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, 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 (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: May 4, 2010

NAME of Project: First Responder Communities of Practice (FR CoP)

Name of Component: Science and Technology

Name of Project Manager: King Waters

Email for Project Manager: King.Waters@dhs.gov

Phone number for Project Manager: 202.254.6766

TYPE of Project:

☒ **Information Technology and/or System***

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

☐ **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:

DHS S&T Directorate's First Responder Technologies (R-Tech) program is developing a secure web application to provide the nation's First Responders with a platform they can use to collaborate on important issues that affect the safety and security of the nation. The First Responders Community of Practice (FR CoP) application will serve federal, state, local and tribal First Responders in fostering information sharing, communication, collaboration and innovation. The system will be owned by DHS S&T and hosted at a DHS data center. The system will be operated by S&T and S&T contractors, who will have access to system user registration data.

Status of Project:

☐ This is a new development effort.

☒ This is an existing project.

Date first developed: 12/11/2009

Date last updated:

December 2009: system initial ATO.

2. 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.

FR CoP is a social networking and collaboration site specifically designed to connect First Responders with one another. Users will be identified by their "real" name and not an alias/username within the system (joe.smith for example). Additionally, users will provide their first and last name, their First Responder discipline (Firefighter, Police, EMT, etc.), First Responder Organization (employer name), First Responder Retirement status, job title, professional (job location) city, state, zip, and email address when they register. Lastly, users will have the optional ability to associate an image/photo with their profile.

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

[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.

☒ 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?

First name, last name, First Responder discipline (e.g. Firefighter, Police Officer, EMT), First Responder Retirement status, First Responder Organization (employer name, e.g. NYPD, Mayberry Fire & Rescue), job location/professional city, state, zip code, phone number, and email address. This information will be retained in the FR CoP database for six years or until no longer necessary for all users that submit a registration form, regardless of whether or not the submitting individual is ultimately approved for an FR CoP user account. The purpose of this is to assist vettors in determining if a new registration is being submitted by a prospective user that has previously been rejected. Users will also be asked to choose a number of "security questions" and provide the answers to the system. The questions will be used in the event the user needs to reset their password. Lastly, users will have the optional ability to associate an image/photo with their profile.

Aside from these obvious data points, the system, by nature, will facilitate "open" collaboration and information sharing and therefore any individual user may potentially provide additional information about themselves, their professional experience, work location/experience, etc. (though what exactly can/should be provided is covered in the system's Rules of Behavior which will be read and acknlowdged before any user account is granted). Any additional information (to include profile photo, phone, bio, associations, certifications and interests) a user would voluntarily provide to the system will be disclosed only to other FR CoP users of their choosing through connection requests (initiated by the user themselves or another user). Each user can approve or deny connection requests to control who

can view their voluntary information. Once connected with another system user, the individuals Connected Profile (which consists of full name, email, first responder retirement status, organization, title, city, State, discipline, and any other volunteered information) will be disclosed to the allowed user (adding to the list of any existing user to which they are connected).

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. Can the system be accessed remotely?

☐ No.

☒ Yes. When remote access is allowed, is the access accomplished by a virtual private network (VPN)?

☒ No. The FR CoP information system is available on the Internet to the general public (pending identification and authentication for priveledged areas).

☐ Yes.

8. Is Personally Identifiable Information[2] 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.

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

☒ No

☐ Yes. Please list:

10. 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.

11. 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)

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: June 23, 2010

NAME of the DHS Privacy Office Reviewer: Rebecca 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

☒ A PIA is required

☒ System covered by existing PIA: DHS-Wide Portals PIA

☐ A new PIA is required.

☐ A PIA Update is required.

☒ A SORN is required

☒ System covered by existing SORN: DHS/ALL-004; DHS/ALL-002

☐ A new SORN is required.

DHS PRIVACY OFFICE COMMENTS

For more information on the vetting process see earlier PTA – July 20, 2009