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: 9 December 2010

Name of Project: Technical Resource for Incident Prevention (TRIP*wire*)

System Name in TAFISMA: Technical Resource for Incident Prevention (TRIPwire)

Name of Component: National Protection and Programs Directorate

Name of Project Manager: Charlie Payne

Email for Project Manager: Charlie.Payne@dhs.gov

Phone Number for Project Manager: 703-603-4845

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:

The Office for Bombing Prevention (OBP) sponsors the Technical Resource for Incident Prevention (TRIPwire) Portal. The portal serves the bombing prevention community as a consolidated and expert-validated resource of near real-time information on improvised explosives and IEDs, relevant news, and threat alerts.

The purpose of TRIPwire is to provide information regarding the processes by which terrorist groups design, develop, manufacture, deploy, train with, and employ IEDs. Content is available to members of the portal who are individually vetted by the TRIPwire help desk as valid users of the system. The community of interest served by the TRIPwire portal is law enforcement for the purpose of bombing prevention.

By combining expert analysis and reports with relevant documents, images, and video gathered directly from terrorist sources, TRIPwire helps homeland security professionals anticipate, identify, and prevent bombing incidents.

All TRIPwire users are verified members of the U.S. bombing prevention community including homeland and national security officials at the local, state, and federal levels. Analysts review the biographical, professional, and eligibility verification information of registrants, paying particular attention to the primary job function selected, to determine eligibility and access to TRIPwire.

The system does not allow access to individuals unless they are members of one of the above disciplines. DHS may sponsor members of the bombing prevention community outside of DHS and grant access to the system. Access to the system will be restricted to U.S. citizens unless the DHS sponsor provides written approval to waive this restriction.

Much of the information currently available within the government regarding explosive terrorist devices is classified, which restricts access to the information first responders need in the event of such an attack. Because these types of data are relevant to potential terrorist methodologies and operations both abroad and within the homeland, a better holistic understanding of these materials benefits the U.S. Government in general, and specifically, DHS and its constituents at state and local levels.

Portal content is derived from reputable sources, such as established news companies, government publications, and published books. The contractor cross-references content and avoids relying on a single source. SMEs vet the information. Government-sanctioned sources (e.g., The Encyclopedia of Explosives) are also available in TRIPwire. These sources provide context to the terrorist source material and assist users in properly interpreting the portal content. If two information sources give conflicting information, the researchers document that in the user profile.

2. Status of Project:

☐ This is a new development effort.

☒ This is an existing project.

Date first developed: September 26, 2006

Date last updated: 27 October 2010

The October release was a standard monthly release that involved closing several defects and implementing: system enhancements related to the annual re-verification process, a unit mapping tool, and a training module.

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?

TRIPwire users provide their first and last name, email address, professional phone number, business affiliation, mailing address, and supervisor contact information. This information is stored in a secure database. Individual users may elect to disclose or not disclose their contact information via the member directory. The member directory is an internal component of TRIPwire and cannot be accessed outside of the system.

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.

☐ 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

[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.

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

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

Date reviewed by the DHS Privacy Office: January 24, 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: DHS-Wide Portals
  - ☐ New PIA is required.
  - ☐ PIA update is required.
- ☐ SORN not required at this time.
- ☒ SORN is required.
  - ☒ System covered by existing SORN: DHS/ALL-002, DHS/ALL-004
  - ☐ New SORN is required.

DHS PRIVACY OFFICE COMMENTS