Privacy Impact Assessment (PIA)

for the

Adobe Sign

October 3, 2023

Point of Contact

Contact Person: Vijay Sharma
Title: Deputy Director, Office of the Chief Information Officer/Information Technology Program Services
Email: Vijay.Sharma@ed.gov

System Owner

Name: Vijay Sharma
Title: CTO
Principal Office: Office of the Chief Information Officer

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

FY 2022

*Please complete this **Privacy Impact Assessment (PIA)**, which describes 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, answer with N/A.

- **Please ensure all responses are written in plain language. Write out all acronyms on first use and use acronyms consistently thereafter.**

- **For questions that are identical to those in the Privacy Threshold Analysis (PTA), please review the responses provided in the most recently approved PTA, determine whether the responses remain accurate, and, if so, use the same response in the PIA.**

1. Introduction

1.1. Describe the project or program that uses this information technology (IT) system, including the purpose of the project or program.

Adobe Sign is a FedRAMP-approved, cloud-based electronic signature platform used by the U.S. Department of Education (Department) that allows individuals and organizations to securely sign, send, and manage digital documents. It also provides advanced features such as automated workflows, document tracking, and audit trails. Adobe Sign will be used by the Department for a variety of documents that require signature.

Adobe Sign will allow the Department to create, send, track, and manage digital signatures and to streamline workflows. Adobe Sign will be used to augment current email-based or manual processes that create and track the status of documents and document signatures.

1.2. How does the IT system function to support the project or program as described in Question 1.1?

When uploading and preparing a document for signature, Adobe Sign is accessed through a web portal by Department employees and contractors, with access managed through the Department's Active Directory. Through the web portal, users can add signature fields to existing documents, create email routing chains for documents that require multiple signatures, and design workflow templates that allow similar signature processes to be created and repeated.

The Department's implementation of Adobe Sign has the ability to integrate with development tools such as Appian or UiPath. These low-code applications and software automation products provide Adobe Sign with documents that are pre-filled with application data, or they can use the signed documents to trigger new actions, for example, employee account creation.

Adobe Sign enables users outside the Department to access documents they are requested to sign. Once a signing workflow has been applied to a document, Adobe Sign will route the document to each recipient via email and provide the document owner with emailed status updates as the document moves through the signature workflow. When a recipient receives an email, they will follow a link contained within the email to the Adobe Sign web portal to access the document. The recipient can view the document, fill in any necessary fields, and sign electronically. After signing, Adobe Sign saves the signed document and notifies the document owner that the signing process is complete. Recipients may also view statuses of documents through the web portal and set up email notifications for reminders of outstanding document actions.

1.3. What are the technical elements and/or components of the IT system? Mark all that apply.

☒ Website	☒ Portal	☒ Application
☐ Database	☐ Server	☐ Other (Specify Below)

If you have been directed to "specify below," describe the type of technical elements and/or component:

1.4. Describe the purpose for which the Personally Identifiable Information (PII)[1] is created, collected, used, processed, stored, maintained, disseminated, or disclosed by the IT system. If there is more than one type of individual from whom PII is collected (e.g., grantees, parents, Federal employees, contractors), specify the purpose for each type of individual.

When the recipient signs a document using Adobe Sign, their name, email address, and Internet Protocol (IP) address are collected. Adobe Sign uses this information to establish an audit trail for the signature, thereby ensuring the authenticity of the document and enabling it to provide legally binding signatures. Additional PII potentially could be used or maintained within the Adobe environment when it is deemed necessary by the document owner to be included on a document requiring signature.

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

Contractor

[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

1.6. If the IT system is operated by a contractor, describe the contractor's role in operating the system.

Adobe owns and operates Adobe Sign. It is responsible for managing the infrastructure of the system.

- **Software Development and Maintenance:** Adobe develops and maintains the Adobe Sign software. They provide capability updates and bug fixes to the Adobe Sign application.
- **Infrastructure Management & Security:** Adobe manages the web portal and back-end servers to provide the Adobe Sign capability, including management of the environment's security.
- **Compliance:** Adobe maintains the Adobe Sign Authorization to Operate under a FedRAMP package.

☐ N/A

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

Yes

☐ N/A

2. Legal Authorities and Other Requirements

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

2.1. What specific legal authorities permit and regulate the collection and use of data by the IT system? Include name and citation of each authority.

The content of documents signed using Adobe Sign can be subject to different legal authorities depending on the specific information within each document. The legal implications, requirements, and authorities governing a document are largely determined by its content and context. For instance, an employment agreement could be governed by labor laws, and student transcripts may be covered under FERPA. Therefore, while Adobe Sign provides a platform for secure, legally binding digital signatures, the legal authority pertaining to the signed documents' content varies based on the nature and context of the individual document.

System of Records Notice (SORN)

2.2. Has the Department's Privacy Program determined that the PII maintained by the IT system is or will be maintained as part of a Privacy Act system of records? Refer to the "SORN" item in the "Privacy Program Determination" section of the PTA if unsure.

☐ Yes

☒ No

2.3. If yes, provide the full name(s), number(s), and Federal Register citation of the applicable SORN(s) and/or a statement indicating that a new or modified SORN is being prepared.

☑ N/A

Records Management

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

2.4. Is there an applicable records retention schedule(s) for the information maintained in the IT system? Note: If no records schedule is in place or you are unsure of the applicable records schedule, reach out to your records liaison or the Records Management Office.

☒ Yes, there is/are approved records retention schedule(s) for the information. List the schedule(s):

All records generated by this application that document the workflow to complete forms, including completed forms, must be systematically emailed to content creators in PDF format. Once received in the Department's email application, MS Office 365, the appropriate records disposition schedule will be applied, and final disposition will be managed by the Office of the Chief Information Officer (via the Department Records Officer) and the content creator(s). To ensure Adobe Sign does not become a recordkeeping system, all content in the application will be considered "duplicate" and be deleted only after it is emailed to the content creator and when it is no longer needed for business use or auditing purposes (e.g., 90, 120, 180 days).

☐ No, there are currently no approved records retention schedules, but there is a proposed schedule or plan to establish a schedule. Explain:

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

☒ Yes

☐ No

3. Information Collection, Maintenance, Use, and/or Disclosure

Collection

Select the types of PII that are collected, maintained, used, and/or disclosed by the IT system. **Note:** PII includes any information that is linked or linkable to an individual, including business or contact information, information that is publicly accessible elsewhere, and ordinarily non-sensitive information.

Biographical and Contact Information

☒ Name	☒ Date of Birth	☒ Gender or Sex
☒ City, State, or County of Birth	☒ Country of Birth	☒ Home Address
☒ Personal Phone Number	☒ Work Phone Number	☒ Personal Email Address
☒ Work Email Address	☒ Work Address	☒ Personal Fax Number
☒ Work Fax Number	☒ Digital Signature ☒ Hand Signature	☒ Mother's Maiden Name

Other Demographic Information

☒ Citizenship and/or Alien Registration Number (A-Number)	☒ Military Service	☒ Marital Status, Spouse, and/or Child Information (Specify below)
☒ Educational Background/Records	☒ Group/ Organization Membership	☒ Employment Information
☒ Physical Characteristics or	☒ Race/Ethnicity	☒ Religion

Biometrics (Height, Weight, etc.)		

Identification Numbers

☒ Social Security Number	☒ Truncated/Partial Social Security Number	☒ Driver's License Number
☒ Passport Number	☒ Employee Identification Number	☒ Professional License Number
☒ Credit/Debit Card Number	☒ Bank/Financial Account Number	☒ Personal Device Identifiers/Serial Numbers
☒ License Plate Number	☒ File/Case ID Number	☒ Federal Student Aid Number
☒ Student ID Number	☒ Student Loan Number	☒ Grant Number
☒ Other ID That Can Be Traced to Individual (Specify below)		

Electronic and Miscellaneous Information

☒ Username/User ID	☒ Password	☒ IP Address
☐ MAC Address	☒ Complaint Information (Specify below)	☒ Medical Information (Specify below)
☐ Location Data	☒ Log Data That Can Be Traced to Individual	☐ Photographs of Individuals
☐ Videos of Individuals	☐ Criminal history	☒ Other (Specify below)

If you have been directed to "specify below," describe the PII: Any information contained in documents processed through Adobe Sign will be maintained on the system.

3.1. Select the category of individuals from whom information is collected, maintained, used, or disclosed by the IT system and, if applicable, list what information from Question 3.1 is collected from each. Check all that apply:

☒ Federal Employees

Specify types of information collected from Federal employees:

Name, email address, IP address, digital signature.

Additional information collected will vary by user and by the types of documents that require signature. Any information contained in documents processed through Adobe Sign will be maintained on the system.

☒ Federal Contractors

Specify types of information collected from Federal contractors:

Name, email address, IP address, digital signature.

Additional information collected will vary by user and by the types of documents that require signature. Any information contained in documents processed through Adobe Sign will be maintained on the system.

☒ General Public (Any individual not employed by the Department).

Specify categories of the general public (e.g., teachers, students, parents, institution representatives, grantees, State and local government employees), and the types of information collected from each:[2]

From members of the general public signing documents through Adobe Sign: name, email address, IP address, digital signature.

The specific PII elements will depend on the particular document that is required to be signed. Adobe Sign will capture signatures and will assign access to users based on their email address. However, based on each user's activity any of the information types in question 3 could be included in documents that require signature.

3.2. What are the sources of PII collected, maintained, used, or disclosed by the IT system (e.g., individual, school, another agency, commercial sources)?

When utilizing Adobe Sign, there is the potential for individuals, schools, or other entities to utilize Adobe Sign to sign documents initiated by the Department. When these entities use Adobe Sign to sign documents, the PII will be made available to the system as part of that process. For example, the Department will utilize Adobe Sign to obtain signatures on certain documents related to grants administered by the Department's grants office. These documents include the Grant Award Notification (GAN) signed during the obligation procedure and the External Payee Access Form.

- The **GAN signing process** will use Adobe Sign to send a generated GAN document to Adobe Sign for digital signature. Once the GAN document is signed by the user, the document is retrieved from Adobe Sign to the Department's G5 grant system for further processing.

[2] For example:
From students: name, email address, phone number.
From institution representatives: name, email address, username, password.

- The **External Payee Access Form** will be automated using Adobe Sign. The Department's G5 system will use an External Payee Access Form template existing in Adobe Sign to send the form to an external user and obtain their signature.

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

The mode of data collection depends on the specific PDF document that is requested to be signed. The more common modes of data collection include web-based data collection tools, paper forms, and sharing of information with Department partners. When the recipient signs a document using Adobe Sign, their name, email address, digital signature, and IP address are collected. Adobe Sign uses this information to establish an audit trail for the signature, thereby ensuring the authenticity of the document and enabling it to provide legally binding signatures.

3.4. Privacy law and policy generally requires agencies to collect or maintain only the minimum amount of PII necessary to accomplish an authorized purpose. For each of the PII elements that are indicated in Question 3.1, please describe why the information is necessary.

Adobe Sign allows users to sign their PDF documents electronically. Users can upload their custom PDFs into the Adobe Sign platform, after which they can designate signature fields and specify signatories. Once the document is prepared, recipients receive an email notification prompting them to affix their electronic signatures. The platform ensures the security, authenticity, and validity of the signature while maintaining the integrity of the original PDF document. The only PII that will be processed or stored by Adobe Sign is the data that is required to process the PDF form. Each document owner is responsible for determining the specific types of PII that will be contained within the PDF.

When the recipient signs a document using Adobe Sign, their name, email address, and IP address are collected. Adobe Sign uses this information to establish an audit trail for the signature, thereby ensuring the authenticity of the document and enabling it to provide legally binding signatures.

3.5. Who can access the information maintained in the IT system?

☒ Federal Employees
☒ Federal Contractors
☒ General Public (Any individual not employed by the Department)

3.6. How is the PII validated or confirmed to ensure the integrity or quality of the information (e.g., form restricting, verifying newly collected information matches previously collected information, account verification, periodically requesting system users verify their own information in the system)?

Adobe Sign authenticates a user's digital identity to ensure that the person interacting with the platform is who they claim to be. When a user initiates a signing process or creates an Adobe Sign account, the platform sends a verification email to the user's registered email address. Users must click a link or enter a code to their email to confirm their identity.

The content of documents signed using Adobe Sign can be different based on the subject of the document itself. It is the responsibility of the document owner to validate the integrity and quality of information that is contained within each document that is required to be signed through Adobe Sign.

Information Use for Testing

3.7. Is the PII maintained in the IT system used for internal testing, training, and researching new applications or information systems?

No

3.7.1. If the above answer to question 3.9 is **YES**, are you authorized to use PII when such information is used for internal testing, training, and research?

☑ N/A

Click here to select.

3.7.2. If the above answer to question 3.9 is **YES,** what controls are in place to minimize the privacy risk and protect the data?

☑ N/A

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 IT system collect or maintain Social Security numbers (SSNs)?

Yes

3.8.1. If the above answer to question 3.10 is **YES**, cite the authority for collecting or maintaining the SSNs.

☐ N/A

Adobe Sign allows users to sign their PDF documents electronically. Users can upload their custom PDFs into the Adobe Sign platform, after which they can designate signature fields and specify signatories. However, the SSN maybe maintained within a document that is requested to be signed. The authority and purpose for the collection of the SSN is delineated in the applicable PIA for the respective source system. Each document owner is responsible for determining the specific types of PII that will be contained within the PDF.

3.8.2. If the above answer to question 3.10 is **YES**, explain the purpose for the collection/maintenance and how the SSNs are used.

☐ N/A

Adobe Sign allows users to sign their PDF documents electronically. Users can upload their PDFs into the Adobe Sign platform, after which they can designate signature fields and specify signatories. In some instances, documents may contain a person's SSN for various purposes. Each document owner is responsible for determining the specific types of PII and purposes of the PII that will be contained within the PDF.

3.8.3. If the above answer to question 3.10 is **YES**, specify whether the collection of the SSNs is mandatory or voluntary. What are the consequences for the individual of not providing the SSN, if any?

☐ N/A

Adobe Sign allows users to sign their PDF documents electronically. Users can upload their PDFs into the Adobe Sign platform, after which they can designate signature fields and specify signatories. In some instances, documents may contain a person's SSN for various purposes. Each document owner is responsible to discern whether the SSNs on their forms is a mandatory or voluntary requirement.

3.8.4 If the above answer to question 3.10 is **YES**, specify any alternatives to SSNs that were considered and explain why they were not used.

☐ N/A

Adobe Sign allows users to sign their PDF documents electronically. Users can upload their PDFs into the Adobe Sign platform, after which they can designate signature fields and specify signatories. In some instances, documents may contain a person's SSN for various purposes. Each document owner is responsible to have considered alternatives to the use of SSNs and to ensure that SSNs are only used when absolutely necessary, and no viable alternatives exist.

4. **Notice**

4.1. How does the IT system provide individuals with a privacy notice about the collection, maintenance, use, and disclosure of PII prior to its collection? For example, does the IT system provide a Privacy Act Statement (if applicable) or other privacy notices provided at the point of collection? If a notice is not provided, explain why not.

Use of Adobe Sign to gather a signature is initiated through another integrated source system. Therefore, Adobe Sign does not provide a privacy notice to individuals about whom it collects PII. Individuals are provided notice by the integrated source systems from which the document owners retrieve information and send the request for signature via Adobe Sign. Notice is provided through the publication of Department SORNs for those systems, which are available at: https://www2.ed.gov/notices/ed-pia.html, as well as notice about the collection and use of their information, as appropriate, at the point at which it is collected. Additionally, this PIA serves as notice with respect to the collection, use, and disclosure of PII. For further reference, the Department PIA website is located at https://www2.ed.gov/notices/pia/index.html.

4.2. If you, or a partner, maintain a program website that is not hosted on the ed.gov domain and is accessible to the public, does the program website have a webpage privacy policy?

Yes

4.3. Provide a link to the webpage where the privacy notice referenced in Question 4.1 is posted. If there is no publicly accessible link, provide the text of the privacy notice. Do not include security banners, security notices, Paperwork Reduction Act statements, or other notices not specifically related to privacy.

☐ N/A

https://www.adobe.com/privacy/policy.html

4.4. What opportunities are available for individuals to consent to uses of their PII, decline to provide PII, or opt out of the project? If these options are not available, state why not.

Individuals do not have the ability to consent to additional uses, decline to provide information, or opt out of their information being maintained in Adobe Sign. Opportunities to decline to provide PII or opt out are at the initial point of collection. If a user does not create an account or sign into Adobe Sign to digitally sign a document, the action may be deemed incomplete and further processing may cease. See section 4.1 for additional information.

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

N/A

5. Information Sharing and Disclosures

Internal

5.1. Is PII maintained in the IT system shared internally with any other Department IT system(s) and/or principal offices? If the answer is **NO**, skip to Question 5.4.

Yes

5.2. Which categories of PII from Question 3.1 are shared and with which Department IT system(s) and/or principal offices?

☐ N/A

See the response for question 3. Any information contained in documents processed through Adobe Sign will be maintained on the system and could be shared with Department principal offices who are responsible for the documents that are requested to be processed through Adobe Sign.

5.3. What is the purpose for sharing the specified PII with each Department IT system(s) and/or principal office specified in Question 5.2?

☐ N/A

The Department may share comments internally with Department principal offices who are responsible for the documents that are requested to be processed through Adobe Sign, upon request from the authorized Department staff and in connection with their duties.

External

5.4. Is PII maintained in the IT system shared with any external entities (e.g., another agency, grantee, school district, the public)? If the answer is **NO**, skip to Question 6.1.

Yes

5.5. Which categories of PII from Question 3.1 are shared and with whom?

☐ N/A

See the response for question 3. Any information contained in documents processed through Adobe Sign will be maintained on the system and could be shared with external Department partners, who are responsible for the documents that are requested to be processed through Adobe Sign. Document owners are responsible for ensuring that any sharing of information external to the Department is in accordance with the routine uses stipulated in the Department's SORNs, which are available at: https://www2.ed.gov/notices/ed-pia.html.

5.6. What is the purpose for sharing the PII with each external entity specified in Question 5.5?

☐ N/A

Any sharing of information of documents processed through the Adobe Sign system varies by the mission of the program offices and is within the scope of the Department's governing statues and regulations. Document owners are responsible for ensuring that any sharing of information external to the Department is in accordance with the routine uses stipulated in the Department's SORNs, which are available at: https://www2.ed.gov/notices/ed-pia.html.

5.7. What are the specific authorities that authorize sharing the PII with the external entities specified in Question 5.5?

☐ N/A

Any sharing of information of documents processed through the Adobe Sign system varies by the mission of the program offices and is within the scope of the Department's governing statues and regulations.

5.8. Does the IT system maintain an accounting of any disclosures made to an external entity?

☐ N/A

Yes

5.8.1. If so, is the accounting of disclosures made to external entities available in response to a Privacy Act request?

Yes

5.9. How is the PII shared with the external entity (e.g., encrypted email, transport layer security (TLS) line)? Specify whether the PII is encrypted in transit and state the encryption method that is used.

☐ N/A

5.10 Is the sharing conducted pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with the external entities?

☐ N/A

Yes

5.11 Does the project allow for the PII to be redisclosed by the external entities or require the external entities to request permission prior to its redisclosure? If so, describe the limitations on redisclosure and how they are documented and enforced.

☐ N/A

Yes

6. Redress

6.1. What are the procedures that allow individuals to access their own information in the IT system? If there are no such procedures, state why not.

The individual will need to coordinate with the document owner to access the data on the form. Please review the PIAs for source systems for further information about accessing and correcting information in those systems.

Alternatively, individuals can download a copy of the form from the Adobe Sign application.

6.2. What procedures are in place to allow individuals to correct or amend inaccurate or erroneous information?

The individual will need to coordinate with the document owner to amend the data on the form. Please review the PIAs for source systems for further information about accessing and correcting information in those systems.

6.3. How does the program or IT system notify individuals about the procedures for accessing or correcting their information?

The document owner is responsible for notifying individuals about the procedures for accessing or correcting information. Please review the PIAs for source systems for further information about procedures to access and correct information in those systems.

7. Safeguards

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

7.1. Does the principal office work with their ISSO to build privacy and security safeguards into the IT system?

Yes

7.2. Is an authorization to operate (ATO) required for the IT system?

Yes

7.2.1. If the answer to Question 7.2 is **YES**, does the IT system have an active ATO?

Yes

7.3. What is the NIST Federal Information Processing Standard 199 security categorization of this IT system?

☐Low

☒Moderate
☐High

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

Access to information in Adobe Sign is protected by the Department's Single Sign On (SSO) service provided by the Enterprise Identify, Credential, and Access Management (ICAM) system.

Adobe Sign implements a multi-faceted approach to ensure the protection of information. The protection mechanisms are categorized into administrative, technical, and physical safeguards.

Administrative Safeguards:

- **Policies and Procedures:** Adobe Sign has established policies and procedures to protect user data. This includes guidelines for data access, handling, and disclosure.
- **Training:** Periodic training sessions are conducted to ensure that all employees know the privacy policies and the significance of data protection.
- **Access Controls:** Role-based access ensures that only authorized individuals can access specific data, based on their job functions.
- **Audit Trails:** Regular audits are conducted to monitor and review data access logs and actions, identifying any potential unauthorized access or anomalies.

Technical Safeguards:

- **Data Encryption:** Adobe Sign employs encryption standards, both in transit (as data moves across the internet) and at rest (when stored on servers). This ensures that even if data is intercepted, it remains unreadable to unauthorized parties.
- **Multi-factor Authentication:** Adobe Sign leverages the Department's ICAM SSO multi-factor authentication (MFA) to ensure that only authorized users can access their accounts.
- **Regular Security Patches:** Adobe continuously monitors for vulnerabilities and releases regular patches and updates to safeguard against potential threats. The Adobe Sign FedRAMP package is enrolled in the General Services Administration (GSA) continuous monitoring program.

Physical Safeguards:

- **Data Center Security:** The physical locations where Adobe Sign's servers are housed employ strict security measures. This includes security personnel, surveillance cameras, and biometric access controls to prevent unauthorized entry.
- **Hardware Security:** All the hardware devices are securely stored and have mechanisms to prevent tampering.

8. Auditing and Accountability

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

The system owner works with the Department's Privacy Program to complete a PIA and to ensure the PIA is accurate and updated as required. The system owner also completes the Department Risk Management Framework process to secure an ATO. The system owner works with contractors to ensure the system is being used appropriately and in accordance with the practices detailed in this document. In addition, all Adobe Sign users sign a user agreement that indicates the proper use of the data and the consequences of not following the rules of behavior. User accounts are reviewed by the Office of the CIO annually to ensure only authorized users have access.

8.2. How does the ISO continuously monitor and audit the security and privacy controls to ensure effective implementation and safeguarding of PII?

The Information System Owner safeguards PII by providing oversight of a continuous monitoring program managed by Adobe Sign. This program aims to assess and respond to risks associated with information systems, ensuring that PII remains shielded from current and emergent threats. Adobe Sign is responsible for continuously scanning for, evaluating, and remedying systems vulnerabilities that might compromise PII. The systems must stay updated with the ever-evolving threat landscape and ensure that security controls are consistently effective. Additionally, Adobe Sign is responsible for conducting regular audits and system scans to detect anomalies or unauthorized access. The Information System Owner is responsible for reporting on the status of risks, mitigative measures, and any that may impact the overall risk posture of the system.

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

The main privacy risks associated with Adobe Sign include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII are potentially hazardous to both individuals and organizations. Individual harm may include identity theft, embarrassment, or financial loss. Organizational harm may include a loss of public trust, legal liability, or remediation costs.

The risks are mitigated by the above-mentioned safeguards, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department. To further mitigate this risk, the following safeguards have been implemented:

- **Authentication and Access:** All Department Adobe Sign users are required to maintain valid credentials, be approved for Adobe Sign access, and access the system through the Department's SSO.
- **Monitoring and Auditing:** Adobe Sign is monitored through continuous monitoring. Additionally, the system must maintain accreditation as required by Department policies.
- **Training and Awareness**: Authorized users of Adobe Sign must take annual Department's Cybersecurity and Privacy Awareness (CSPA) training.