Privacy Impact Assessment
for the

Deployment Programs

DHS/FEMA/PIA-032

August 16, 2013

Contact Point
Richard Rosene
Incident Workforce Management Office
Response Directorate
Office of Response and Recovery
(202) 212-2270

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 (OR&R), Response Directorate, Incident Workforce Management Office (IWMO) Deployment Unit coordinates deployment programs under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act). To deploy disaster response and recovery personnel, the IWMO Deployment Unit operates the Automated Deployment Database (ADD) system. FEMA collects information from FEMA disaster response and recovery personnel assigned to support disaster response and recovery operations and uses that information to coordinate and manage deployments. FEMA is conducting this Privacy Impact Assessment (PIA) because FEMA collects, uses, maintains, retrieves, and disseminates personally identifiable information (PII) through ADD for the purpose of coordinating and managing deployments.

Overview

To meet the challenges of its long-standing all-hazards response mission under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act), and to deliver coordinated, successful response operations, the IWMO Deployment Unit has established several Information Technology (IT) systems that support deployment of FEMA disaster response and recovery personnel.

When a Presidentially-declared disaster occurs under the Stafford Act, FEMA relies on not only its own employees, but also on number of personnel. FEMA's disaster response and recovery personnel include: FEMA Permanent Full Time Employees (PFT), Temporary Full Time Employees (TFT), FEMA Reservists, Cadre of On-call Response Employees (CORE), the FEMA Corps, and DHS Surge Capacity Force (SCF) programs. Through partnerships and mission assignments, FEMA also uses employees and contractors from DHS headquarters, DHS components, and other federal agencies, as well as representatives of state, local, and tribal governments and voluntary agencies. FEMA appoints CORE employees for 2-4 years for the purpose of performing disaster preparedness, response, recovery, and mitigation-related activities under the Stafford Act. The new FEMA Corps program is an innovative partnership between FEMA and the Corporation for National and Community Service (CNCS) that enhances FEMA's disaster response and recovery personnel with a trained and reliable corps of 18-24 year olds, devoted solely to FEMA disaster response and recovery efforts. The DHS SCF provides the ability to rapidly expand and supplement FEMA's disaster response and recovery personnel with DHS headquarters and other DHS component personnel following a major disaster. Under FEMA's "Every Employee is an Emergency Manager" initiative, FEMA trains, qualifies, and assigns regular and recurring emergency management duties to PFT, TFT, CORE, and Reservist disaster response and recovery personnel.

The IWMO Deployment Unit owns and operates ADD, FEMA's official deployment coordination and management system used to contact, monitor, request, and deploy disaster response and recovery personnel to disasters throughout the nation. ADD monitors overall program readiness and capabilities and tracks the deployment of disaster response and recovery personnel. ADD also maintains basic information regarding federal contractors and representatives from non-profit organizations, state, local, and tribal government agencies who are serving as FEMA partners in the field. In addition to ADD,

the following systems support deployment: FEMA's Enterprise Data Warehouse/Operational Data Store (EDW/ODS) for reporting and the Availability Reporting System (ARS) for personnel to report status.

FEMA collects, uses, maintains, retrieves, and disseminates PII of disaster response and recovery personnel pursuant to its authorities and obligations under the Stafford Act and Post-Katrina Emergency Management Reform Act (PKRMRA). FEMA collects social security numbers (SSN) of FEMA and other DHS employees pursuant to 5 U.S.C. § 1302 Regulations, 31 U.S.C. § 7701(c), "General Assistance Administration," Executive Order 13478, "Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers," and Executive Order 9397, "Numbering System for Federal Accounts Relating to Individual Persons."

Automated Deployment Database (ADD): Initial Setup and Notice

FEMA's deployment programs provide the requisite notice of FEMA's collection of information to facilitate its deployment programs through many different media. FEMA provides notice through Privacy Act Statements on the following forms: *Automated Deployment Database Employee Information Form* (Appendix A); *Automated Deployment Database Standard Deployment Order Form* (Appendix B); *Automated Deployment Database Name Deployment Order Form* (Appendix C); and *Non-FEMA Deployment Information Form* (Appendix D). FEMA also provides a privacy notice to FEMA employees requesting access to ADD (Appendix E) and then again to authorized ADD users prior to granting access to the system (Appendix F). In addition, FEMA's Availability Reporting System (ARS) provides notice to callers before they provide any PII or updates to their availability. Lastly, this PIA and DHS/ALL-014 Department of Homeland Security Emergency Personnel Location System of Records, 73 FR 24807, October 17, 2008, provide notice to disaster response and recovery personnel regarding FEMA's collection of information.[1]

Once FEMA collects the information from the individual, the IWMO Deployment Unit manually enters the data into the ADD system, which stores the individual's personal contact information, along with additional data such as emergency contacts, sponsoring organizations, and job titles. ADD contains two modules of information about the groups of individuals who may be eligible for deployment during a national disaster. The F2 module includes information about FEMA PFT, TFT, DHS SCF, CORE, Reservists, and FEMA Corps. The F7 module consists of information about federal contractors and employees of non-DHS federal agencies, state, local, and tribal government agencies, and non-profit organizations that are not part of the SCF.

F2: FEMA PFT, TFT, CORE, and Reservist Employees

With the on-boarding process, every new FEMA employee must complete an *Automated Deployment Database Employee Information Form* (Appendix A), which collects pertinent information, such as the name, organization, SSN, date of birth (DOB), gender, deployment job titles, contact information, and emergency contact information. Either the employee, Regional Office point-of-contact (POC), or a FEMA Human Capital (HC) representative completes the form, and the IWMO Deployment Unit manually enters the data into ADD. In addition, an import from the U.S. Department of Agriculture (USDA) National Finance Center (NFC) verifies the PII, including SSN, name, address, and phone, and

---

[1]See http://www.gpo.gov/fdsys/pkg/FR-2008-10-17/html/E8-24807.htm

adds or updates employment information, such as entrance on duty (EOD) date, organization, and grade/step/series/salary.

F2: DHS SCF Volunteers

For DHS headquarters and component employees who volunteer and are approved for the SCF, component POCs collect the pertinent employee registration information via specified forms approved by the respective headquarters or component leadership. However, each component collects and securely transmits the data in a unique manner. For instance, members of the SCF must enter their SSN, DOB, and other information directly onto the *Surge Capacity Force Volunteer Registration Form*. U.S. Citizenship and Immigration Services (USCIS) collects the required information through its registration form and securely forwards the information to the USCIS Office of Human Capital and Training (HCT). A USCIS HCT representative, in turn, verifies the information from USDA/NFC and manually enters it into the spreadsheet for secure transmittal to the IWMO Deployment Unit. In contrast, the U.S. Coast Guard (USCG) avoids manual input by creating a unique identifier for each SCF participant via email, then linking that identifier to data from the USDA/NFC before securely transmitting the data to the IWMO Deployment Unit. The IWMO Deployment Unit requires each participating component POC to securely transmit updates to its SCF volunteer information via email on a quarterly basis. DHS SCF volunteers may contact their respective SCF office/component POCs in order to access and correct their information; the POCs, in turn, may contact the Deployment Unit.

F2: FEMA Corps Members

For FEMA Corps members, a CNCS team leader collects the necessary information and securely transmits it to FEMA. These POCs manually enter the information into spreadsheets and securely transmit it to the IWMO Deployment Unit. Following the collection of this information, ADD creates database records for each employee. Additionally, in order to update and reconcile the records for FEMA employees in ADD, FEMA imports an organizational abstract and an employee file from the NFC Database biweekly via an automated ADD script. FEMA and CNCS are currently developing an automated process for transferring this data to FEMA during Phase 2 of FEMA Corps implementation. In order to access and update their information, FEMA Corps members may contact their team leaders, who in turn may contact the IWMO Deployment Unit.

F7: Non-FEMA Partners

A typical transaction for the F7 module involves the collection of information from other federal (non-DHS) agency employees and contractors who are not members of the SCF; state, local, and tribal government employees, and non-profit organizations who may collaborate with FEMA during disaster response and recovery. While the collection process varies by region and federal agency, these individuals usually complete a *Non-FEMA Deployment Information Form* (Appendix D) at the Joint Field Offices (JFO) for a specified disaster. The JFO manually enters the information into ADD for tracking purposes. These federal, state, local, and tribal representatives, contractors, and representatives of non-profit organizations may request that their supervisors, program managers, or FEMA POCs access and update their information through the Deployment Unit.

Deployment Orders, ADD Updates, and ARS

For any new DHS SCF volunteer or FEMA employee record who is entered into ADD, the ADD system assigns a personal identification number (PID) to track and monitor each individual's assignment(s) and stores the name, SSN, DOB, job title(s), and disaster assignment experience that supports position qualification and currency, along with other specified PII. The ARS system is the method by which the deployment database identifies, maintains, and archives a DHS SCF volunteer's status for deployment. DHS SCF employees who are not currently deployed are required to update their availability status by calling FEMA's automated ARS, which immediately updates their availability status in ADD. The system asks identifying questions, including the SSN and DOB, then states the SCF volunteer's current status and asks him or her to confirm or change his or her deployment status as "available" or "unavailable." FEMA employees who are currently deployed are instructed to call ARS only to check-in, change lodging, duty station, and/or check-out. FEMA Reservists, who are now required to make themselves available all but 60 days per year, do not use ARS for changes to their availability status; instead, reservists remain "available" unless they are pre-approved for non-availability. When FEMA leadership determines that a particular event requires additional staff support, the IWMO Deployment Unit may request the deployment of FEMA employees and/or members of the SCF. To do so, the IWMO Deployment Unit may complete an _Automated Deployment Database Standard Deployment Order Form_ (Appendix C) for deployment activation. The form includes the needed program areas, job titles, and specialties, the tour duty station and location, and the name, phone number, and position of the POC and Alternative POC. In situations when specific uniquely qualified individuals are needed for specialized tasks, the IWMO Deployment Unit may submit an _Automated Deployment Database Name Deployment Order Form_ (Appendix D) for specialized deployment activation. For instance, all staffing requirements in legal affairs, alternative dispute resolution, equal rights, security, and safety require name deployment orders.

Qualifications, Sharing, and Privacy Protections

Under its deployment qualifications program, FEMA qualifies PFTs, TFTs, COREs, and Reservist employees who hold FEMA Qualification System (FQS)[2] disaster titles. To do so, ADD will share, via FEMA's Enterprise Data Warehouse/Operational Data Store (EDW/ODS), basic employment and experience data on these employees with the U.S. Department of Interior (DOI), Bureau of Land Management (BLM), Incident Qualifications and Certification System (IQCS) through an Interagency Agreement (IAA) and Memorandum of Understanding (MOU).[3]

---

[2] FQS is a set of doctrine used to establish and measure the performance, experience, training, and certifications of disaster response and recovery personnel against a qualifications standard for incident management and support positions. For more information on FQS and the process through which FEMA qualifies deployment eligible personnel, see the _FEMA Deployment Qualifications Program PIA_.

[3] FEMA will use the ADD-generated PID number as a unique identifier to query FEMA's training databases and Learning Management System (LMS) to collect specified training data. FEMA will share the resulting data, along with the PID and other PII from ADD, including position title, deployment experience, FQS program-specific organization code, employment type (PFT, CORE, TFT, or Reservist), and EOD date, with DOI/BLM's IQCS via a secured flat file. DOI/BLM's IQCS updates the records and transfers the responders' qualification status back to

FEMA continually replicates ADD data in real time to the EDW/ODS for ad hoc data retrieval, report generation, and storage. In Phase 2 of FQS/IQCS implementation, scheduled for 2013, FEMA will share ADD information and training datasets with IQCS, and vice versa, via an automated process to and from EDW/ODS as a storage and retrieval site.

ADD collects and maintains unique and pertinent information, such as SSN, name, DOB, home address, phone number, emergency contact information, duty station location, and limited training information, such as courses completed by those individuals related to their assignment. ADD receives PII data by both manual and automated entry. The ADD system protects privacy using role-based access within the database and granting an employee access to the system if and only if his or her program leadership approves an access request on a "need to know" basis. ADD prevents the inappropriate use of the information collected by granting access to information that is pertinent to the respective user's role. FEMA uses the information in ADD to determine deployment assignments. When individuals are terminated as DHS or FEMA employees, the biweekly import from the NFC Database updates the individual's record in ADD. When SCF volunteers or FEMA Corps members are terminated, the approved Program Official notifies the IWMO Deployment Unit so that their database records may be updated in ADD. Additionally, when any active FEMA employees, SCF volunteers, or FEMA Corps members are restricted from involvement in FEMA's deployment programs for reasons other than termination, the approved Program Official notifies the IWMO Deployment Unit so that their information may be updated in the system. The IWMO Deployment Unit is currently working with the FEMA Records Management Division (RMD) and the National Archives and Records Administration (NARA) to finalize a suitable approved retention schedule for ADD.

The primary privacy risk associated with ADD is that manual data entry will result in erroneous data being saved in ADD. To mitigate this risk, FEMA uses a bi-weekly NFC Database import. In addition, the IWMO Deployment Unit regularly reviews records for accuracy. Following the biweekly NFC Database import, if the IWMO Deployment Unit finds a discrepancy regarding SSNs or other PII, the IWMO Deployment Unit will verify the information with the respective individual and/or POC to ensure accuracy. Both FEMA Corps team leaders and FEMA supervisors and program managers verify the names of the team members upon deployment to ensure accuracy.

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?

- Sections 303, 306, 403, 502, and 621 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended, Pub. L. No. 93-288, and codified at 42 U.S.C. §§

ADD to update the individual's record. This sharing will occur on a regular basis. For more information on FQS and the FEMA's sharing of information with BLM's IQCS, see the *FEMA Deployment Qualifications Program PIA.*

5144, 5149, 5170, and 5197;

- Sections 503, 504, and 624 of the Homeland Security Act of 2002, codified at 6 U.S.C. §§ 313, 314, 320, and 711;
- Exec. Order No. 13478, "Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers;"
- Exec. Order No. 9397, "Numbering System For Federal Accounts Relating to Individual Persons;"
- 5 U.S.C. § 1302, "Government Organization and Employee Regulations;"
- 31 U.S.C. § 7701(c), "General Assistance Administration;"
- 44 CFR §§ 206.5, 206.7-206.8, 206.43; and
- Homeland Security Presidential Directive 5, "Management of Domestic Incidents."

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-014 Department of Homeland Security Emergency Personnel Location System of Records, 73 FR 61888, October 17, 2008, (http://www.gpo.gov/fdsys/pkg/FR-2008-10-17/html/E8-24807.htm);
- DHS/ALL-021 Department of Homeland Security Contractors and Consultants, 73 FR 63179, October 23, 2008, (http://www.gpo.gov/fdsys/pkg/FR-2008-10-23/html/E8-25205.htm); and
- DHS/ALL-004 Department of Homeland Security General Information Technology Access Account Records System of Records, 77 FR 70792, November 27, 2012, (http://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm).

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

ADD was originally a sub-system of FEMA's National Emergency Management Information System (NEMIS) and was covered under the NEMIS Certification and Accreditation (C&A) until 2006. At that time, ADD's classification changed from sub-system to major application, which required its own C&A. On January 9, 2006, FEMA's Office of the Chief Information Officer (OCIO) granted ADD an Interim Approval to Operate (IATO) to allow for completion of the WebADD system development and C&A process, which did not occur at that time. The current ADD C&A was completed in May 2013.

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, data will be retained and once NARA has approved this retention and disposal schedule, this PIA will be updated and all data will be retained and disposed of in accordance with the NARA approved schedule, including retroactively.

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.

Some of the information that FEMA collects is exempt from PRA pursuant to 44 U.S.C. § 3502(3)(A) and Presidential Memorandum, "Information Collection under the Paperwork Reduction Act," April 7, 2010. Information collected from state points of contact and other non- federal entities will be covered PRA-approved forms. The PRA package for the *Non-FEMA Deployment Information Form* (Appendix D) is in the approval process.

Section 2.0 Characterization of the Information

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

FEMA collects identification and contact information from individuals who participate in deployment programs through various means, depending on the program. These participants include FEMA employees, DHS employees, and other federal agency employees. In addition, as described below, in certain situations, FEMA may collect information from employees of state, local, and tribal government agencies, federal contractors, and non-profit organizations who partner with FEMA at JFOs or elsewhere in the field. ADD is the workforce management tool that FEMA uses to contact, assign, and track the deployment experience of those individuals whom FEMA may deploy in response to a disaster or incident. For its deployment programs, FEMA may collect PII from its employees, employees of other DHS components, employees of other federal agencies, state, local, and tribal government agencies, federal contractors, and non-profit organizations. ADD stores this information, along with additional data, such as emergency contacts, sponsoring organizations, and job titles. All ADD data is also stored in EDW/ODS. In addition, ADD produces and stores reports that provide deployment information that is used by FEMA management and those responsible for deployment coordination and management. Once FEMA fully implements Phase 2 of its deployment qualifications program, which is scheduled for 2013, FEMA will share ADD information and training datasets with DOI/BLM's IQCS, and vice versa, via an automated process to and from FEMA's EDW/ODS as a storage and retrieval site.

ADD contains two modules, "F2" and "F7," that store information about a subset of the individuals participating in FEMA's deployment programs. The F2 module consists of information regarding FEMA employees, FEMA Corps members, and SCF volunteers. The F7 module consists of

information on federal contractors, representatives of non-profit organizations, and non-DHS federal agencies, as well as state, local, and tribal governments. F7 does not include SCF volunteers.

Each subset of individuals whose data appears in ADD is listed below, along with the corresponding data elements that are collected for each respective subset:

FEMA Employees

ADD collects the following information from FEMA employees (including PFT, TFT, CORE, and Reservist personnel) through the *Automated Deployment Database Employee Information Form* (Appendix A) or the NFC Database import file:

Data Entered by the IWMO Deployment Unit and NFC Database Import:
- Full Name;
- SSN;
- DOB;
- Gender;
- Home Address;
- Email Address;
- Phone Numbers (home, work, and cell);
- Emergency Contact Information (name, relationship, and phone number);
- Organizations, Job Titles, Program Areas, and Proficiency Levels of Each;
- Specialty(ies);
- Grade/Step/Series/Salary;
- EOD Date;
- Type of Employee (PFT, TFT, CORE, or Reservist);
- Pay Type/Pay Period Information; and
- Government Charge Card? (yes or no).

Data Collected by ADD from ARS as a Result of Phone Updates by FEMA Employees:
- Check-In/Check-Out Date/Time;
- Lodging; and
- Duty Station.

DHS Headquarters and Component SCF Volunteers

ADD collects information from DHS headquarters SCF volunteers through the online *Surge Capacity Force Volunteer Registration Form* and securely transmits the data via a spreadsheet to the IWMO Deployment Unit. For DHS Component SCF volunteers, Component POCs collect information (data elements vary slightly by component) through respective online and paper registration forms and securely transmit the data via a spreadsheet to the IWMO Deployment Unit. The following data elements may be included for Headquarters and Component SCF volunteers:

Data Entered into ADD by the IWMO Deployment Unit:
- Full Name;

- SSN;
- DOB;
- Gender;
- Office/Duty Station Location;
- Home Address;
- Email Address(es);
- Phone Numbers (home, work, and cell);
- Emergency Contact Information (name, relationship, email address, and phone numbers);
- Job Series Code;
- Confirmation of Supervisor's Written Approval for Training Authorization and SCF Volunteer Eligibility;
- Government Charge Card? (yes or no);
- Confirmation of Supervisor's Written Approval for Training Authorization and SCF Volunteer Eligibility; and
- Authorization and Certification Statement (attached to registration form).

Data Collected by ADD from ARS as a Result of Phone Updates by SCF Volunteers:
- Availability Status ("available" vs. "unavailable")

Other Federal Agency Employees, Contractors, State/Local/Tribal Government Employees, and Non-Profit Organization Representatives

ADD collects information from other federal agency employees; contractors; state, local, and tribal government agency employees; and representatives of non-profit organizations located at JFOs throughout the nation, via the *Non-FEMA Deployment Information Form* (Appendix D):

Data Entered into ADD by the IWMO Deployment Unit:
- Full Name;
- Gender;
- Agency Name and Address;
- Employee Type (i.e., contractor, state/local/tribal agency, or voluntary agency);
- Deployment Tour Information (job number, date on site, and departure date);
- Tour Lodging Information (name of establishment, address, and phone number);
- Agency Job Information (job title, job description, and state/end dates);
- Agency POC Information (name, job title, and phone number); and
- Emergency Contact Information (name, relationship, and phone numbers).

Data Generated by ADD for Each Individual with Information in ADD
- PID Number

Data Transferred Back to FEMA for Upload into ADD after Updates in DOI/BLM's IQCS

The following information is returned from DOI/BLM's IQCS to FEMA's ADD following qualification and training updates:

- PID (referred to as the Employee ID or *EmplID* in IQCS); and
- Current FQS Position Title(s), plus corresponding qualification status (i.e., trainee or qualified).

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 ADD through paper forms, data extracts from the USDA/NFC Database, and telephone keypad update entries by disaster response and recovery personnel. FEMA deployment programs use a combination of manual and automated processes to collect information and ultimately store it in ADD.   The sources of information for FEMA's deployment programs and ADD include: 1) individuals who are participating in FEMA's deployment programs; 2) individuals who collaborate with FEMA through a JFO in response to a disaster; 3) USDA/NFC Database; 4) ARS; 5) ADD itself, which creates a PID for each individual in the system; and 6) DOI/BLM's IQCS, which returns to ADD update qualification information.[3]

FEMA may collect information directly from the individual through a paper form, or in the case of ARS, via telephone; FEMA may collect information from the deployable individuals through another person, such as a program or Regional Office POC; 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, neither FEMA's deployment programs nor ADD use information from commercial sources or publicly available sources.

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, as often as possible. In other cases, Regional Office POCs, FEMA Corps leaders, FEMA HC representatives, POCs at DHS Headquarters and other DHS components, and other federal agencies may provide the information on behalf of individuals under their purview. The POCs and HC representatives are responsible for verifying the information, and the IWMO Deployment Unit also reviews the records. For SCF volunteers from DHS headquarters and other DHS

---

[3] For more information, see the *FEMA Deployment Qualifications PIA*.

components, the IWMO Deployment Unit requires each POC to send updates to its SCF volunteer information on a quarterly basis. For instance, if the NFC Database import results in two names corresponding with the same SSN or the same name corresponding with two different SSNs, the IWMO Deployment Unit verifies the information with the respective individuals and/or POCs. In this manner, the data extracts from the USDA/NFC Database assist FEMA in ensuring the accuracy of its information. In addition, FEMA program managers, who are responsible for reviewing the employee records, may contact the IWMO Deployment Unit to correct discrepancies. The IWMO Deployment Unit also monitors the database records daily, providing reports to management and forwarding concerns or suspected inaccuracies to the IWMO Deployment Unit and/or the employee's manager. Finally, in order to reconcile the database records, organizational abstracts and employee files from the USDA/NFC Database are imported biweekly into ADD via an automated script.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: The privacy risk associated with FEMA's deployment programs is that the Agency could collect inaccurate information on disaster response and recovery personnel due to the manual data entry of information into ADD.

Mitigation: This privacy risk is mitigated by requiring regular reviews of the data for accuracy by the IWMO Deployment Unit. Additionally, in order to ensure accuracy following each biweekly USDA/NFC Database import, employees of the IWMO Deployment Unit who note any discrepancies regarding the SSNs or other information immediately verify the information with the respective individual and/or POC. Furthermore, FEMA Corps team leaders and FEMA program managers verify the names of the team members upon deployment to ensure accuracy.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

FEMA uses this information to determine deployment assignments and manage the availability of disaster response and recovery personnel. In addition, the information in ADD is used to track the deployment and training experience and availability status. The information, including the SSN and DOB, is required to uniquely identify and track individuals to coordinate and manager their deployments. The ARS system is the method by which the deployment database identifies, maintains, and archives a DHS SCF volunteer's status for deployment. DHS SCF employees who are not currently deployed are required to update their availability status by calling FEMA's automated ARS, which immediately updates their availability status in ADD. The system asks identifying questions, including the SSN and DOB, then states the SCF volunteer's current status and asks him or her to confirm or change his or her deployment status as "available" or "unavailable." FEMA employees who are currently deployed are instructed to call ARS only to check-in, change lodging, duty station, and/or check-out.

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, neither FEMA's deployment programs nor ADD conduct electronic searches, queries, or analyses in an electronic database to discover or located a predictive pattern or an anomaly.

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

The IWMO Deployment Unit manages FEMA's deployment programs and ADD. No other DHS components have assigned roles and responsibilities within ADD; however, the IWMO Deployment Unit requires each participating component POC to securely transmit updates to its SCF volunteer information via email on a quarterly basis. In addition, when an SCF volunteer is first approved, the designated component POC collects the employee's registration information via a specified form, which has been approved by the respective headquarters or component leadership, then securely transmits the data to FEMA. Most DHS headquarters and component POCs use their own unique forms and methods of collection for use in ADD.

3.4 <u>Privacy Impact Analysis</u>: Related to the Uses of Information

<u>Privacy Risk:</u> The privacy risk associated with FEMA's deployment programs is that the Agency could use the information in ADD for purposes other than that for which it was originally collected.

<u>Mitigation:</u> FEMA mitigates this privacy risk by limiting the collection of information to that which is necessary to contact individuals and manage and coordinate their deployments. In addition, FEMA limits access to the information and ADD 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 ADD to "read only" access by the IWMO Deployment Unit and to the occasions in which FEMA Regional Office personnel or FEMA HR personnel at JFOs may run ADD reports. Regional Office and JFO personnel, however, are prohibited from editing or adding information in ADD. Only FEMA personnel who are authenticated through Active Directory and are granted a password by the IWMO Deployment Unit or ADD's Information Systems Security Officer (ISSO) may edit information in ADD.

Section 4.0 Notice

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

FEMA provides notice of its collection of information to facilitate the provision of its deployment programs through many different media (see Appendices). Once approved, FEMA will use the *ADD Employee Information Form* and FEMA will provide a privacy notice on the form. Similarly, FEMA will use the *Non-FEMA Deployment Information Form* and FEMA provides notice through a Privacy Act Statement on the form. Additionally, once ADD users enter the system, FEMA provides a privacy notice. ARS also provides a privacy notice to FEMA and DHS SCF callers prior to collecting any information or availability updates. For non-FEMA disaster response and recovery professionals, either the FEMA Corps team leader or the component/agency/organization POC provides a verbal privacy notice to the respective personnel. This PIA and DHS/ALL-014 Department of Homeland Security Emergency Personnel Location System of Records, 73 FR 61888, October 17, 2008, (http://www.gpo.gov/fdsys/pkg/FR-2008-10-17/html/E8-24807.htm) provides notice of FEMA's collection of information. The DHS/ALL-004 Department of Homeland Security General Information Technology Access Account Records System of Records, 77 FR 70792, November 27, 2012, (http://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm) provides notice of FEMA's collection of information to grant FEMA employees access to ADD.

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, once he or she accepts a FEMA position, is accepting the terms of employment, the position description, and performance plans, which include requirements for participation in deployment programs. For FEMA employees, the failure to provide their information may directly impact their qualifications for employment. Reasonable accommodations will be made with respect to deployment for employees with qualifying disabilities. For employees of DHS Headquarters or DHS components who volunteer for the SCF, the failure to provide this information may jeopardize their position on the SCF. In a similar fashion, for FEMA Corps members, the failure to provide their information to CNCS could ultimately jeopardize their positions as FEMA Corps members.

4.3 <u>Privacy Impact Analysis</u>: Related to Notice

Privacy Risk: The privacy risk associated with FEMA's deployment programs is that individuals will not receive notice that their information is being provided to FEMA and ADD for deployment program management and coordination.

Mitigation: FEMA mitigates this privacy risk by providing notice of its collection of information for disaster response and recovery through Privacy Act Statements on FEMA forms (see Appendices), a

verbal privacy notice provided by FEMA Corps team leaders, DHS component or other federal agency POCs, and a verbal notice to FEMA employees who call ARS prior to collection. Finally, this PIA and DHS/ALL-014 Department of Homeland Security Emergency Personnel Location System of Records, 73 FR 61888, October 17, 2008, (http://www.gpo.gov/fdsys/pkg/FR-2008-10-17/html/E8-24807.htm) 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, 77 FR 70792, November 27, 2012, (http://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm) provides notice of FEMA's collection of information to grant FEMA employees access to ADD.

Section 5.0 Data Retention by the project

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

FEMA's 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. Once NARA has approved this retention and disposal schedule, this PIA will be updated and all data will be retained and disposed of in accordance with the NARA approved schedule.

5.2   <u>Privacy Impact Analysis</u>: Related to Retention

<u>Privacy Risk:</u>   There is a privacy risk that ADD will retain information longer than necessary and relevant.

<u>Mitigation:</u> FEMA mitigates this privacy risk by establishing a NARA approved retention and disposal schedule and minimizing the time the Agency keeps data, in line with the mission of its deployment programs.   In addition, FEMA leverages training and documentation, such as 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 information collected and entered into ADD with the following agencies: 1) USDA/NFC for the purposes of verifying information regarding disaster response and recovery personnel via an MOU and interconnection security agreement (ISA); and 2) DOI/BLM in order to share information and FQS training and certification requirements with IQCS via an IAA and MOU for the purpose of matching job titles of FEMA employees with qualifications and training criteria.[4] FEMA will only share the information within ADD outside of FEMA in accordance with the routine uses published in DHS/ALL-014 Department of Homeland Security Emergency Personnel Location System of Records, 73 FR 61888, October 17, 2008, (http://www.gpo.gov/fdsys/pkg/FR-2008-10-17/html/E8-24807.htm).

---

[4] See the *FEMA Deployment Qualifications PIA* for further details on FEMA's information sharing with DOI/BLM.

Responsible program and project managers review all MOUs, IAAs, and ISAs between FEMA and its partners, FEMA Privacy Officers, FEMA Chief Information Security Officer, FEMA Chief Counsel, and FEMA Operations Center (FOC) Director, and are then forwarded to DHS for formal review and approval. Information related to access to the ADD IT system will be shared in accordance with the routine uses in the DHS/ALL-004 Department of Homeland Security General Information Technology Access Account Records System of Records, 77 FR 70792, November 27, 2012, (http://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm).

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

Any sharing of deployment-related information in ADD is conducted in accordance with the Privacy Act and the routine uses prescribed in DHS/ALL-014 Department of Homeland Security Emergency Personnel Location System of Records, 73 FR 61888, October 17, 2008, (http://www.gpo.gov/fdsys/pkg/FR-2008-10-17/html/E8-24807.htm). The ADD system collects information from disaster response and recovery personnel to support disaster operations and uses that information for the purpose of deploying individuals to assist with natural and man-made disasters nationwide. This is carried out in a manner that is consistent with the published routine uses and is also compatible with the original purpose of collection. Information related to access to the ADD IT system will be shared in accordance with the routine uses in the DHS/ALL-004 Department of Homeland Security General Information Technology Access Account Records System of Records, 77 FR 70792, November 27, 2012, (http://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm).

6.3 Does the project place limitations on re-dissemination?

Yes, FEMA shares information only if a routine use outlined in the SORN listed under Section 6.2 above permits disclosure, and/or through an approved MOU or ISA, 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 SORN listed under Section 6.2 above, requests for ADD records should be made to the FEMA Disclosure Officer, who maintains the accounting of what records are disclosed and to whom. Requests for FEMA Corps personnel records should be made to the Chief Freedom of Information Act (FOIA) Officer at CNCS, and requests for SCF personnel records from DHS headquarters and other DHS components are made to the FOIA/Disclosure Office at the respective DHS offices/components.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a privacy risk that information in ADD could be erroneously disclosed.

Mitigation: FEMA mitigates this privacy risk only by sharing the information in the ADD system outside of FEMA pursuant to the routine uses found in the appropriate SORN as listed in section 1.2, such as DHS/ALL-014 Department of Homeland Security Emergency Personnel Location System of Records, 73 FR 61888, October 17, 2008, (http://www.gpo.gov/fdsys/pkg/FR-2008-10-17/html/E8-24807.htm), through an MOU or ISA, and/or pursuant to a written request submitted to the DHS Headquarters or the FEMA Disclosure Officer. 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 ADD 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 ADD is part of the DHS/ALL-014 Department of Homeland Security Emergency Personnel Location System of Records, 73 FR 61888, October 17, 2008, (http://www.gpo.gov/fdsys/pkg/FR-2008-10-17/html/E8-24807.htm) and individuals may access their information via a Privacy Act or FOIA request to the DHS Headquarters or the FEMA Disclosure Officer. Additionally, within the ADD system, the IWMO Deployment Unit may access the information regarding FEMA employees, FEMA Corps members, and SCF volunteers. FEMA employees, including Reservists, may contact their supervisors or program managers to access their information. FEMA Corps members may contact their team leaders to access their information; in turn, their team leaders may contact the IWMO Deployment Unit. For SCF, the respective DHS office/component POCs may forward updates to the IWMO Deployment Unit. State, local, and tribal representatives, contractors, and representatives of non-profit organizations in the field may ask their supervisors, program managers, or FEMA POCs to access their information through the IWMO Deployment Unit. Information related to access to the ADD IT system are part of the DHS/ALL-004 Department of Homeland Security General Information Technology Access Account Records System of Records, 77 FR 70792, November 27, 2012, (http://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm) and individuals may access their information via a Privacy Act or FOIA request to the DHS Headquarters or the FEMA Disclosure Officer.

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

The information within ADD is part of the DHS/ALL-014 Department of Homeland Security Emergency Personnel Location System of Records, 73 FR 61888, October 17, 2008, (http://www.gpo.gov/fdsys/pkg/FR-2008-10-17/html/E8-24807.htm) and individuals may access their information via a Privacy Act or FOIA request to the DHS Headquarters or the FEMA Disclosure Officer. Additionally, within the ADD system, the IWMO Deployment Unit may access the information regarding FEMA employees, FEMA Corps members, and SCF volunteers. FEMA employees, including Reservists,

may contact their supervisors or program managers to access their information. FEMA Corps members may contact their team leaders to access their information; in turn, their team leaders may contact the IWMO Deployment Unit. For SCF, the respective DHS office/component POCs may forward updates to the IWMO Deployment Unit. State, local, and tribal representatives, contractors, and representatives of non-profit organizations in the field may ask their supervisors, program managers, or FEMA POCs to access their information through the IWMO Deployment Unit. Information related to access to the ADD IT system are part of the DHS/ALL-004 Department of Homeland Security General Information Technology Access Account Records System of Records, 77 FR 70792, November 27, 2012, (http://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm) and individuals may access their information via a Privacy Act or FOIA request to the DHS Headquarters or the FEMA Disclosure Officer.

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 provide notice regarding ways in which DHS employees, contractors, and other individuals may correct their information. In addition, FEMA provides notice of redress in ADD directly to FEMA disaster response and recovery professionals during their initial disaster responder orientation as well as subsequent training courses. The redress process is explained to the FEMA employees' supervisors and program managers, the SCF volunteer POCs, and the FEMA Corps team leaders either via email, verbally, or telephone. These POCs and team leaders, in turn, describe the redress process to their respective participants.

7.4   <u>Privacy Impact Analysis</u>: Related to Redress

Privacy Risk: There is a privacy risk that individuals whose information appears in the ADD system will be unaware of the redress process.

Mitigation: FEMA mitigates this privacy risk by providing notice of redress in ADD directly to FEMA disaster responders, their POCs/team leaders/program managers during their initial training, and during subsequent training courses, as noted above in Section 7.3. The redress process is explained to the FEMA employees' supervisors and program managers, the SCF volunteer POCs, and the FEMA Corps team leaders either via email, verbally, or telephone. These POCs and team leaders, in turn, describe the redress process to their respective participants. In addition, DHS SCF volunteers and FEMA employees are notified when calling the ARS toll-free hotline that they can update their information in ADD through ARS. Furthermore, ADD provides users with a privacy notice, which includes redress information, prior to entry into the ADD system. Finally, this PIA, the ADD User Manual, and the DHS/ALL-014 Department of Homeland Security Emergency Personnel Location System of Records, 73 FR 61888, October 17, 2008, (http://www.gpo.gov/fdsys/pkg/FR-2008-10-17/html/E8-24807.htm) 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 IWMO Deployment Unit ensures that FEMA follows the practices stated in this PIA by leveraging 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 ADD system to successfully meet annual privacy awareness and information security orientation and training requirements according the FEMA training guidelines, as well as program-specific ADD system training. Moreover, the IWMO Deployment Unit provides additional orientation and training for ADD users, which includes usage of the system, as well as 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 uses SOPs to document ADD protocols and establish guidelines for how FEMA employees use ADD. FEMA has promised its DHS Headquarters and DHS component SCF partners that FEMA will provide accountability for all deployed personnel under SCF through ADD. FEMA allows personnel in its Regional Office and JFOs to view information in ADD with "read only" access on a "need to know" basis and may generate reports that include PII; however, Regional Office personnel are now prohibited from adding or editing information in ADD. Only FEMA staff who are authenticated through Active Directory and are granted a password by the IWMO Deployment Unit or ADD's ISSO may edit information in ADD. To become an ADD user, an ADD *User Access Control Form* (Appendix E) must be completed and signed by the employee and his or her supervisor. This form includes the justification for accessing the system, the type of access required, and confirmation of training completion. Upon approval, role-based access is granted, limiting the individual to only 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?

The ADD System leverages MOUs and ISAs as necessary to facilitate the information exchange needed to accomplish its mission. All MOUs and ISAs between FEMA and its partners are reviewed by responsible program/project managers, FEMA Privacy Officer, FEMA Chief Information Security Officer, FEMA Chief Counsel, and FOC Director and are then forwarded to DHS for formal review and approval. Currently, for deployment purposes, FEMA maintains an MOU/ISA with the USDA/NFC to verify information relating to disaster response and recovery personnel and an MOU/ISA with DOI/BLM to match FQS training and qualifications criteria with FEMA employees' job titles.[5]

Responsible Officials

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

Approval Signature

Original signed and on file at the DHS Privacy Office.

_____

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

---

[5] See the *FEMA Deployment Qualifications PIA* for further details about FEMA's information sharing with DOI/BLM.

Appendix A: Automated Deployment Database Employee Information Form

PRIVACY ACT STATEMENT

AUTHORITY: The Homeland Security Act of 2002, §§ 503, 504, and 624, 6 U.S.C. §§ 313, 314, 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, 5170a, and 5197; Exec. Order No. 13478, 73 FR 70239, November 18, 2008; Exec. Order No. 9397, 8 FR 16095, Nov. 30, 1943; 5 U.S.C. § 1302, "Government Organization and Employees Regulations"; The Debt Collection Improvement Act of 1996, 31 U.S.C. § 7701(c), "General Assistance Administration"; 44 C.F.R. §§ 206.5, 206.7-206.8, 206.43; and Homeland Security Presidential Directive 5, "Management of Domestic Incidents."

PURPOSE(S): This information is being collected and maintained to contact individuals for deployment in the event of a disaster.

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 in DHS/ALL – 014 Department of Homeland Security Emergency Personnel Location Records System of Records, 73 FR 61888, October 17, 2008, and upon written request, by agreement, or as required by law.

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.

Appendix B: Automated Deployment Database Standard Deployment Order Form

PRIVACY ACT STATEMENT

AUTHORITY: The Homeland Security Act of 2002, §§ 503, 504, and 624, 6 U.S.C. §§ 313, 314, 320, and 711; the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act) as amended, §§ 303, 306, 403, and 502, 42 U.S.C. §§ 5144, 5170a, and 5197; Exec. Order No. 13478, 73 FR 70239, Nov. 18, 2008; Exec. Order 9397, 8 FR 16095, Nov. 30, 1943; 5 U.S.C. § 1302, "Government Organization and Employees Regulations"; The Debt Collection Improvement Act of 1996, 31 U.S.C. § 7701(c); and Homeland Security Presidential Directive 5, "Management of Domestic Incidents."

PURPOSE(S): This information is being collected and maintained to enable FEMA's Deployment Unit to identify resource needs, determine the duty location, and deploy FEMA response and recovery professionals during a disaster according to their program areas, job titles, and specialties. In addition, the emergency contact information provided will allow FEMA to contact the employee's family and/or friends in the event of an emergency affecting the deployed individual.

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 in DHS/ALL – 014 Department of Homeland Security Emergency Personnel Location Records System of Records, 73 FR 61888, October 17, 2008, and upon written request, by agreement, or as required by law.

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.

Appendix C: Automated Deployment Database Name Deployment Order Form

PRIVACY ACT STATEMENT

AUTHORITY: The Homeland Security Act of 2002, § 501 et. seq., 6 U.S.C. §§ 313, 314, 320, and 711; the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act), as amended, §§ 303, 306, 403, and 502, 42 U.S.C. §§ 5144, 5149, 5170, and 5197; 5 U.S.C. § 1302, "Government Organization and Employees Regulations;" The Debt Collection Improvement Act of 1996, 31 U.S.C. § 7701(c); and Homeland Security Presidential Directive 5, "Management of Domestic Incidents."

PURPOSE(S): This information is being collected and maintained to enable FEMA to contact particular FEMA response and recovery professionals who have been selected for disaster deployment, based on their qualifications and areas of specialization.

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 in DHS/ALL – 014 Department of Homeland Security Emergency Personnel Location Records System of Records, 73 FR 61888, October 17, 2008, and upon written request, by agreement, or as required by law.

DISCLOSURE: The disclosure of information on this form is voluntary, but failure to provide the information requested may delay or prevent FEMA from locating and deploying the individuals named in a disaster deployment order.

Appendix D: Non-FEMA Deployment Information Form

PRIVACY ACT STATEMENT

AUTHORITY: The Homeland Security Act of 2002, §§ 503, 504, and 624, 6 U.S.C. §§ 313, 314, 320, and 711; the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act) as amended, §§ 303, 306, 403, and 502, 42 U.S.C. §§ 5144, 5149, 5170a, and 5197; , 5 U.S.C. § 1302, "Government Organization and Employee Regulations"; The Debt Collection Improvement Act of 1996, 31 U.S.C. § 7701(c), "General Assistance Administration"; 44 C.F.R. §§ 206.5, 206.7-206.8, and 206.43; and Homeland Security Presidential Directive 5, "Management of Domestic Incidents."

PURPOSE(S):   The information is being collected and maintained to enable FEMA to contact individuals who are serving at a FEMA Joint Field Office (JFO) during disaster response and recovery operations and to provide such individuals with access to FEMA information technology resources as needed.   In addition, the emergency contact information provided will allow FEMA to contact the individual's family and/or friends in the event of an emergency affecting the individual.

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 in DHS/ALL – 014 Department of Homeland Security Emergency Personnel Location Records System of Records, 73 FR 61888, Oct. 17, 2008; DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS), 77 FR 70792, November 27, 2012, and upon written request, by agreement, or as required by law.

DISCLOSURE: The disclosure of information on this form is voluntary, but failure to provide the information requested may delay or prevent individuals from being granted access to Information Technology resources and/or equipment at JFOs or elsewhere in the field.

Appendix E: Automated Deployment Database User Access Control Form

PRIVACY ACT STATEMENT

AUTHORITY: 44 U.S.C. §§ 3101 and 3534. The Social Security Number is collected pursuant to Exec. Order No. 13478, 73 FR 70239, Nov. 18, 2008; and Exec. Order No. 9397, 8 FR 16095, November 30, 1943.

PURPOSE(S): This information is being collected to enable FEMA to grant access to it Automated Deployment Database (ADD) system.

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 in DHS/ALL – 004 General Information Technology Access Account Records System of Records, 77 FR 70792, Nov. 27, 2012, and upon written request, by agreement, or as required by law.

DISCLOSURE: The disclosure of information on this form is voluntary, however failure to provide the information requested could delay or prevent FEMA from granting access to ADD.

Appendix F: Automated Deployment Database IT System Privacy Notice

FEMA is collecting this information to grant access to the Automated Deployment Database (ADD) under the authority of 44 U.S.C. §§ 3101 and 3534. The information 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 in DHS/ALL – 004 General Information Technology Access Account Records System of Records, 77 FR 70792, Nov. 27, 2012, and upon written request, by agreement, or as required by law. The disclosure of information on this form is voluntary, however failure to provide the information requested could delay or prevent FEMA from granting access to ADD.