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 9

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.

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 2 of 9

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: April 22, 2010

NAME of Project: FEMA Logistics Management Demonstration Program -- Logistics Capability Assessment Tool (LCAT)

Name of Component: Federal Emergency Managment Agency

Name of Project Manager: Ms. Mary Anne Lyle

Email for Project Manager: MaryAnne.Lyle@dhs.gov

Phone number for Project Manager: 202.646.7093

TYPE of Project:

☐ **Information Technology and/or System**▯

▯ 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:

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 3 of 9

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

☒ **Other: Voluntary state program; States self-assess logistics process maturity levels; Purpose of information capture is for state educatio nand continuous improvement, enhanced collaboration, and increasing Federal-to-state common operating picture only. Participation is not required.**

SPECIFIC QUESTIONS

•"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.

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 4 of 9

1. **Describe the project and its purpose:**

   The Logistics Capability Assessment Tool (LCAT) is a maturity model for states to measure disaster logistics planning and response capabilities and identify areas of relative strength and weakness. The LCAT is facilitated through two-day collaborative sessions at states and is co-hosted by state emergency managers and the associated FEMA Region. FEMA provides state emergency management agencies with a detailed analysis report and roadmap for continuous improvement. Designated LCAT questions are used as application review questions for Critical Emergency Supplies (CES) allowable expenses under the State Homeland Security Program (SHSP) and Emergency Management Performance Grant (EMPG). The LCAT is a planning tool focused on building state logistics process maturity over time.

2. **Status of Project:**

   ☐ This is a new development effort.

   ☒ This is an existing project.

   > Date first developed: March 9, 2009

   > Date last updated: April 1, 2010

   > Java-based tool updated for Section 508 Compliance.

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.

   <Please provide a general description of the way the project could relate to an individual.>

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

   ☐ DHS Employees

   ☐ Contractors working on behalf of DHS

   ☐ The Public

---

[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.

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 5 of 9

$\boxtimes$ The System does not contain any such information.

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 6 of 9

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?**

   None

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.

   ☐ Yes.

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 7 of 9

9. **Is Personally Identifiable Information[2] physically transported outside of the LAN? (This can include mobile devices, flash drives, laptops, etc.)**

    ☒ No.

    ☐ Yes.

10. **Does the system connect, receive, or share Personally Identifiable Information with any other DHS systems[3]?**

    ☒ 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 Accreditation[4]?

    　　☐ 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

---

[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.

[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)

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 8 of 9

Integrity: ☐ Low ☐ Moderate ☐ High ☐ Undefined

Availability: ☐ Low ☐ Moderate ☐ High ☐ Undefined

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 9 of 9

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 reviwer.>

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