Privacy Impact Assessment

For

SecurityTouch

Date:
12/28/10

Point of Contact:
Benjamin Terry

System Owner:
Deborah Coleman
Author:
Benjamin Terry

Office of the Chief Information Officer
U.S. Department of Education

1. **System Information. Describe the system** - include system name, system acronym, and a description of the system, to include scope, purpose and major functions.

SecurityTouch, application maintains IT Security Awareness Training & IT Specialized training courses in addition to training records for contractors, interns, and volunteers. SecurityTouch is used to assist in satisfying tracking needs for external users for the Department of Education.

2. **Legal Authority. Cite the legal authority to collect and use this data.** What specific legal authorities, arrangements, and/or agreements regulate the collection of information?

NIST 800-16, NIST 800-50

3. **Characterization of the Information. What elements of PII are collected and maintained by the system (e.g., name, social security number, date of birth, address, phone number)?** What are the sources of information (e.g., student, teacher, employee, university)? How the information is collected (website, paper form, on-line form)? Is the information used to link or cross-reference multiple databases?

SecurityTouch application collects name and work email, Based on guidance provided by the Information Security Officer (ISSO) and the Computer Security Officer (CSO), the individual logs in and creates their own accounts in order to conduct training. Information is not linked or crossed referenced with any other databases.

4. **Why is the information collected? How is this information necessary to the mission of the program, or contributes to a necessary agency activity**. Given the amount and any type of data collected, discuss the privacy risks (internally and/or externally) identified and how they were mitigated.

The SecurityTouch application maintains IT Security Awareness Training & IT Specialized Training courses in addition to training records for contractors, interns, and volunteers. SecurityTouch is used to assist in satisfying tracking needs for external users. The CSO's upon completion of training will retrieve the results in the form of a report/transcript from the Learning Management System (LMS).

5. **Social Security Numbers - If an SSN is collected and used, describe the purpose of the collection, the type of use, and any disclosures.** Also specify any alternatives that you considered, and why the alternative was not selected. **If system collects SSN, the PIA will require a signature by the Assistant Secretary or designee. If no SSN is collected, no signature is required.**

No SSNs are being collected.

6. **Uses of the Information. What is the intended use of the information?** How will the information be used? Describe all internal and/or external uses of the information. What types of methods are used to analyze the data? If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

The SecurityTouch application maintains IT Security Awareness Training & IT Specialized training courses in addition to training records for contractors, interns, & volunteers. SecurityTouch is used to assist in satisfying tracking needs for external users. The CSO's upon completion of training will retrieve the results in the form of a report/transcript from the Learning Management System (LMS).

7. **Internal Sharing and Disclosure. With which internal ED organizations will the information be shared?** What information is shared? For what purpose is the information shared?

The SecurityTouch application intends to disseminate training reports/transcripts to the computer security officers throughout the department.

8. **External Sharing and Disclosure. With what external entity will the information be shared (e.g., another agency for a specified programmatic purpose)?** What information is shared? For what purpose is the information shared? How is the information shared outside of the Department? Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding or other type of approved sharing agreement wit another agency?

Information collected is not shared with external entities.

9. **Notice. Is notice provided to the individual prior to collection of their information (e.g., a posted Privacy Notice)?** What opportunities do individuals have to decline to provide information (where providing the information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent?

The SecurityTouch application is not publicly accessible, therefore no Privacy Notice is required.

10. **Security. What administrative, technical, and physical security safeguards are in place to protect the PII?** Examples include: monitoring, auditing, authentication, firewalls, etc. Has a C&A been completed? Is the system compliant with any federal security requirements?

Monitoring, auditing, and authentication are included to protect user information. The C&A is currently in process expected to be completed early February. The system compliance office (Information Assurance) is in the process of validating federal security requirements that apply.

11. **Privacy Act System of Records. Is a system of records being created or altered under the Privacy Act, 5 U.S.C. 552a?** Is this a Department-wide or Federal Government-wide SORN? If a SORN already exists, what is the SORN Number?

A system of record notice is not needed because the information collected from SecurityTouch is not retrieve by any personal identifiers. Therefore, a system of record as defined by the Privacy Act is not being created and the reporting requirements of OMB Circular A-130 do not apply.

12. **Records Retention and Disposition. Is there a records retention and disposition schedule approved by the National Archives and Records Administration (NARA) for the records created by the system development lifecycle AND for the data collected?** If yes – provide records schedule number:

GRS 23, Item 1, Temporary, cut off annually. Destroy/delete 2 years after employee terminates, separate or retires.