



**Homeland
Security**

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version date: June 10th, 2009
Page 1 of 8

PRIVACY THRESHOLD ANALYSIS (PTA)

**This form is used to determine whether
a Privacy Impact Assessment is required.**

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Rebecca J. Richards
Director of Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 703-235-0780

PIA@dhs.gov

Upon receipt, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSOnline and directly from the DHS Privacy Office via email: pia@dhs.gov, phone: 703-235-0780.



PRIVACY THRESHOLD ANALYSIS (PTA)

Please complete this form and send it to the DHS Privacy Office.
Upon receipt, the DHS Privacy Office will review this form
and may request additional information.

SUMMARY INFORMATION

DATE submitted for review: August 1, 2009

NAME of Project: FEMA FY 2009 Emergency Operations Center (EOC) Grant Program

Name of Component: Federal Emergency Management Agency

Name of Project Manager: Paul Belkin

Email for Project Manager: Paul.Belkin@fema.gov

Phone number for Project Manager: 202-786-9771

TYPE of Project:

- Information Technology and/or System[□]
- A Notice of Proposed Rule Making or a Final Rule.
- Other: FEMA is seeking OMB clearance for FEMA's Emergency Operations Center (EOC) Grant Program.

[□] The E-Government Act of 2002 defines these terms by reference to the definition sections of Titles 40 and 44 of the United States Code. The following is a summary of those definitions:

- "Information Technology" means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. See 40 U.S.C. § 11101(6).

- "Information System" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Note, for purposes of this form, there is no distinction made between national security systems or technologies/systems managed by contractors. All technologies/systems should be initially reviewed for potential privacy impact.



SPECIFIC QUESTIONS

1. Describe the project and its purpose:

FEMA has the lead for designing and operating the programmatic and administrative mechanisms for the FY 2009 Emergency Operations Center (EOC) Grant Program. The purpose of the EOC is intended to improve emergency management and preparedness capabilities by supporting flexible, sustainable, secure, and interoperable EOCs with a focus on addressing identified deficiencies and needs. The only eligible EOC applicants are Governor-designated State Administrative Agencies (SAAs).

A national review panel comprised of FEMA officials (headquarters and regions) and peer subject matter experts review, evaluate, and prioritize proposals (based on need and impact) of those applicants that have complied with all administrative and programmatic grant requirements, as determined by state officials in concert with local and/or tribal officials. additional details on the EOC can be found at http://www.fema.gov/pdf/government/grant/eoc/fy09_eoc_guidance.pdf.

2. Status of Project:

This is a new development effort.

This is an existing project.

Date first developed: 2002

Date last updated: 2009

FEMA is seeking Office of Management and Budget (OMB) clearance for the EOC.

3. Could the project relate in any way to an individual?¹

No. Please skip ahead to the next question.

Yes. Please provide a general description, below.

The type of information that may be collected and/or retained are the names of organizational Point(s) of Contact, organizational address, organizational email addresses, and additional contact information. No Personally Identifiable Information (PII) is collected outside of the organizational information.

¹ Projects can relate to individuals in a number of ways. For example, a project may include a camera for the purpose of watching a physical location. Individuals may walk past the camera and images of those individuals may be recorded. Projects could also relate to individuals in more subtle ways. For example, a project that is focused on detecting radioactivity levels may be sensitive enough to detect whether an individual received chemotherapy.



4. Do you collect, process, or retain information on: (Please check all that apply)

- DHS Employees
- Contractors working on behalf of DHS
- The Public
- The System does not contain any such information.



5. Do you use or collect Social Security Numbers (SSNs)? (This includes truncated SSNs)

No.

Yes. Why does the program collect SSNs? Provide the function of the SSN and the

legal authority to do so:

<Please provide the function of the SSN and the legal authority to do so.>

6. What information about individuals could be collected, generated or retained?

EOC awards are made by organization, not by individual. The only eligible applicants are SAAs. EOC has four standard federal grant forms: Application for Federal Assistance SF-424, Disclosure of Lobbying Activities SF-LLL, Budget Information - Construction Form SF-424C, and Assurances - Construction Programs SF-424D. Consequently, FEMA collects and/or retains applicant information including:

- * Type of submission;
- * Type of Application;
- * Date Received;
- * Applicant Identifier;
- * Federal Entity Identifier;
- * Federal Award Identifier;
- * Date Received by State;
- * State Application Identifier;
- * Names of Organizational Point(s) of Contact;
- * Employer Identification Number (EIN);
- * Dun & Bradstreet (DUNS) Numbers;
- * Organizational Address;
- * Organizational Email Addresses;
- * Department Name;
- * Division Name;
- * Organizational Telephone and Fax Number;
- * Organizational Investment Justification;
- * Name of Federal Agency;



- * Catalog of Federal Domestic Assistance (CFDA) Number;
- * CFDA Title;
- * Funding Opportunity Number;
- * Competition Identification Number; and
- * Areas Affected by Project.

7. If this project is a technology/system, does it relate solely to infrastructure? [For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)]?

- No. Please continue to the next question.
- Yes. Is there a log kept of communication traffic?
- No. Please continue to the next question.
- Yes. What type of data is recorded in the log? (Please choose all that apply.)
- Header
- Payload Please describe the data that is logged.
- <Please list the data elements in the log.>

8. Can the system be accessed remotely?

- No.
- Yes. When remote access is allowed, is the access accomplished by a virtual private network (VPN)?
- No. Applicants provide application data upon submitting their proposals to FEMA via grants.gov, which is accessible via Internet.
- Yes.

9. Is Personally Identifiable Information² physically transported outside of the LAN? (This can include mobile devices, flash drives, laptops, etc.)

- No.

² Personally Identifiable Information is information that can identify a person. This includes; name, address, phone number, social security number, as well as health information or a physical description.



Yes. PII, as it relates to an individual's employment by an eligible grant entity, is transported outside the LAN (via Internet) and transmitted to grants.gov. FEMA accesses grants.gov to download application data, which includes PII, such as an organization's Point of Contact (POC) name, organizational POC's email address, and organizational POC's telephone number .

10. Does the system connect, receive, or share Personally Identifiable Information with any other DHS systems³?

No

Yes. Please list:

11. Are there regular (ie. periodic, recurring, etc.) data extractions from the system?

No.

Yes. Are these extractions included as part of the Certification and Accreditation⁴?

Yes.

No.

12. Is there a Certification & Accreditation record within OCIO's FISMA tracking system?

Unknown.

No.

Yes. Please indicate the determinations for each of the following:

Confidentiality: Low Moderate High Undefined

Integrity: Low Moderate High Undefined

Availability: Low Moderate High Undefined

³ PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in TAFISMA.

⁴ This could include the Standard Operation Procedures (SOP) or a Memorandum of Understanding (MOU)



PRIVACY THRESHOLD REVIEW

(To be Completed by the DHS Privacy Office)

DATE reviewed by the DHS Privacy Office:

NAME of the DHS Privacy Office Reviewer: <Please enter name of reviewer.>

DESIGNATION

This is NOT a Privacy Sensitive System - the system contains no Personally Identifiable Information.

This IS a Privacy Sensitive System
Category of System

- IT System
- National Security System
- Legacy System
- HR System
- Rule
- Other:

Determination

- PTA sufficient at this time
- Privacy compliance documentation determination in progress
- PIA is not required at this time
- A PIA is required
 - System covered by existing PIA:
 - A new PIA is required.
 - A PIA Update is required.
- A SORN is required
 - System covered by existing SORN:
 - A new SORN is required.

DHS PRIVACY OFFICE COMMENTS