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)

DHS WEB PORTALS

This form is used to determine whether the DHS Web Portals Privacy Impact Assessment (PIA) covers the relevant portal.

Many DHS operations and projects require collaboration and communication amongst affected stakeholders. One method of effectuating such collaboration is the establishment of an online "portal" allowing authorized users to obtain, post and exchange information, access common resources, and generally communicate with similarly situated and interested individuals. DHS has written the DHS Web Portals PIA to document these informational and collaboration-based portals in operation at DHS and its Components, which collect, use, maintain, and share limited personally identifiable information about individuals who are "members" of the portal or who seek to gain access to the portal "potential members."

To determine whether your portal is covered please review the DHS Web Portals PIA, 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 the DHS Privacy Office determines that your portal is covered, the name of your project to Appendix A of the Web Portals PIA. If the Privacy Office determines that your portal is not covered, we will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

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:** February 4, 2011

NAME **of** Project**: CyberFETCH**

Name of Component: Science and Technology

Name of Project Manager: Douglas Maughan

Email for Project Manager: douglas.maughan@dhs.gov

Phone number for Project Manger: 202-254-6145

SPECIFIC QUESTIONS

1. Describe the project and its purpose:

The S&T Cyber Security Division is funding ITT Information Systems to develop and administer the CyberFETCH portals system. CyberFETCH is a secure, web-based portal for computer forensics practitioners, investigators, analysts, and technologists to share and exchange information for cyber-crime related topics. The purpose of the CyberFETCH system is to create a clearinghouse to provide practitioners with an "all-in-one" web-based repository that encompasses state-of-the-art Web 2.0 technology, as well as proven collaborative and useful interfaces. CyberFETCH will only be used for collaborative purposes and to distribute/share information.

ITT Information Systems, the adminstrator, will collect registration information on behalf of S&T Cyber Security. S&T will provide managerial oversight of this system.

2. Status of Project:

☒ This is a new development effort.

☐ This an existing project.

Date first developed:

Date last updated:

<Please provide a general description of the update.>

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

☒ First and Last Name	☒ Email Address
☒ Phone Number	☒ Business Affiliation
☒ Mailing Address	☐ Supervisor Information

☒ Other: The following is requested for new accounts in addition to above information: US Person acknowledgement and Job Title. In the event a user does not provide a organizational email address (if the user provides a hotmail, yahoo, gmail, etc.) the following will be requested: Sponsor Informaiton (existing user) including Name, Email address, phone, and affililation of sponsor.

4. What information is collected for security questions[1]?

[1] The Privacy Office encourages Components to collect non-sensitive PII as an alternative to sensitive PII wherever possible, including for registration purposes. If your Component seeks coverage by this PIA and collects sensitive PII for registration

☐ Mothers Maiden Name

☐ Social Security Number

☐ Date of Birth

☒ Other: No security questions will be asked of users to the portal. When a user enters their email in the forgot password area, the system will email a new password to the email on record. If they changed emails they will need to reregister.

5. **Is the information collected directly from the individuals seeking membership to the informational/collaboration-based portal?**

☒ Yes.

☐ No. Please describe the information source and collection method.

<Please describe the information source and collection method.>

6. **Please describe how individuals are verified during the portal registration process.**

☐ Email Supervisor

☐ Phone Supervisor

☒ Other: Validation of orgnizational affiliation and/or validation via an existing user (Sponsor).

☐ No verification is performed.

7. **Is the personally identifiable information exchanged on the portal limited to members' contact information?**

☒ Yes.

☐ No.

8. **Is the personally identifiable information collected, used, or exchanged limited to the purpose(s) of facilitating registration, providing information to, and collaboration among authorized members?**

☒ Yes.

---

purposes, please consult with the Privacy Office and provide justification for the collection of this information. The Privacy Office will then determine whether the relevant portal may be covered by this PIA.

☐ No.

9. Can web portal member routinely post commercial or publicly available data containing PII?

☐ Yes.

☒ No.

10. Is an appropriate Privacy Act notice (e)(3) statement given to the potential member outlining the uses of personally identifiable information?

☒ Yes. Please attach the (e)(3) statement.

☐ No.

11. Has an Authority to Operate from the Chief Information Security Officer been granted to the portal or to the larger information technology system on which the portal resides?

☒ No.

☐ Yes. Please provide the date of the ATO and indicate the determinations for each of the following:

Confidentiality:	☐ Low	☐ Moderate	☐ High	☐ Undefined
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 REVIEW

(To be Completed by the DHS Privacy Office)

DATE **reviewed by the DHS Privacy Office: February 16, 2011**

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
  - ☐ A new SORN is required.

DHS PRIVACY OFFICE COMMENTS

Program will be added to the Portals PIA appendix.