5.0 Data Retention by the project

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

Currently, DTS inputs and any associated outputs are being treated as permanent records, until the appropriate schedules can be identified or written.

5.2 Privacy Impact Analysis: Related to Retention

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

Mitigation: This risk is not currently mitigated. FEMA is working to mitigate this privacy risk by applying for and establishing NARA-approved retention and disposal schedules for DTS, in order to minimize the time FEMA 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 Operating 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 the PII stored in DTS outside of DHS for the purpose of informing emergency contacts in the event that FEMA Personnel or Non-FEMA Personnel are injured pursuant to their FEMA duties. The data would be shared on a limited basis with a responder's self-selected emergency contact when informing the emergency contact that the responder has been harmed as a result of his or her FEMA duties. The information shared would generally be limited to include the responder's name, the event and duty station to which the responder is deployed, and a point of contact for the emergency contact to submit any further inquiries to.

FEMA may share information with federal, state, tribal, local, international, or foreign government agencies or executive offices, relief agencies, and non-governmental organizations when the disclosure is appropriate in the performance of official duties required in response to technical, manmade, or natural disasters. This shared information is generally aggregated and is presented in standardized reports from DTS that do not contain PII.

FEMA shares aggregated, snapshotted FEMA Corps Member location and Team Lead work contact information with CNCS staff. The information that DTS shares with CNCS is aggregated by FEMA Corps Team and is used only to validate project assignment information and to ensure a common operating environment between the two agencies during both steady-state and disaster events. This aggregated data does not contain PII.

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

FEMA only shares the information within DTS outside of FEMA in accordance with routine uses defined in the Personnel Emergency Contact Information SORN.[29] The data maintained about personnel while deployed is necessary in order to ensure the safety and maintain

[29] DHS/ALL-014 Personnel Emergency Contact Information System of Records, 81 FR 48832 (Aug. 25, 2016).

the accountability of all personnel for which FEMA is responsible. Routine Use J of that SORN allows the data in DTS to be shared with a responder's self-selected emergency contact. This is compatible with the original collection because information is shared to support DHS emergency response deployments and to contact designated persons in the event of an emergency.

FEMA also shares aggregated deployment location and contact information with CNCS as prescribed in Routine Use F of the Personnel Emergency Contact Information SORN, which allows FEMA to share FEMA Corps staff contact and location information with CNCS pursuant to an Interagency Reimbursable Work Agreement (IRWA) between FEMA and CNCS.[30] This is compatible with the original collection because the sharing of information is necessary to accomplish functions related to DHS workforce accountability and supporting DHS emergency response deployments.

Persuant to Routine Use I, FEMA may share information with federal, state, tribal, local, international, or foreign government agencies or executive offices, relief agencies, and non-governmental organizations when the disclosure is appropriate in the performance of official duties required in response to technical, manmade, or natural disasters. This shared information is generally aggregated and is presented in standardized reports from DTS that do not contain PII.

6.3 Does the project place limitations on re-dissemination?

Yes. FEMA shares information only pursuant to the routine uses outlined in the SORNs mentioned in Section 1.2 and with CNCS, as described in 6.1. If additional sharing is planned in the future, a Memorandum of Understanding (MOU), Interagency Agreement (IAA), IRWA, or Information Sharing Access Agreement (ISAA) will be executed between FEMA and the external entity, such as another federal agency, SLTT partner, or other voluntary relief agencies.In addition, NFC and CNCS re-disseminate information only in accordance with the Privacy Act and the SORNs cited in 1.2.

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

As described in 6.1, FEMA only shares PII outside of DHS under limited circumstances, in the event of an emergency and the need to disclose to the injured party's emergency contact information. If a responder is injured or dies while on deployment, and responder information from DTS is shared with the respective emergency contact, such a disclosure will be logged by the System Owner. In addition, the system will store an audit log for each time a responder's emergency contact information is accessed.

[30] https://careers.fema.gov/fema-corps.

6.5 Privacy Impact Analysis: Related to Information Sharing

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

Mitigation: The only external-to-DHS entity with which FEMA regularly shares DTS information is CNCS, as defined in Section 6.1 and per the agreement between CNCS and FEMA. FEMA shares snapshotted FEMA Corps Member contact and location information with CNCS staff for validation and to ensure a common operating environment between the two agencies.

Section 7.0 Redress

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

Individuals have direct access to their own data through the DTS Responder portal. The deployment information within DTS is part of the SORNs mentioned in Section 1.2 of this PIA. Individuals may also access their information via a Privacy Act (PA) or Freedom of Information Act (FOIA) request to the DHS HQ Chief FOIA Officer or FEMA Disclosure Office Branch Chief. The SORNs that cover DTS provide instructions for all PA and FOIA requests within DTS.

Information related to access to the DTS IT system is part of the GITAARS SORN.[31] Individuals may access their information via a PA 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?

All responders with a profile in DTS, regardless of citizenship status, can update and correct their stored information through the DTS Responder portal. All active DTS account holders have access to correct their own data that is stored in NFC through MyEPP or through the FEMA OCCHCO. Individuals who are U.S. citizens may also correct or update their information via a PA request to the FEMA Disclosure Office Branch Chief. Individuals who are not U.S. citizens do not have access to this form of redress. However, it is highly unlikely that there are individuals who are not U.S. citizens with DTS accounts. In the event that such a user does exist, he or she can correct his or her own information in DTS by accessing his or her account in the DTS Responder portal. The SORNs that cover DTS provide instructions for all PA redress within DTS. The deployment information within DTS is part of the SORNs mentioned in Section 1.2 of this PIA. Information related to access to the DTS IT system falls under the GITAARS SORN.

[31] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) System of Records, 77 FR 70792 (November 27, 2012), *available at* https://www.dhs.gov/compliance.

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

This PIA and the aforementioned SORNs in Section 1.2 inform FEMA and Non-FEMA Personnel how to correct their information in DTS. In addition, FEMA provides notice of redress in DTS directly to DTS account holders during their initial disaster responder orientation, as well as during subsequent training courses. FEMA verbally explains the redress process to employees' supervisors and program managers, or via email or telephone.

Additionally, all DTS account holders have access to correct their own data within DTS. Moreover, all active federal employees have access to correct their own data that is stored in NFC through MyEPP, or through FEMA OCCHCO.

7.4 Privacy Impact Analysis: Related to Redress

There is no risk to redress because all individuals may access and correct any records maintained by FEMA in DTS. FEMA employees can change information from the NFC through MyEPP or FEMA OCCHCO.

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?

DTS maintains auditing and accountability logs that are reviewed on a monthly basis for suspicious activity or activity in excess of a user's assigned privileges.

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

DHS requires all personnel to successfully meet annual privacy awareness and information security training. DTS's support personnel do not receive additional role-based privacy training.

DTS also protects privacy by using role-based access; employees are granted access to perform specific tasks on specific portions of the system only if both their program leadership and DTS managers approve an access request on a "need-to-know" basis. System audit logs are reviewed on a montly basis by the Information System Security Officer and the DTS System Administrator to ensure that role-based activities comport with the user's authorized permissions. If access in excess of a user's role is discovered, the user's access is removed and the user's supervisor is alerted. If further misuse is discovered, an incident is created with the FEMA Security Operations Center.

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 governing DTS use. Designated WMD Deployment and Analysis Branch personnel determine which FEMA employees require access to DTS. Once WMD confirms a new user's need for access with the appropriate manager, DTS managers manually apply the requested roles to the user's profile in DTS. Functional roles can be restricted by Cadre/Program Area, Region, or Event. WMD assigns most roles to users via the personnel submodule of the DTS Deployer portal. Upon approval as a DTS Deployer user, FEMA grants role-based access limiting the individual to only that 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?

If any external-to-DHS information sharing were planned for the future, WMD/Deployment & Analysis Branch/System Integration & Reports Section would execute an MOU, ISAA, and an Interconnection Security Agreement. FEMA Privacy and the Office of Chief Counsel review all such documents for privacy and cybersecurity equities, before final execution. At this time, the WMD Deployment Branch does not envision external information sharing.

Responsible Officials

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

Approval Signature

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

____

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

Appendix A: Deployment Tracking System IT System Privacy Notice

AUTHORITY: The Homeland Security Act of 2002, §§ 313, 314, 317, 320, and 711,; the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act) as amended, §§ 303, 306, 403, and 502, and 621, 42 U.S.C. §§ 5144, 5149, 5170b, 5192, and 5197; Exec. Order No. 13478, 73 Fed. Reg. 70,239, (November 18, 2008); Exec. Order No. 9397, 8 Fed. Reg. 16,095, (Nov. 30, 1943); and 5 U.S.C. § 552a(b).

PURPOSE(S): This information is being collected and maintained to contact individuals for deployment in the event of a disaster, as well as to ensure their safety while on deployment.

ROUTINE USE(S): The information on this form may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974, as amended. This includes using this information as necessary and authorized by the routine uses published DHS/ALL-014 Personnel Emergency Contact Information System of Records, 81 Fed. Reg. 48,832 (August 25, 2016) and OPM/GOVT-001 General Personnel Records System of Records, 77 Fed. Reg. 73,694 (December 11, 2012), and upon written request, by agreement, or as required by law. The Department of Homeland Security's Systems of Records notices may be found at https://www.dhs.gov/system-records-notices-sorns.

DISCLOSURE: The disclosure of information on this form is voluntary, but failure to provide the information requested may delay or prevent FEMA from selecting and locating employees with particular job titles and specialties for deployments.