

U.S. Department of Commerce OS



Privacy Threshold Analysis for the Commerce Learning Center (CLC)

U.S. Department of Commerce Privacy Threshold Analysis

OS/Commerce Learning Center (CLC)

Unique Project Identifier: Contract No.: SS1301-17-BU-0002, Order No. SS130117CC0033

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system: *Provide a brief description of the information system*

The E-Government Act of 2002 defines “information system” by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: “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).

The Commerce Learning Center (CLC) is the learning management system used by the Department of Commerce and its bureaus. The system manages instructor led training by providing a mechanism for creating courses, scheduling classes, and registering users for those courses. The system also tracks instructors and rooms that are used for training. In addition to managing instructor led training, the system also provides access to online courses. The system supports processing of external training requests via Standard Form (SF) 182 Authorization, Agreement and Certification of Training, and allows for entry of training records completed outside of the system. The CLC provides the capabilities of reporting on how training is configured within the system, trainings completed, and assigned trainings not completed. The system can also send email notification to remind users of training events and required training not completed.

In order for the system to provide this functionality, the system stores training information (courses, training rooms, instructors, and training completion history), non-sensitive personally identifiable information (PII), and human resource (HR) information.

a) Whether it is a general support system, major application, or other type of system

The CLC is a Major Application used to support training management and training record keeping for DOC and its bureaus.

b) System location

The physical location of the system is managed by Cornerstone, who uses the Equinix data centers. The production system is located in El Segundo, CA and the disaster recovery site is located in Ashburn, VA.

- c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*

The CLC is a standalone system that does not currently interconnect with systems. Data is populated in this system via a manual data feed process.

- d) *The purpose that the system is designed to serve*

This system serves in administering human resources programs by the delivery, maintenance and reporting of agency training and training initiatives.

- e) *The way the system operates to achieve the purpose*

The following functions can be performed within CLC to achieve its purposes:

1. Employee Registers for Instructor Led Training
 - a. Employee logs into system.
 - b. Employee searches for training.
 - c. Employee registers for training.
2. Employee Completes Online Course
 - a. Employee logs into system.
 - b. Employee searches for online training. Otherwise, the training may be assigned to the employee.
 - c. Employee launches online training by selecting the link to start the online course.
 - d. Employee completes online course.
3. Employee Requests External Training
 - a. Employee logs into system.
 - b. Employee completes SF-182. The online SF-182 does not capture the Social Security Number (SSN) or Date of Birth (DoB). The employee is tracked via User ID which is his/her email address.
 - c. Employee submits SF-182.
 - d. Supervisor reviews request as well as other individuals (second tier supervisor, training administrators, financial approvers) and approves or denies the request.
 - e. Employee completes post-course survey after successful completion of course.
4. Administrator Creates Training
 - a. Administrator logs into system.

- b. Administrator inputs supporting information for course including provider, room information, and instructor information.
 - c. Administrator creates course including information such as course description, target audience, subject areas, and related competencies.
 - d. Administrator creates session for course if led by instructor, including dates, times, and locations where the course session will be offered.
- 5. Administrator Runs Learning History Report
 - a. Administrator logs into system.
 - b. Administrator chooses report to run.
 - c. Administrator chooses criteria for report, such as users and courses to include.
- 6. Office of Personnel Management (OPM) Enterprise Human Resource Integration (EHRI) Data Management
 - a. Administrator logs into system.
 - b. Administrator chooses report to run.
 - c. Administrator chooses criteria for report, including training related data feeds from the system.

f) A general description of the type of information collected, maintained, use, or disseminated by the system

The personal information collected in this system includes Employee ID, Name, , , Email Address, Occupation, Job Title, Work Address and Telephone Number. This system also maintains training courses/details, training transcripts (assigned, in progress, completed and archived) and training reports (run by administrators). The PII on this system will only be used for the purposes of tracking training.

g) Identify individuals who have access to information on the system

The information in this system is accessed by all DOC employees and approved contractors and outside partners. These users are limited to only seeing their own data. In addition, trained administrators have access to the data based upon what they need to perform their specific job functions.

h) How information in the system is retrieved by the user

Users login to the system over an encrypted link that is secured by TLS 1.2, 1.3. or single sign on from the user's respective bureau.

i) How information is transmitted to and from the system

Information is transmitted to and from the system over an encrypted linked secured by TLS 1.2, 1.3, RSA with 256 key exchange and AES256.

Questionnaire:**1. Status of the Information System****1a. What is the status of this information system?**

_____ This is a new information system. *Continue to answer questions and complete certification.*

_____ This is an existing information system with changes that create new privacy risks.
Complete chart below, continue to answer questions, and complete certification.

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

_____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

 X This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment. *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

_____ Yes. This is a new information system.

_____ Yes. This is an existing information system for which an amended contract is needed.

_____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

 X No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

_____ Yes. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

☒ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

☐ Yes, the IT system collects, maintains, or disseminates BII.

☒ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

☒ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

☒ DOC employees

☒ Contractors working on behalf of DOC

☐ Other Federal Government personnel

☐ Members of the public

☐ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

☐ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
--

Provide the legal authority which permits the collection of SSNs, including truncated form.

☒ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

☒ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

☐ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

☐ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

☒ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

 X I certify the criteria implied by one or more of the questions above **apply** to the Commerce Learning Center (CLC) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

 I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Gary Haney Office: Enterprise Services Phone: 202-482-1691 Email: ghaney@doc.gov Signature: _____ Date signed: _____	Information Technology Security Officer Name: Densmore Bartly Office: Office of the Chief Information Officer Phone: 202-482-3186 Email: DBartly@doc.gov Signature: _____ Date signed: _____
Privacy Act Officer Name: Tahira Murphy Office: Office of Privacy and Open Government Phone: 202-482-8075 Email: tmurphy2@doc.gov Signature: _____ Date signed: _____	Authorizing Official Name: Lawrence W. Anderson Office: Office of the Chief Information Officer Phone: 202-482-2626 Email: LAnderson@doc.gov Signature: _____ Date signed: _____
Bureau Chief Privacy Officer Name: Maria Dumas Office: Office of Privacy and Open Government Phone: 202-482-5153 Email: mdumas@doc.gov Signature: _____ Date signed: _____	Empty space for signature and date