



**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 7

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: Driver's License Security Grant Program (DLSGP, formerly known as REAL ID)

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: <seeking OMB clearance for FEMA's Buffer Zone Protection 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:

The primary mission of FEMA is to reduce the loss of life and property and protect the Nation from all hazards by leading and supporting the Nation in a risk-based, comprehensive emergency management system of preparedness, protection, response, recovery, and mitigation. One of FEMA's objectives is to prepare America for these hazards by developing and implementing national programs to enhance the capacity of state and local agencies to respond to these incidents through coordinated training, equipment acquisition, technical assistance, and support for Federal, state, and local exercises. FEMA fulfills this mission through a series of grant programs that provide funding to enhance the capacity of state and local jurisdictions to prevent, respond to, and recover from disaster and non disaster incidents.

FEMA's Driver's License Security Grant Program (DLSGP, formerly known as REAL ID) is an important part of the Administration's larger, coordinated effort— known as the Federal Investment Strategy— to strengthen homeland security preparedness against risks associated with potential terrorist attacks. The purpose of DLSGP is to prevent terrorism, reduce fraud, and improve the reliability and accuracy of personal identification documents States and territories issue. FEMA was authorized and appropriated funds for the DLSGP through the FY 2009 Department of Homeland Security Appropriations Bill (Public Law 110-329), the REAL ID Act of 2005 (49 U.S.C. §30301 et seq.) and developed the program reporting using the "Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes: Final Rule," January 29, 2008, 6 CFR Part 37

2. Status of Project:

This is a new development effort.

This is an existing project.

Date first developed: August 1, 2008

Date last updated: August 1, 2009

The program priorities and pool of eligible applicants, among other items such as allowable costs or cost share requirements, can differ by grant year.

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

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



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

The System does not contain any such information.

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.



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?

DLSGP awards are made by organization. Consequently, 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

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.



9. Is Personally Identifiable Information² 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 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

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)



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