Privacy Impact Assessment (PIA)
for the

The LINCS Technology Project
January 11, 2022

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

<u>Contact Point</u>

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

<u>System Owner</u>

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

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.

1. Introduction

1.1. Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

The Literacy Information and Communications System (LINCS) provides evidence-based resources for adult educators at the state and local level to enable them to design and deliver learning opportunities for adults so they can successfully transition to and complete college career pathways leading to 21st century jobs.

The LINCS Technology Project is a system, comprised of public-facing websites with the following components:

- **LINCS** (https://lincs.ed.gov) – Main site for the LINCS Technology Project. Allows open access to a searchable collection of vetted resources for adult education practitioners, resources for teachers and program managers, and links to other LINCS system components. Does not support user registration.
- **LINCS Community** (https://community.lincs.ed.gov) – Open-access community of practice (forum) where adult educators can discuss effective instructional practices and strategies in content-based groups. Requires user registration to access some site content.
- **LINCS Learning Portal** (https://courses.lincs.ed.gov) – Open-access learning platform with over 20 self-paced courses that support professional development for adult education practitioners. Requires user registration to access most site content.
- **LINCS Learner Center** (https://learner.lincs.ed.gov) – Public resources for adult learners that include Federal resources to help them achieve their goals and continue their studies outside the classroom. Does not support user registration.
- **Student Achievement in Reading (STAR)** (https://star.lincs.ed.gov) – Resources and discussion forum for instructors teaching intermediate-level adult learners (grade level equivalent 4.0 – 8.9). Requires user registration to access site content.
- **Adult Education and Family Literacy Act (AEFLA)** (https://aefla.ed.gov) – Public resources to support the AEFLA program, which helps adults get the basic skills they need to be productive workers, family members, and citizens,

including reading, writing, math, English language proficiency, and problem-solving. Does not support user registration.

Each LINCS system component (listed above) is built using a virtual computing "instance" within the Amazon Web Services (AWS) Elastic Computer Cloud (EC2). LINCS exists in a virtual private cloud (VPC) that provides logical isolation from the rest of the AWS cloud.

LINCS Learning Portal and LINCS Community are running the following:

- Red Hat Enterprise Linux (RHEL) with SELinux enabled
- Drupal Content Management System (CMS) engine for dynamic website content and web services
- Moodle Learning Management System (LMS) which provides the courses

The CMS and LMS applications enable site users to access content stored within a backend MySQL database for display within dynamically generated web pages. LINCS components are hosted on virtual machine instances located in the FedRAMP-certified, US-East (N. Virginia) AWS cloud.

With regard to LINCS database connectivity, each LINCS instance has an internal database. LINCS does not connect to any other databases.

To continually improve the user experience, the LINCS Technology Project periodically conducts user research. Research involves the use of a screener survey to identify potential participants, and user interviews to gather data on the user experience.

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

The LINCS Technology Project collects PII from three sources:

1. LINCS Community, a community of practice
2. LINCS Learning Portal, a learning platform
3. User research

[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. OMB Circular A-130, page 33

LINCS COMMUNITY AND LINCS LEARNING PORTAL

These sites collect the minimum PII that is required for user registration, and the PII data is for internal system use only. The LINCS Community and LINCS Learning Portal instances each maintain local records of its registered users. LINCS Community provides single sign-on (SSO) for both sites.

The PII for user registration includes the following attributes:

- **Email address**

  During registration, the user provides an email address, which can be personal or work-related. The system sends a confirmation message to the email address, and when the user clicks the link in the message to confirm the registration, the system activates the registered user account.

  The email address is always stored on the LINCS Community instance because it is the SSO provider, and if the user registered for the LINCS Learning Portal, the email address is also stored locally on that instance to create the registered user account.

  The registered user's email address is not visible to other users. The registered user chooses a display name so that the email address remains private.

  When logging in to the LINCS Community or LINCS Learning Portal, the registered user must provide the email address.

  In addition to authentication, the system uses the email address to send password reset requests, add the user to courses in the LINCS Learning Portal, and send various email notifications based on user activity and notification preferences.

- **Single sign-on password**

  During registration, the user chooses a password, and LINCS Community, the SSO provider, stores the password for authentication to LINCS Community and LINCS Learning Portal.

- **First name, last name**

  The system uses first and last names to address registered users and provide a personalized learning experience. The registered user provides first and last names, but names are not validated for authenticity.

- **LINCS Community display name**

  When registering, users choose a display name so that their email address remains private. The display name is similar to a social media handle in that it does not need to be a realistic name.

Optional profile data

Both LINCS Community and LINCS Learning Portal allow registered users to populate and manage (add/edit/delete) profile data. Each site stores user profiles locally. Profile data is not shared across sites or services. Profile data is not validated for authenticity.

- **LINCS Community**: Profile data is visible only to other registered users, and includes fields for organizational affiliation, interests, "about me", and social media links. While profile data remains restricted to registered users, posts in LINCS Community are public, and post authors are identified using their display names.

- **LINCS Learning Portal**: Profile data is visible only to other registered users who are enrolled in the same course, and includes a profile photo and time zone, as well as a toggle control for showing/hiding the user's email address.

USER RESEARCH

LINCS is also beginning research to better understand our users' experience. This will consist of two parts - a screener survey to identify potential users willing to talk about their experiences with LINCS, and a set of user interviews to better understand users' experiences.

Screener survey

A screener survey is used to identify current and prospective LINCS users as potential participants for one-on-one interviews. When a user research project is being conducted, a link to the screener survey is posted in a discussion forum, in an informational bar on the site, and on social media. Participation is completely voluntary.

The screener survey collects the following information:

- **Email address**
  Users are informed up front in the introductory text that this survey, through Microsoft Forms, is for users who are interested in participating in 25-minute interviews. If they are interested in participating, they can choose to share their email address in the Microsoft Forms survey created by the System Owner's U.S. Department of Education account. All data will be handled through the U.S. Department of Education account and will also be provided as a "responses

spreadsheet" that will be accessible by only the System Owner and the User Experience Design and Research Lead (Contractor).

- **First name, last name**
  If they are interested in participating, they can choose to share their first name and last name in the Microsoft Forms survey created by the System Owner's U.S. Department of Education account. All data will be handled through the U.S. Department of Education account and will also be provided as a "responses spreadsheet" that will be accessible by only the System Owner and the User Experience Design and Research Lead.

User interviews

The purpose of the interviews is that we will use the insights collected from users and potential users of the LINCS site in order to improve user experience and to better understand the features and functionalities that our users would find useful.

During the user interviews, interviewees will be informed that any information they share will be recorded in notes format and as a video recording, and that these interviews will not have their names attached to them. We will, for example, be asking them some version of "Tell me about yourself.", so information shared by the interviewee might include job title, job role, and geographic location. These recordings and interview notes will be stored using a randomized User Interview ID# and will not include their name. The recordings and interview notes will be accessible only by the System Owner and the User Experience Design and Research Lead (Contractor). The User Interview ID# is necessary for the validity of the work, in case in the future, we want to follow-up with someone (for example, to better understand something they said about a particular feature, or to ask them to clarify the context in which they mentioned a particular challenge when it comes to website usage).

The spreadsheet containing User Interview ID#s will be kept only by the System Owner for the duration of the contract (another 4.5 years). The purpose for keeping this data is in support of future research efforts (in case we want to follow up with the same set of participants as the website changes, or in case we want to make sure not to reach out again and overburden people we have already talked to).
After the interviews, the data will be summarized in presentation form, and the summary presentation will be shared with the contractor (IT and UX), OCTAE (Department of Education), and our site content partners. All summary information will only be shared internally to the project team, and we have no plans to share to a broader audience.

1.3. Is this a new system, or one that is currently in operation?

Currently in operation

1.4. Is this PIA new or is it updating a previous version?

This PIA is being updated to include user research projects. The LINCS Technology Project is beginning research to better understand our users' experience and will be introducing screener surveys to identify participants for user interviews. Surveys will be administered using Microsoft Forms. Interviews will be conducted over a secure Zoom account.

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

Contractor

1.5.1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

☑ N/A

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? Please include name and citation of the authority.

Under Title II of the Workforce Innovation and Opportunity Act, Public Law 113-128, Section 242, the Office of Career, Technical, and Adult Education (OCTAE) carries out a program of national leadership activities to enhance the quality and outcomes of adult education and literacy activities and programs nationwide. OCTAE uses these funds to provide technical assistance and professional development to programs, and to contribute to research and evaluations of adult education programs and activities.

SORN

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?

No

2.2.1. If the above answer is **YES,** this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).[2] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

☑ N/A

2.2.2. If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

□ N/A

The system does not retrieve information by name or identifier.

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. What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

- **Login information: GRS 3.2, item 030: System access records, systems not requiring special accountability for access.**
  Retention: Temporary. Destroy when business use ceases.
  Covers: Records created as part of the user identification and authorization process to gain access to systems. Includes: user profiles, log-in files, password files, etc.

- **LINCS Community information: GRS 6.4, item 020: Public correspondence and communications not requiring formal action.**
  Retention: Temporary. Destroy when 90 days old, but longer retention is authorized if required for business use.
  Covers: Records related to correspondence and communication, including comments, to and from the public that require no formal response or action. Includes: personal opinions on current events or personal experiences and

[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

comments posted by the public on an agency website that do not require response or that the agency does not collect for further use.

- **LINCS Learning Portal information: ED 091, item a3: Printed and electronic publications and print materials produced or funded by the Department for internal or external distribution.**
  Retention: Permanent. Cut off at the end of the fiscal year. Transfer to NARA in 5 year blocks when the most recent records are 5 years old.

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

Yes

3. Characterization and Use of Information

Collection

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

For LINCS Community and LINCS Learning Portal, the system collects the following information for internal system use.

- **Email address**
  - During user registration: The user provides an email address (personal or work-related) for registration, and the system uses the email address to send a confirmation message and register the user.
  - After initial registration: The system uses the email address to authenticate the user, send password reset requests, add the user to courses, and send various email notifications based on user activity and notification preferences.
- **LINCS Community password**
  During registration, the user chooses a login password, and the system stores the password and email address as authentication credentials.
- **First name, last name**
  The system uses names to address registered users and provide a personalized learning experience. Names are not validated for authenticity.

Optionally, registered users can populate profile data, such as organizational affiliation, interests, about me, and social media links. Registered users manage their own profile data while logged in to the system, and can add/edit/delete profile data at will.
The LINCS Community component allows Community users to populate their user profiles to enhance the user experience, and as part of online coursework. When registered users add data to their user profiles, the data become visible to other Community users, but are never disclosed or disseminated. Profile data are not validated for authenticity.

While access to user profile data are restricted to registered Community users, posts are public.

Current and prospective LINCS users who volunteer to participate in user research provide their names and email addresses in the screener survey.

3.2. Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2?

Yes

The LINCS Technology Project collects PII from three sources:

1. LINCS Community, a community of practice
2. LINCS Learning Portal, a learning platform
3. User research

LINCS sites collect the minimum PII that is required for user registration, and the PII data is for internal system use only. During user research, the researcher collects the minimum PII required to contact participants by email and coordinate interviews.

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

- **Registered users**: Registered users enter their own account and profile data on the LINCS site. There are no external data sources.

- **Privileged users**: LINCS site administrators provide the names, email addresses, and temporary passwords for new privileged user accounts. Privileged users are either agency employees or contractors and have been approved by the LINCS management team for privileged user access.

(All privileged users take annual security training and agree to U.S. Department of Education Standard PR.AC: User-Notification Warning Banner Terms and Conditions. Privileged users are reviewed on a quarterly basis.)

- **Research participants**: Current and prospective LINCS users who volunteer to participate in user research provide their names and email addresses in the screener survey.

3.4. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, web page, database, etc.)?

- **Registered users**: Users enter their information into a webform on the LINCS site when registering for an account or profile.

- **Privileged users**: LINCS site administrators enter the names, email addresses, and temporary passwords of privileged users directly into the system. Privileged users are either agency employees or contractors and have been approved by the LINCS management team for privileged user access.

- **Research participants**: Current and prospective LINCS users who volunteer to participate in user research provide their names and email addresses in the screener survey. Participants may also share non-sensitive PII during interviews, such as job titles and roles, but all data is anonymized for privacy and objectivity.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[3] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

- **Registered users**: The email address is confirmed during user registration.

  During registration, the user provides an email address, which can be personal or work-related. The system sends a confirmation message to the email address, and when the user clicks the link in the message to confirm the registration, the system activates the registered user account.

  The email address is always stored on the LINCS Community instance because it is the SSO provider, and if the user registered for the LINCS Learning Portal, the email address is also stored locally on that instance to create the registered user account.

  The registered user’s email address is not visible to other users. The registered

[3] Examples include restricted form filling, account verification, editing and validating information as it’s collected, and communication with the individual whose information it is.

user chooses a display name so that the email address remains private.

When logging in to the LINCS Community or LINCS Learning Portal, the registered user must provide the email address.

In addition to authentication, the system uses the email address to send password reset requests, add the user to courses in the LINCS Learning Portal, and send various email notifications based on user activity and notification preferences.

No other information is confirmed or validated for authenticity.

- **Privileged users**: Privileged users are either agency employees or contractors. Before privileged users can be added to the system, the LINCS management team must approve them and identify them for LINCS site administrators who create user accounts.

- **Research participants**: PII is not validated or confirmed. However, the email address that the user provides must be correct in order for the researcher to contact the participant and coordinate the interview.

Use

3.6. Describe how the PII is used to achieve the purpose stated in Question 1.2 above.

The following response duplicates the response to Question 1.2.

The LINCS Technology Project collects PII from three sources:

1. LINCS Community, a community of practice
2. LINCS Learning Portal, a learning platform
3. User research

LINCS COMMUNITY AND LINCS LEARNING PORTAL

LINCS sites collect the minimum PII that is required for user registration, and the PII data is for internal system use only. The LINCS Community and LINCS Learning Portal instances each maintain local records of its registered users. LINCS Community provides single sign-on (SSO) for both sites.

The PII for user registration includes the following attributes:

- **Email address**

  When logging in to the LINCS Community or LINCS Learning Portal, the registered user must provide the email address.

  In addition to authentication, the system uses the email address to send password reset requests, add the user to courses in the LINCS Learning Portal, and send various email notifications based on user activity and notification preferences.

- **Single sign-on password**
  During registration, the user chooses a password, and LINCS Community, the SSO provider, stores the password for authentication to LINCS Community and LINCS Learning Portal.

- **First name, last name**
  The system uses first and last names to address registered users and provide a personalized learning experience.

- **LINCS Community display name**
  When registering, users choose a display name so that their email address remains private. The display name is similar to a social media handle in that it does not need to be a realistic name.

USER RESEARCH

During user research, the researcher collects the minimum PII required to contact participants by email and coordinate interviews.

Screener survey

A screener survey is used to identify current and prospective LINCS users as potential participants for one-on-one interviews. When a user research project is being conducted, a link to the screener survey is posted in a discussion forum, in an informational bar on the site, and on social media. Participation is completely voluntary.

The screener survey collects the following information:

- **Email address**
  Users are informed in the introductory text that the survey is for users who are interested in participating in 25-minute interviews. If they are interested in participating, they can choose to share their email address in the Microsoft Form created using the U.S. Department of Education account. All survey data is contained in the U.S. Department of Education Microsoft Form account and is also provided as a “responses spreadsheet” that is accessible only to selected project team members.

- **First name, last name**
  If users are interested in participating in the survey, they can choose to share their first name and last name in the Microsoft form created by the U.S. Department of Education account. All survey data is contained in the U.S. Department of Education account and is also provided as a "responses spreadsheet" that is accessible only to selected project team members.

User interviews

During interviews, participants are informed that any information they share will be recorded in notes format and as a video recording, and that these interviews will not have their names associated with them. The interview will include a question like "Can you tell me about yourself", so the participant's response might include job title, job role, and geographic location.

Recordings and interview notes are stored using a User Interview ID# so as to keep names private. Data is accessible only to selected project team members.

3.7. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

3.7.1. If the above answer is **YES,** what controls are in place to minimize the risk and protect the data?

☑ N/A

Click here to enter text.

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.

3.8. Does the system collect Social Security Numbers? Note that if the system maintains Social Security Numbers but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

No

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