Privacy Impact Assessment Update
for the

Enterprise Coordination and Approvals Processing System (eCAPS)

DHS/FEMA/PIA-023(x)

February XX, 2014

Contact Point
Arnie Gonzalez
Mission Assignment Branch
Response Directorate
(202) 646-4313

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The U.S. Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA), Office of Response and Recovery (ORR) operates the Enterprise Coordination and Approvals Processing System (eCAPS) application, an intranet-based web application. Following a Presidentially-declared disaster, ORR enables eCAPS to collect, maintain, and disseminate personally identifiable information (PII) from federal and state points of contact (POCs) who request disaster support from FEMA. eCAPS tracks action requests, coordinates and approves internal requisitions for services and supplies, and mission assignments. FEMA conducts this Privacy Impact Assessment (PIA) Update to reflect a name change for a form used to collect information for eCAPS and to reflect the interconnections with other DHS systems that were not discussed in the previous PIA.

Introduction

The eCAPS system initiates, tracks, and expedites the process of providing direct aid and technical assistance to other federal agencies and states in response to a Presidentially-declared disaster. In order to meet FEMA's response obligations under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act) and the Homeland Security Act of 2002 (Homeland Security Act), FEMA uses eCAPS to collect, maintain, and disseminate information from federal and state POCs who request disaster assistance. eCAPS matches these requests from government entities with FEMA's existing response capabilities and the response capabilities of the other federal agencies (OFAs) to which FEMA may delegate a mission assignment (MA).

Upon a Presidentially emergency declared emergency disaster under the Stafford Act and the Homeland Security Act, federal entities, and most often, state governments, submit requests to FEMA for direct federal support and/or technical assistance. Whether in anticipation of a major catastrophic event or following a major disaster, the governor of a state declares a state of emergency, and then requests federal assistance. State POCs may initiate these requests in several different ways, including by phone and paper form. When FEMA receives a "Resource Request Form" (RRF), formerly the Action Request Form/ARF, numbered as FEMA Form (FF) 010-0-7, from a State Approving Official (SAO), FEMA begins the review/approval process. For example, the State Coordinating Officer (SCO) or other POC completes an RRF, obtains the signature of the SAO, and transmits FF 010-0-7, by hand or electronically to the FEMA Action Tracker or Mission Assignment Manager (MAM), who then delivers the completed RRF to the FEMA Operations Section Chief (OSC) for approval. If there are any discrepancies with the information on the RRF, FEMA returns the form to the State POC by hand or verifies it through an informal phone call by the Action Tracker or MAM. Alternatively, the governor, emergency manager, or other state POC may contact a FEMA official to request support. In this scenario,

the MAM interviews the state POC by phone. During the call, the MAM provides the requisite privacy notice and collects the required information such as name, contact information, and a description of the requested assistance, and then forwards the information to a FEMA Action Tracker. In both instances, the OSC verifies and validates the request and considers whether or not it: 1) is eligible for federal funding; 2) can be supported by the state; 3) constitutes restorative or temporary work; and/or 4) is within the statutory authority of another federal agency. If any questions should arise, the OSC contacts the state POC for additional information.

If FEMA needs one or more other federal agencies to provide or supplement FEMA support, the OSC coordinates with the specified Emergency Support Function (ESF), Other Federal Agency (OFA), and or Recovery Support Function (RSF) POC(s) to ascertain other agency(ies') abilities to meet the request. If the other federal agency(ies) have the capabilities, the OSC assigns a project manager to the Mission Assignment (MA), and the ESF/OFA designates an action officer. Then the FEMA Project Manager and OFA Action Officer jointly develop a Statement of Work (SOW). If the OSC approves the action request and SOW, the OSC hand-delivers the approved, signed FF 010-0-7 (RRF) to the MAM, who in turn opens the Intranet-based eCAPS system. The Intranet is behind the FEMA firewall, so eCAPS is not accessible to those outside of FEMA. In order to access eCAPS, users must first authenticate through the Integrated Security and Access Control (ISAAC) by submitting their username and password. Once ISAAC authorizes the user, FEMA MAM sends a link to the user for eCAPS access. When the user selects the eCAPS, ISAAC redirects the user to the eCAPS application inbox page. For every subsequent request received from the user, eCAPS verifies the user's Session ID with FAMS. ECAPS, once opened, gives the MAM the choice of creating a new FEMA Form 010-0-8, "Mission Assignment Form" (MA) or a new FEMA Form 146-0-2, "Requisition and Commitment for Service and Supplies," (formerly FEMA Form 40-1).

If the MAM initiates an MA, he or she manually enters the information directly from FF 010-0-7 (RRF) into the appropriate fields of FF 010-0-8 (MA) within eCAPS. In addition, if the OSC determines that FEMA requires additional funds to fulfill the action request, and/or if a contract is necessary to fulfill a portion of the request, then either an National Response Coordination Center (NRCC) Ordering Specialist or a Project Officer affiliated with the requested resource uses the same eCAPS login process as the MAM but instead selects the option to create a new FF 146-0-2 (procurement request). This form documents the resource requirements, timelines, coordination, and approvals that are associated with a particular vendor. At this point, the NRCC Ordering Specialist or Project Officer manually enters the requested information from the completed, approved FF 010-0-7 (RRF) into FF 146-0-2 within eCAPS.

Once NRCC or Project Officer enters the information into eCAPS, eCAPS retrieves specified information about the disaster from IMCAD/EC, an enterprise-wide, web-based re-implementation of the previous National Emergency Management Information System (NEMIS) Client Server EC Module. IMCAD/EC provides data and work processes to assist eCAPS users

in managing disaster relief operations immediately following the incident through the creation of preliminary damage assessments (PDAs) and the eventual approval of the disaster declaration. IMCAD/EC shares the following data elements, among others, with eCAPS: the relevant disaster numbers, program and fund codes; incident names, periods, and codes; declaration date, programs, areas, and other information.

After eCAPS obtains the required data from IMCAD/EC, eCAPS automatically routes FF 010-0-8 (MA) to the FEMA MAM, project manager, and Federal Approving Official (FAO) for electronic approval. Upon approval by the MA, SAO and FAO, eCAPS routes FF 010-0-8 (MA) to the ES System for financial processing by the FEMA Comptroller. ES, formerly the NEMIS Client Server ES Module, provides a technology interface for financial transactions, such as Individual Assistance (IA) housing payments and recoupments, Public Assistance (PA) grant obligations and allocation requests, and Hazard Mitigation Grant Program (HMGP) commitments. The Comptroller's financial review of FF 010-0-8 (MA) may require him or her to view attachments, render forms, and/or duplicate data within ES. Subsequently, the Comptroller obligates the required funds in ES. Finally, the FEMA Action Tracker or MAM monitors the status of the FF 010-0-8 (MA) in eCAPS and delivers copies of the form, signed by the comptroller, to the ESF/OFA Action Officer, the FEMA Project Manager, and FEMA Acquisitions for filing and billing accountability. Users who logoff of eCAPS are redirected to the ISAAC logoff page.

FEMA may share ECAPS information with other federal agencies that have a role in providing support to meet the requirements of the state's action request. In addition, in rare circumstances, FEMA may share AR status information with SCOs through eCAPS at Joint Field Offices (JFOs). In these cases, the information in eCAPS is retrieved by a disaster ID number or state name but is not retrieved or retrievable by the PII of any member of the public (state official or OFA employee).

Reason for the PIA Update

FEMA is updating the eCAPS PIA to describe information sharing which FEMA did not describe in the previous PIA. In addition, FEMA has changed the name of FF 010-0-7 from ARF to RRF in order to more accurately describe the function and nature of the form. This PIA Update has incorporated user authentication for eCAPS users through ISAAC, the sharing of disaster declaration information from IMCAD/EC, and financial interface processing through the ES System.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

The System and the Information Collected and Stored within the System

Listed below are the data elements eCAPS receives from other systems, such as ISAAC, IMCAD/EC and the ES System. The previous eCAPS PIA did not include all of these data elements:

From IMCAD/EC:

- Incident Identification Number
- Incident Name
- Incident Period
- Incident State(s) Code(s) (i.e., CA, MD, DC)
- Incident Type Code (i.e., tornado, mudslide, hurricane, tropical storm)
- State/Region Number
- Disaster Finance Program Code
- Disaster Finance Program Number
- Disaster Fund Code
- Disaster Declaration Type Code
- Declaration Date
- Declared Programs
- Declared Areas
- Disaster Number
- Disaster Incident Identification Number
- Disaster State Code
- Disaster Region Number

From ISAAC:

Once logged in, eCAPS retrieves the following user's information from the FEMA Access Management System (FAMS):

- First Name
- Middle initial
- Last Name
- Username

- Email Address
- For Each NACS Role (Users may have multiple):
- Granted Role
- Region Number
- Disaster
- Team ID
- Team Description
- Position ID
- Position Title
- Homebase ID
- Team Key
- Access Control ID
- Module ID
- Position Type Code
- Hierarchy

From the ES System (formerly the NEMIS Client Server ES Module):

The previous PIA listed a number of data elements relating to FEMA employees, contractors, state/local/tribal agency, or other federal agency POCs, that were shared via FF 146-0-2, FF 010-0-7 (RRF), and FF 010-0-8 (MA). The treatment of these data elements remains the same.

Uses of the System and the Information

Users who require access to eCAPS must first authenticate through ISAAC by submitting a username and password. Upon authentication, ISAAC determines whether the user is authorized to access eCAPS, based on the current user role. There is no privacy risk associated with these updates.

Retention

Retention schedules have not changed.

Internal Sharing and Disclosure

While internal sharing and disclosure have not changed, the internal sharing was not discussed in the previous PIA. FEMA has, therefore, updated this PIA with the following discussion of the eCAPS' internal sharing of information:

Interfaces exist between eCAPS and the Incident Management Coordination Assessment and Determination/Emergency Coordination (IMCAD/EC), the Emergency Support (ES), and the Integrated Security and Access Control (ISAAC).

The eCAPS users authenticate via ISAAC. ISAAC includes both the Network Access Control System (NACS) for internal access control and FAMS for account creation and role-based access. NACS keeps track of password expiration and security training requirements. eCAPS shares user profile information with ISAAC to utilize ISAAC's centralized user authentication system. ISAAC, FAMS and NACs are included within the Authentication and Provisioning System (APS) GSS accreditation boundary.

IMCAD/EC provides data and automated work processes to assist eCAPS users in managing emergency and disaster relief operations from the very beginning of incident occurrence through disaster declaration. The primary processes covered within IMCAD/EC include: (1) collection of incident activity; (2) creation of PDAs; and (3) processing disaster declarations. The three primary products of IMCAD/EC processes are incidents since inception, PDAs, and requests for federal assistance.

eCAPS shares disaster declaration information with the ES System to facilitate disaster coordination. After the FAO (and SAO if required) approves/signs FF 010-0-8 (MA) within eCAPS, the form automatically routes to Emergency Support (ES) for financial processing by the Comptroller.

External Sharing and Disclosure

External sharing has not changed with this update.

Notice

Notice of any information collection for IMCAD or ISAAC is provided at the time the information is collected, prior to the information being shared from or with eCAPS.

Individual Access, Redress, and Correction

There has been no change to access, redress, and corrections regarding eCAPS. There is no privacy risk associated with the changes described in this update.

Technical Access and Security

Technical access and security have not changed, even taking into account hardware and software upgrades from December 2012. The data container was taken from a single server and

moved to a 3 node RAC cluster. The user will gain access to the application in the same manner as previously. There is no privacy risk associated with this change.

Responsible Official

Eric M. Leckey, Privacy Officer

Federal Emergency Management Agency

Department of Homeland Security

Approval Signature

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security