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 (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 from the component Privacy Office, 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 DHSConnect and directly from the DHS Privacy Office via email: pia@dhs.gov, phone: 703-235-0780.

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 (PTA)

SUMMARY INFORMATION

Date Submitted for Review: January 31, 2011

Name of Project: State/Local/Tribal Hazard Mitigations Plans (1660-0062)

System Name in TAFISMA: None

Name of Component: Federal Emergency Management Agency

Name of Project Manager: Kathleen Smith

Email for Project Manager: Kathleen.w.smith@dhs.gov

Phone Number for Project Manager: 202-646-4372

Type of Project:
☐ **Information Technology and/or System.***

☐ **A Notice of Proposed Rule Making or a Final Rule.**

☒ **Form or other Information Collection.**

☐ **Other: <Please describe the type of project including paper based Privacy Act system of records.>**

---

* 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:

Under Title 44 Code of Federal Regulations (CFR) Part 201, the Federal Emergency Management Agency (FEMA) requires State, Tribal and local governments to submit to FEMA for approval hazard mitigation plans. Under the said CFR provision, FEMA requires a mitigation plan to be submitted to FEMA for review and approval in order for the state/local/tribe (entity) to be eligible for certain types of FEMA mitigation grants in the future. The entity is NOT applying for the grants at this stage, but rather FEMA is simply evaluating its plans for sufficiency and likely future eligibility if the entity applies for grants. The regulation requires governments to identify in their plan the natural hazards that impact them, to identify actions and activities to reduce any losses from hazards, and to establish a coordinated process to implement the plan. There is no standard form associated with this information collection. Guidance for the plan is provided in the CFR. The purpose of this information collection is to collect said plans from States, local and Tribal governments as required under. 44 CFR Part 201. The mitigation plan is not entered into any IT system. Mitigation plan is stored in a file cabinet or scanned to a compact disc (CD) for storage. Mitigation plans are not retrieved by Personally Identifiable Information (PII) but are retrieved by State, Local or Tribal government.

2. Status of Project:

☐ This is a new development effort.

☒ This is an existing project.

Date first developed: February 26, 2002

Date last updated: June, 2008

In June, 2008, FEMA received approval from OMB for the continued collection of hazard mitigation plans as required and described under 44 CFR Part 201.

3. From whom 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.

4. 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.>

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

The information collection includes points of contact to allow for correspondence between FEMA and the States, Local, and Tribal Governments submitting the Mitigation Plan. This might include names, addresses, phone numbers and work email addresses.

6. 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.>

7. Does the system connect, receive, or share Personally Identifiable Information with any other DHS systems[1]?

☒ No.

☐ Yes.

Please list:

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

☐ Unknown.

[1] 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.

☒ 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

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

Date reviewed by the DHS Privacy Office: February 15, 2011

Name of the DHS Privacy Office Reviewer: Rebecca J. Richards

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.

☐ PIA is required.

☐ System covered by existing PIA:

☐ New PIA is required.

☐ PIA update is required.

☐ SORN not required at this time.

☐ SORN is required.

☐ System covered by existing SORN:

☐ New SORN is required.

DHS PRIVACY OFFICE COMMENTS NO FORM OR SYSTEM IS ASSOCIATED WITH THIS COLLECTION AND CONTAINS NO PII. THE MITIGATION PLAN IS WRITTEN BASED ON THE GUIDANCE FROM THE CFR. NO PIA OR SORN IS REQUIRED.