Privacy Impact Assessment (PIA)
for the

The LINCS Technology Project
January 11, 2022

For PIA Certification Updates Only: This PIA was reviewed on **Enter date** by **Name of reviewer** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Mary Jo Maralit
Contact Email: maryjo.maralit@ed.gov

System Owner

Name/Title: Mary Jo Maralit
Principal Office: Office of Career, Technical, and Adult Education (OCTAE)

Please submit completed Privacy Impact Assessments to the Privacy Office at privacysafeguards@ed.gov

3.8.1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.

☑ N/A

3.8.2. Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

☑ N/A

4. Notice

4.1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? If notice is not provided, explain why not.

- A link to the website privacy policy appears in the site footer.
- Privacy Impact Assessment is posted on the Department's Notices page for public reference.

4.2. Provide the text of the notice or the link to the webpage where the notice is posted if notice is provided other than by SORN or PIA.

☐ N/A

https://lincs.ed.gov/privacy-policy

4.3. What opportunities are available for individuals to consent to uses (including new uses of previously collected PII), decline to provide PII, or opt out of the project?

Opportunities to consent to uses:

- During login, registered users must review the U.S. Department of Education Standard PR.AC: User-Notification Warning Banner Terms and Conditions. When registered users accept the terms and conditions, they are opting in.
- During registration, users are automatically subscribed to email announcements. Registered users can opt out of receiving announcement by updating the subscription settings in their profile.
- Registered users in LINCS Community must explicitly opt in to receive email messages with group content for the groups they join.

Opportunities to decline to provide PII:

- Users may opt out of LINCS services if they want to provide PII. When accessing the LINCS system as anonymous users, they can view the posts in LINCS Community, but they are not able to participate or engage with LINCS Community members. As anonymous users in LINCS Learning Portal, they cannot enroll in courses.

  Registration is separate for LINCS Community and LINCS Learning Portal. Registered users are not required to register for both services.
- Registered users can decline to provide profile data. It is optional and does not impact their access to LINCS features.

Opportunities to opt out of the project:

- Registered users can opt out of the project by closing their accounts. When registered users close their accounts, the accounts are blocked. On the LINCS Community, any discussions or posted content from blocked users remains. For the LINCS Learning Portal, blocked users become invisible to other users; however their course progress is saved. The only information about these users that remains visible is their chosen display name.
- Registered users can request to have their accounts and created content permanently deleted.
- By default, registered users in LINCS Community are subscribed to email announcements. To opt out, registered users can modify the subscription setting in their user profile.

4.4. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practice, policy, or activities that affect the PII and privacy to ensure that individuals are aware of and can consent to, where feasible, these changes?

Yes

5. Information Sharing and Disclosures

Internal

5.1. Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.

No

5.2. What PII will be shared and with whom?

☑ N/A

5.3. What is the purpose for sharing the specified PII with the specified internal organizations?

☑ N/A

External

5.4. Will the PII contained in the system be shared with external entities (e.g. another agency, school district, the public, etc.)? If the answer is **NO**, please skip to Question 6.1.

No

5.5. What PII will be shared and with whom? List programmatic disclosures only.[4]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☑ N/A

5.6. What is the purpose for sharing the PII with the specified external entities?

☑ N/A

5.7. Is the sharing with the external entities authorized?

☑ N/A

5.8. Is the system able to provide and retain an account of any disclosures made and make it available upon request?

☑ N/A

5.9. How is the PII shared with the external entity (e.g., email, computer match, encrypted line, etc.)?

☑ N/A

5.10. Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement

[4] If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.

with another agency?

☑ N/A

5.11. Does the project place limitation on re-disclosure?

☑ N/A

6. Redress

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

Registered users manage their own account and profile data, and they access the data when they log in to their accounts. (The system uses the user-supplied email address to retrieve account and profile data from the application database.)

6.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Registered users manage their own account and profile data. To correct information, a registered user must log in, and then access, update, and save the user profile settings with the corrected information.

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

After registered users add profile data, they follow the same process to access it again and update it, so no special instructions are required.

Users may contact the LINCS Help Desk for direct user support if needed. The LINCS Help Desk collects email addresses for internal use only. The email address is not required to be the same one used to register for LINCS Community or LINCS Learning Portal.

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?

Yes

7.2. Is an Authority to Operate (ATO) required?

Yes

7.3. Under NIST FIPS Pub. 199, what is the security categorization of the system: **Low, Moderate, or High?**

☐ N/A

Low

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

LINCS is built using virtual computing "instances" within the AWS Elastic Computer Cloud (EC2). The instance data storage volumes make use of the Amazon Elastic Block Store (EBS) that provides encryption for data at rest. LINCS exists in a virtual private cloud (VPC) that provides logical isolation from the rest of the AWS cloud. Frontline firewall protection for instances is provided at the VPC network boundary by a collection of "security groups" in which the protocols, ports, and source IP ranges are defined and blocked/allowed as needed.

The entire AWS EC2 "availability zone" in which the LINCS instances reside (us-east-1) has been certified as FedRAMP compliant. FedRAMP is a U.S. Government-wide program that delivers a standard approach to security assessment, authorization, and continuous monitoring for cloud products and services.

System and application security updates are applied twice monthly. System administrators are trained in PII awareness. Their access is restricted to an as-needed basis, and their privileges are revoked when not needed.

7.5. Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?

Yes

7.6. Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?

Yes

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

- On an ongoing basis, Advanced Intrusion Detection Environment (AIDE) and Open-Source Security Host-based Intrusion Detection System (OSSEC HIDS) monitor system files and logs for anomalies and known issues.
- On a monthly basis, the LINCS team assesses the system using vulnerability scans.
- On a monthly basis, the LINCS team assesses the system using Open Security Content Automation Protocol (OpenSCAP) and Open Vulnerability and Assessment Language/ Common Vulnerability Enumeration (OVAL/CVE).
- On a quarterly basis, the LINCS team audits privileged users.

8. Auditing and Accountability

8.1. How does the system owner assess and ensure that the PII is used in accordance with stated practices in this PIA?

The Drupal platform strongly enforces a set of roles and permissions to ensure that general users do not have access to the PII of others without their explicit permission. Drupal core features allow LINCS site administrators to control which content is visible to each designated user role. Email addresses are visible only to site administrators. For registered users, only display names and information they choose to share is visible to other registered users.

The LINCS management team ensures that the privileged users take annual security and privacy awareness training and agree to U.S. Department of Education Standard PR.AC: User-Notification Warning Banner Terms and Conditions.

8.2. Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

8.3. What are the privacy risks associated with this system and how are those risks mitigated?

This PIA details the privacy controls and safeguards implemented for this system to mitigate privacy risk. These controls and safeguards work to protect the data from privacy threats and mitigate the risks to the data. Additionally, privacy risks have been reduced by only collecting the minimum PII necessary and by not collecting any

sensitive PII. Role-based access controls are implemented to ensure access to data is restricted to authorized users only. Access to monitoring and auditing related documents is limited to Department employees with appropriately approved access authorization.

Privacy risks include unauthorized access to PII in the LINCS system. Access to LINCS privileged user credentials is limited to system administrators only. To protect registered user account information and profile data, which are stored in the application database, the LINCS system has the following safeguards:

- Firewalls
- All applicable safeguards prescribed by the National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev. 4
- Trained system administrators
- Restricted access to production data