Privacy Impact Assessment (PIA) for the
SecurityTouch Learning Management System (STLMS)

10/22/2018

This PIA was originally approved on Oct 22, 2018 and reviewed on Nov 20, 2018 by the system owner certifying the information contained here is current and up to date.

Contact Point

Contact Person/Title: Deborah Coleman / STLMS System Owner

Contact Email: Deborah.Coleman@ed.gov

System Owner

Name/Title: Deborah Coleman / STLMS System Owner

Program Office: Office of Chief Information Officer (OCIO)

Please submit completed Privacy Impact Assessments to the Privacy Safeguards Division at privacysafeguards@ed.gov.
Please complete this Privacy Impact Assessment (PIA) on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document. If a question does not apply to your system, please answer with N/A.

All text responses are limited to 1,500 characters. If you require more space, please contact the Privacy Safeguards Team.

1. Introduction

1.1 Describe the system including the system name, system acronym, and a brief description of the major functions.

The SecurityTouch Learning Management System (STLMS) is used to provide mandatory cyber security and privacy awareness training and role-based training to users and to provide mandatory cyber security and privacy awareness training to new employees, interns and volunteers. STLMS tracks and reports on completed awareness and role-based training enabling the Department to meet quarterly and annual FISMA reporting requirements.

1.2 Describe the purpose for which the personally identifiable information (PII)¹ is collected, used, maintained or shared.

To comply with Federal laws and regulations, Agencies must provide initial, continuing, and refresher training at the awareness level, policy level, implementation level, and performance level for executives, program and functional managers, information resources managers, security and audit personnel, automated data processing management, operations, and programming staff, and end users. To comply with Federal law including FISMA, agencies must report to the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) on how effectively they are managing their security and privacy programs including data specific to the successful completion of required Cybersecurity Awareness and Role-based Training.

STLMS is used to provide mandatory cyber security and privacy awareness training and role-based training to users. STLMS tracks and reports on completed awareness and role-based training enabling the Department to meet quarterly and annual FISMA reporting requirements.

¹ The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. [https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf](https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf)
1.3 Is this a new system, or one that is currently in operation?  

Currently Operating System

1.4 Is this PIA new, or is it updating a previous version? If this is an update, please include the publication date of the original.  

Updated PIA  
Original Publication Date: 12/28/2010

1.5 Is the system operated by the agency or by a contractor?  

Contractor

2. Legal Authorities and Other Requirements

If you are unsure of your legal authority, please contact your program attorney.

2.1 What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system?

The legal authority to collect and use this data include the, Federal Information Security Modernization Act (FISMA) of 2014 (Title III of Public Law 107-347), OMB Circular A-130, Security of Federal Automated Information Resources, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-16, Revision (Rev) 1, A Role-Based Model for Federal Information Technology / Cyber Security Training and NIST SP 800-50, Building an Information Technology Security Awareness and Training Program.

2.2 Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification? Please answer YES or NO.

Yes
2.2.1 □ N/A If the above answer is **YES** this system will need to be covered by a Privacy Act System of Records Notice(s) (SORN(s)).² Please provide the SORN name and number, or indicate that a SORN is in progress.

Information within the system is retrieved by personal identifier. As a system of records, STLMS is covered by a Federal Government-wide SORN, OPM/Government 1 – General Personnel Records System of Record Notice. Please see: https://www.gpo.gov/fdsys/pkg/FR-2006-06-19/pdf/06-5459.pdf

---

**Records Management**

*If you do not know your records schedule, please consult with your records liaison or send an email to RMHelp@ed.gov.*

2.3 Does a records retention schedule, approved by the National Archives and Records Administration (NARA), exist for the records contained in this system? If yes, please provide the NARA schedule number.

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

---

² A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. [https://connected.ed.gov/om/Documents/SORN-Process.pdf](https://connected.ed.gov/om/Documents/SORN-Process.pdf)
2.4 Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule? Please answer **YES** or **NO**.

Yes

3. Characterization and Use of Information

Collection

3.1 List the specific personal information data elements (e.g., name, email, address, phone number, date of birth, Social Security Number, etc.) that the system collects, uses, disseminates, or maintains.

Data elements collected include the following: Title, first name, middle initial, last name, job role, company name, full address, phone number, time zone, Principal Office, and email address.

3.2 Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2? Please answer **YES** or **NO**.

Yes

3.3 What are the sources of information collected (e.g., individual, school, another agency, commercial sources, etc.)?

A secure web form on the user registration page of the STLMS web application collects the personally identifiable information (PII) from STLMS users.
3.4 How is the information collected from stated sources (paper form, web page, database, etc.)?

A secure web form on the user registration page of the STLMS web application collects the personally identifiable information (PII) from STLMS users.

The SecurityTouch application functionality also includes an import feature which allows application administrators to efficiently create user accounts for employees and contractors by uploading a spreadsheet or comma separated values file containing the same PII data collected through the online user registration page. Additionally, training completion report data from the Talent Management System (TMS) is imported into the SecurityTouch database to consolidate training completion tracking and reporting into a single system. In addition to the information collected during user registration, the TMS import also collects supervisor’s name, sub-office, curriculum name, training status (enrolled, in progress, not completed) and date training completed. The information collected is not used to link or cross-reference multiple databases.

3.5 How is this information validated or confirmed?

A secure web form on the user registration page of the STLMS web application collects information from STLMS users. End user training profiles are accessible for validation by authorized Information System Security Officers (ISSOs) within each Principal Office, the Office of the Chief Information Officer (OCIO)/Information Assurance Services/Policy and Planning Branch personnel that manage the Department’s cybersecurity training program, and contractor personnel that provide Help Desk support services for STLMS.

Examples include form filling, account verification, etc.
Use

3.6 Describe how and why the system uses the information to achieve the purpose stated in Question 1.2 above.

The Department uses the information collected to create and update training accounts for end users, enroll end users into training courses, facilitate the completion of the training course(s), provide end users with completion certificates, communicate with end users, and track and report training completions and failures. In addition, the Department uses the information it collects from end users to confirm the individual’s identity, establish their eligibility for system access, and to provide and monitor system security. Additionally, training completion data for Federal employees is imported from the Department of Interior’s TMS into the STLMS database to consolidate all training records into a single system. This consolidation enables the Department to efficiently track and report training completions and failures as required to comply with mandated FISMA reporting. PII collected or maintained by STLMS is not shared with outside of the Department. SecurityTouch does not utilize data mining to identify previously unknown patterns in the information collected and no tools are used to analyze or produce new data. It does not use commercial information or publicly available information.

3.7 Is the project using information for testing a system or for training/research purposes? Please answer YES or NO.

[ ] NO

3.7.1 [ ] N/A If the above answer is YES, what controls are in place to minimize the risk and protect the data?
3.8 Does the system use "live" PII for the development or testing of another system? Please answer YES or NO.

No

3.8.1 N/A If the above answer is YES, please explain.

Social Security Numbers

*It is the Department's Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.*

3.9 Does the system collect Social Security Numbers? Please answer YES or NO.

No

3.9.1 N/A If the above answer is YES, explain the purpose for its collection, and how the SSN will be used. *Please note if the system collects SSNs, the PIA will require a signature by the Assistant Secretary or equivalent.*
3.10 N/A Specify any alternatives considered in the collection of SSN and why the alternatives were not selected.

4. Notice

4.1 How does the system provide individuals notice about the collection of PII prior to the collection of information (i.e. written Privacy Act notice, link to a privacy policy, etc.)? If notice is not provided, explain why not.

The Department provides notice of its information collection in several ways. First, notice is provided through this Privacy Impact Assessment and the government-wide OPM/Government 1 – General Personnel Records System of Record Notice (SORN). Secondly, the Department provides notice via a Privacy Act Statement, which is included on the SecurityTouch online user registration page. Finally, SecurityTouch states the privacy policy on a dedicated web page.
4.2 □ N/A  Provide the text of the notice, or the link to the webpage where the notice is posted.

URL: https://securitytouch.ed.gov/privacy_policy.k2

4.3 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Prior to a user submitting registration information, the user must agree to the following statement: By submitting your registration information, you indicate that you agree to the Terms of Use and have read and understand the SecurityTouch Privacy Policy.

5. Information Sharing

Internal

5.1 Will information be shared internally with other ED organizations? Please answer YES or NO. If the answer is NO, please skip to Question 5.4.

Yes
5.2 N/A  What information will be shared and with whom?

Access to view end user training profiles and training completion reports is limited to authorized Information System Security Officers (ISSOs) within each Principal Office, the Office of the Chief Information Officer (OCIO)/Information Assurance Services/Policy and Planning Branch personnel that manage the Department’s cybersecurity training program, and contractor personnel that provide Help Desk support services for SecurityTouch.

5.3 N/A  What is the purpose for sharing the specified information with the specified internal organizations? Does this purpose align with the stated purpose in Question 1.2 above?

Information is shared to allow each Principal Office the capability to ensure assigned users are in compliance with the Department’s cybersecurity training program requirement. This aligns with the stated purpose in Question 1.2 above.

External

5.4 Will the information contained in the system be shared with external entities (e.g. another agency, school district, etc.)? Please answer YES or NO. If the answer is NO, please skip to Question 5.8.

Yes
5.5 □ N/A  What information will be shared and with whom? Note: If you are sharing Social Security Numbers, externally, please specify to whom and for what purpose.

Only the total numbers and percentages of personnel trained data is shared. PII collected and maintained by STLMS is not shared with outside of the Department.

5.6 □ N/A  What is the purpose for sharing the specified information with the specified external organizations? Does this purpose align with the stated purpose in Question 1.2 above?

FISMA mandates training information be reported to the Office of Management and Budget (OMB) and the U.S. Department of Homeland Security (DHS). This aligns with the stated purpose in Question 1.2 above.
5.7 □ N/A  How is the information shared and used by the external entity?

The total numbers and percentages of personnel trained data shared is used by OMB and DHS to compile training data for all government users across the federal government.

5.8 □ N/A  Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU) or other type of approved sharing agreement with another agency? Please answer YES or NO.

No

5.9 □ N/A  Does the project place limitation on re-disclosure? Please answer YES or NO.

Yes

6. Redress

6.1 What are the procedures that allow individuals to access their own information?

Users have the ability to access their information via the "User Properties" web page within the STLMS application. This page is accessible via: https://securitytouch.ed.gov/user_properties.k2?accountInfo=1

4 If the system has a System of Records Notice (SORN), please provide a link to the SORN in Question 6.1 and proceed to Section 7 - Safeguards.
6.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Users have the ability to correct and update their information via the "User Properties" web page within the STLMS application. This page is accessible via: https://securitytouch.ed.gov/user_properties.k2?accountInfo=1

6.3 How does the project notify individuals about the procedures for correcting their information?

STLMS users are informed on the STLMS homepage that their account username must be identical to their ED Network email address and if they are not certain if they have been assigned an ED Network account and email address, to contact their Contracting Officer’s Representative (COR) before registering for a STLMS account. If users currently have an ED Network account and are using a personal or company provided email address to access STLMS, users are advised to contact the STLMS helpdesk. Additionally, users have the ability to contact STLMS support personnel via the email address stated in the Privacy Policy.

7. Safeguards

*If you are unsure which safeguards will apply, please consult with your ISSO.*

7.1 Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible? Please answer **YES** or **NO**.

Yes
7.2 What procedures or access controls are in place to determine which users may access the information and how does the project determine who has access?

The Department of Education Handbook for Information Assurance Security Policy is the overarching security policy for all IT systems. Section 4.1 identifies personnel security policies. The OCIO also publishes the Handbook for Personnel Security-Suitability Program for more detailed guidance. The Director of Information Assurance Services is responsible for ensuring that IT personnel security policy is developed, maintained, and distributed to Department of Education personnel. The Department of Education, Office of Management, also provides the Clearance of Personnel for Separation or Transfer and the Contractor Employee Personnel Security Screenings that provide additional guidance for each of these groups. The Office of Management, Chief of Personnel Security is responsible for maintaining and distributing guidance for government employees and contractors that has access to Department of Education facilities, IT systems or information.

In accordance with ED’s access control policies, STLMS user access is granted based on the need to know and the least privilege required to perform his/her duties. Specific technical privileges are limited to those specifically required for a specific job or an individual’s position.

7.3 What administrative, technical, and physical safeguards are in place to protect the information?

Administrative, technical, and operational security controls required by NIST SP 800-53, Rev 4 for a Federal Information Processing Standards (FIPS) low impact system are implemented as described in the System Security Plan; security control assessments have been successfully completed by the Department’s independent Security Control Assessors, STLMS has been granted an Authority to Operate by a Department Authorizing Official, and continuous monitoring performed to ensure the risk of operating the system remains acceptable.

STLMS enforces the concept of least privilege through a role-based access system, according to the user roles described in the LMS System Characterization Document. STLMS does not utilize temporary/guest accounts. Each level provides the user with access to certain areas of the system. By default, newly-registered users have User (Student) access and can only view the student home page. To obtain a higher level of access, the user must contact the Campus Manager.

STLMS locks users out after 3 unsuccessful logon attempts. Lockout duration is set to “Forever” to require administrator intervention for all locked-out accounts.

The system administrator monitors and tracks invalid logon attempts to ensure that security violations and breaches are investigated and pursued.

Non-registered/non authenticated users by default are only allowed to see the home page and any other pages created by the administrator which are flagged as public content.

7.4 Is an Authority to Operate (ATO) required? Please answer YES or NO.

Yes

7.5 Is the system able to provide account of any disclosures made? Please answer YES or NO.

Yes
7.6 Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by federal law and policy? Please answer YES or NO.

Yes

7.7 Has a risk assessment been conducted where appropriate security controls to protect against that risk been identified and implemented? Please answer YES or NO.

Yes

7.8 Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the controls continue to work properly at safeguarding the information.

STLMS system performs audit monitoring, analysis and reporting. Currently, the Cisco ASA firewall provides IDS/IPS functionality and sends alerts if suspicious traffic to the STLMS is detected and/or blocked. STLMS logs user activities and retains an audit trail at the page level. Failed login attempts are logged along with the IP address and browser information. The audit trail follows users from page to page including user ID and IP address information. The audit logs are accessed by system administrators from within STLMS. STLMS administrators are responsible for configuring and administering the firewall to block unwanted traffic and to protect STLMS from unauthorized access from the Internet. All unauthorized functions, ports, protocols, and/or services are prohibited. STLMS administrators conduct internal and external network vulnerability scans at monthly intervals and after any significant change in the network. Networks and systems are also monitored by an intrusion detection/prevention system that alerts personnel of potential compromises. The intrusion detection/prevention system is constantly monitored and security events evaluated as they occur by the STLMS system administrators. Testing of the STLMS Contingency Plan is an essential element of a viable contingency capability and is conducted at least annually. This enables plan deficiencies to be identified and addressed prior to implementation during an actual disruption or disaster. Each element of this plan is included in the testing schedule to confirm the accuracy of individual recovery procedures, the effects on Departmental operations and assets, and the overall effectiveness of the plan.

8. Auditing and Accountability

8.1 How does the system owner ensure that the information is used in accordance with stated practices in this PIA?

A risk assessment is conducted for STLMS system as part of the certification and authorization process. Risk assessment activities include reviewing STLMS documentation, interviewing designated STLMS management and technical personnel, and observing controls where STLMS is physically located. The vulnerabilities identified during the risk assessment of the system will be assigned a risk level of high, medium, or low. This qualitative risk assessment approach enables STLMS management to make informed risk-based business decisions.

System owners/managers are required to update risk assessments at least every three (3) years or whenever there is a significant change to the system, the facilities where the system resides, or other conditions that may impact the security or authorization status of the system as required by OMB A-130. The system owner/manager may acquire a third party to conduct the assessment, or use in-house personnel.
8.2 What are the privacy risks associated with this system and how are those risks mitigated?

Privacy risk are minimized due to the non-sensitive nature of the PII collected, such as would be found on a business card. Risks are mitigated by complying with NIST 800-53 Rev. 4 privacy controls in conjunction with the Department of Education privacy and security guidance.

Additionally, in accordance with OMB Memorandum 03-22, STLMS is required to conduct a PIA because the system collects individual’s name, address and email address of individuals that access the system. A PIA is conducted to meet this requirement.

Finally, a risk assessment is conducted for the STLMS system as part of the certification and authorization process. Risk assessment activities include reviewing STLMS documentation, interviewing designated STLMS management and technical personnel, and observing controls where STLMS is physically located. The vulnerabilities identified during the risk assessment of the system will be assigned a risk level of high, medium, or low. This qualitative risk assessment approach enables STLMS management to make informed risk-based business decisions.