U.S. Department of Commerce

Privacy Impact Assessment
for the
Commerce Learning
Center (CLC)
April 24, 2018

Reviewed by: Michael Toland, Bureau Chief Privacy Officer

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CATRINA PURVIS

Digitally signed by CATRINA PURVIS
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2018.05.10 15:31:07 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
Commerce Learning Center (CLC)

Unique Project Identifier: Contract No: SS13017 BU-0002, Order No: SS130117CC0033

Introduction: System Description

Provide a description of the system that addresses the following elements:

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

The Cornerstone OnDemand (CSOD) Next Generation Learning Management System (NGLMS) is the learning management system for DOC 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 provides access to online courses. The system supports processing of external training requests via Standard Form (SF) 182, Authorization, Agreement and Certification of Training. The system allows entry of training records completed outside of the system. The system provides the capabilities of reporting on how training is configured within the system, training completed, and assigned training not completed. The system can also send email notifications to remind users of training events and required training not completed. The system may eventually allow name and email information to be transferred from other HR systems, such as the National Finance Center (NFC).

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.

(b) System location

The physical location of the system is managed by Cornerstone. Cornerstone uses Equinix data centers, and the production system is located in Equinix El Segundo, California. 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).

There are internal and external interfaces as shown in the table below.

Internal / External	URL
Internal	client.csod.com

Internal	client-stage.csod.com
Internal	client-pilot.csod.com
External	https://doc.csod.com/client/doc/default.aspx

In order to enable the WebEx functionality, the CLC is required to have open connectivity over ports 80 and 443 for the following domains:

- webex.com
- webexconnect.com
- all the sub-domains of webex.com and webexconnect.com

(d) The way the system operates to achieve the purpose(s) identified in Section 4

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.

(e) 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.

(f) How information is transmitted to and from the system

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

(g) Any information sharing conducted by the system

Reports generated from this system are shared within the bureaus and the department to manage compliance training. Managers and training administrators have access to the reports. Training completion data and metrics are sent to OPM as required

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107. Executive Order 13197 empowers OPM to collect the personnel data in EHRI.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

Moderate

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.

_____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

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.

X___ This is an existing information system in which changes do not create new privacy risks, and this Privacy Impact Assessment serves as a recertification (version 01-2015 or later). *Skip questions and complete certification*

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID	X	g. Passport		k. Financial Transaction	
d. Employee ID	X	h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify): DOC MASTER ID (OS generated number used to uniquely identify employees throughout the Department). The PII data will be used to associate users with training registrations and training histories. The PII data will also be used to contact employees to follow up on completing training and other learning and development activities. The PII data will be used to manually transmit EHRI data to OPM.					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias	X	i. Home Address		o. Medical Information	
d. Gender	X	j. Telephone Number		p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity	X	l. Education	X	r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): Occupational series, pay plan, grade, Personnel Office Identifier (POI), Entry On Duty date, Entry On Position Date-, supervisory code, supervisor email, user type, instructional program, country code, duty county name, agency code, Education Level					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	d. Queries Run	X	f. Contents of Files	
g. Other system administration/audit data (specify): Actions taken within the system, such as modifying training events and records.					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	X
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

The accuracy of the information in the system is protected using various security integrity controls as documented in the CLC and Cornerstone Unified Talent Management Suite (CUTMS) System Security Plans. Additionally, there is *DOC NGLMS: Human Resource (HR) Data Management Plan* to ensure that the data from data sources are processed according to a repeatable process.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

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

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters		To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated

will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The PII on the system will be used only for the purpose of administering training to Department of Commerce employees, contractors, and outside partners.

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Possible Threats to Privacy Include:

- Malicious insiders who have privileged access could obtain user PII and post it on a public facing Internet site.
- An adversary could break into the system through unknown methods/zero day exploits and steal PII.
- An adversary could break into the system through unknown methods/zero day exploits and change existing PII.
- In working on a support issue, an Administrator could inadvertently email PII to another Administrator over the Internet in the clear.

The Department of Commerce recognized that PII is a liability, and therefore it only collects the minimum amount of PII necessary for employees to be legally employed at the Department. Since PII is limited to only that which is specifically required, the attack surface has been minimized.

Threats to privacy have been mitigated through background checks on employees and through training and built-in security controls.

The system is scanned and patches regularly by Cornerstone.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X	X	
DOC bureaus	X	X	
Federal agencies	X	X	
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify): Partners that are neither contractors or government employees.			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement

	and/or privacy policy can be found at: https://www.commerce.gov/page/privacy-policy .	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Users may choose to not provide PII during application for employment. Users are notified during in processing briefings by their Human Resources department representatives of their option to decline to provide PII. Declining to provide PII effectively declines employment.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Users may choose to not provide PII during application for employment. Users are notified during in processing briefings by their Human Resources department representatives of their option to decline to provide PII. Declining to provide PII effectively declines employment.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: PII data can be updated by employees (email address, office phone, and office address) through their email staff directory.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Activity within the system is tracked by IP address and User ID. Standard IT best practices are in place to monitor access to system databases.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 5/11/17 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
X	Other (specify): Administrators and supervisors of administrators with access to PII will be required to sign a "rules of behavior" document that dictates Standards of Acceptable System Use and Account Approval. These standards apply to all users of OHRM Information Technology (IT) resources and are intended to increase individual awareness and responsibility, and to ensure that all users utilize OHRM IT resources in an efficient, ethical, and lawful manner. Failure to abide by these rules may constitute grounds for termination of access privileges, administrative actions such as disciplinary actions, and/or criminal prosecution, if warranted. All users must read and acknowledge these standards to receive access to OHRM IT resources, including specific provisions outlined in the document.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

The system employs a FedRAMP Moderate control baseline to protect information contained within. HR data files are transferred to CSOD via Secure File Transfer Protocol (SFTP). Databases and backup files are AES256 encrypted. In addition, the files are Pretty Good Privacy (PGP) encrypted

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: General Personnel Records, OPM/GOVT-1, COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: General Records Schedule (GRS) 29.a.1
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	X
Degaussing		Deleting	
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: The system directly identifies all Department of Commerce employees and contractors (approximately 50,000) using names and email addresses.
X	Quantity of PII	Provide explanation: The information system directly identifies all Department of Commerce employees and contractors (approximately 50,000).
	Data Field Sensitivity	Provide explanation:
	Context of Use	Provide explanation:
X	Obligation to Protect Confidentiality	Provide explanation: PII must be protected per the Privacy Act and OMB policies.
	Access to and Location of PII	Provide explanation:

	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Possible Threats to Privacy Include:

- Malicious insiders who have privileged access could obtain user PII and post it on a public facing Internet site.
- An adversary could break into the system through unknown methods/zero day exploits and steal PII.
- An adversary could break into the system through unknown methods/zero day exploits and change existing PII.
- In working on a support issue, an Administrator could inadvertently email PII to another Administrator over the Internet in the clear.

The Department of Commerce recognized that PII is a liability, and therefore it only collects the minimum amount of PII necessary for employees to be legally employed at the Department. Since PII is limited to only that which is specifically required, the attack surface has been minimized.

Threats to privacy have been mitigated through background checks on employees and through training and built-in security controls.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.