PRIVACY IMPACT ASSESSMENT

Bureau of Educational and Cultural Affairs DocuSign Privacy Impact Assessment

1. Contact Information

A/GIS Deputy Assistant Secretary Bureau of Administration Global Information Services

2. System Information

(a) Date of completion of this PIA: September 2021
(b) Name of system: DocuSign
(c) System acronym: DocuSign Federal
(d) Bureau: ECA
(e) iMatrix Asset ID Number: 318427
(f) Child systems (if applicable) and iMatrix Asset ID Number: N/A
(g) Reason for performing PIA:

- ☒ New system
- ☐ Significant modification to an existing system
- ☐ To update existing PIA for a triennial security reauthorization

(h) Explanation of modification (if applicable):

N/A

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?

☒Yes
☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?

☒Yes
☐No

If yes, has the privacy questionnaire in Xacta been completed?

☒Yes
☐No

(c) Describe the purpose of the system:

DocuSign Federal is a cloud Software as a Service (SaaS) that will provide ECA the capability to electronically sign exchange programs and administrative documents remotely. DocuSign Federal will provide users the ability to send, receive and electronically sign documents for/from government agencies, implementing partners, private business, and members of the public. The DocuSign Federal software will be used to support business processes for timely, secure, and accurate submission of government forms.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

PII is collected by DocuSign via forms that request PII for a business purpose. The following list itemizes the PII collected from three groups of individuals.

1. PII about U.S. Citizens (U.S. government employees): Name (Last, First, Middle Names; Suffix), date of birth, work email, work title, work phone number, work address and social security number (SSN).

2. PII about U.S. Citizens (non- U.S. government employees): Name (Last, First, Middle Names; Suffix), date of birth, personal phone number, personal email address, personal home address and social security number (SSN).

3. PII about non-U.S. Citizens: Name (Last, First, Middle Names; Suffix), date of birth, place of birth, citizenship, educational, financial information, work email, work title, work phone number, work address, personal phone number, personal address, personal email, mother's maiden name and medical records.

For the remainder of this PIA, non-U.S. Citizens will not be discussed.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 5 U.S.C. 301 (Management of the Department of State);
- 22 U.S.C. 1431 et seq. (United States Information and Educational Exchange Act of 1948) (Smith-Mundt Act);
- 22 U.S.C. 2451-58, (Mutual Educational and Cultural Exchange Act of 1961) (Fulbright-Hays Act);
- 22 U.S. C. 3921 (Management of Foreign Service);
- 44 U.S.C. Chapter 35 (Paperwork Reduction Act); and
- 22 U.S.C. 2651a (Organization of the Department of State).

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number, etc.)?

☒Yes, provide:

- SORN Name and Number:
  Educational and Cultural Exchange Program Records, State-08; Human Resource Records, State-31; General Personnel Records, OPM/GOVT-1; Speaker/Specialist Program Records, State-65; and Records of the Office of Citizen Exchanges, State-62.

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
  July 30, 2020; July 19, 2013; December 11, 2012; December 10, 2009 and May 31, 2001.

☐No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Office at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov.)

If yes provide (Consolidate as much as possible):

- Schedule number (e.g., (XX-587-XX-XXX)):
  N/A

- Disposition Authority Number:
  See table below

- Length of time the information is retained in the system:
  See table below

- Type of information retained in the system: see table below

Record Type	Disposition Authority Number	Length of Retention (time)	Information Type
Program Records	DAA-0059-2019-0007-0002 (pending approval by NARA)	Permanent. Cut-off at the end of the year, activity, or	Records include, but are not limited to proposals,

		engagement. Transfer to the National Archives 25 years after cut-off.	participant data, organization and institution information (private, foreign, and federal), country information.
Exchange Program Participant Data	DAA-0059-2019-0007-0007 (pending approval by NARA)	Temporary. Cut off at end of fiscal year when grant/cooperative agreement/program ends or birth date of alumni. Destroy or delete when 75 years old.	Participants and grantees such as biographic information and host information; funding, itineraries, and organization information on all institutional grants and cooperative agreements with U.S. not-for-profit institutions for professional, cultural, and youth exchanges.
Speaker/Specialist Program Records	DAA-0059-2019-0007-0015 (pending approval by NARA)	Temporary: Cutoff at end of fiscal year. Destroy 50 years after cutoff.	Records contain biographic information about the speaker/specialist including names, social security and passport numbers, contact information, education and professional experience, financial information, correspondence between the subject, the Department and overseas posts regarding the subjects

			participation in the program; travel itineraries and visa documentation; grant authorization numbers and types; copies of the grant documents; cost and fiscal data; payment vouchers; country clearance telegrams; and, when available, program evaluations and speaker reports.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒Members of the Public

☒ U.S. Government employees/Contractor employees

☒ Other (people who are not U.S. Citizens or LPRs)

(b) On what other entities above is PII maintained in the system?

☐ Members of the Public

☐ U.S. Government employees/Contractor employees

☐ Other

☒ N/A

(c) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☒Yes ☐No ☐N/A

- If yes, under what authorization?
  Collection of SSNs will be necessary consistent with 22 U.S.C. § 1431 et seq. and 22 U.S.C. § 2451-68. More specifically, each form housed in DocuSign is owned by an ECA office. The office form owner designs the form to collect the information desired. If they want to collect SSN, they are required to include a Privacy Act statement stating any additional programmatic authorities permitting the collection of SSN. The authorizing statement is displayed on the respective form(s).

(d) How is the PII collected?

All ECA program forms will be administered through DocuSign. The information collected, including PII, is obtained directly from the users who complete the form. Once the form is complete and the user submits it, it is automatically uploaded into the system.

(e) Where is the information housed?

☐ Department-owned equipment
☒ FEDRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☐ Other

- If you did not select "Department-owned equipment," please specify.

Although the information is not housed on the Department owned equipment, it is Contractor-Owned, Government -Operated (COGO). DocuSign Federal is housed within heavily access-restricted datacenter cages within each facility in geographically diverse locations within the USA. Multiple layers of physical access control, authentication, and authorization are required before personnel or information system components are permitted access. Further, DocuSign Federal has dedicated multi-tenant security appliances and network area storage units to segregate Federal Agency data from other DocuSign customers.

(f) What process is used to determine if the PII is accurate?

The information is verified by the relevant ECA directorates and program offices whose forms are automated in the tool. Users are responsible for ensuring the accuracy of their data and have access to their own information to make corrections or updates as needed.

(g) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

The information is current and is verified by the user submitting the form. For applicable forms, an approver may manually review information and request updates to submitted information directly from the user that submitted the form.

(h) Does the system use information from commercial sources? Is the information publicly available?

The system does not use information from commercial sources nor is it publicly available.

(i) How was the minimization of PII in the system considered?

The ECA Executive Office conducted a bureau-wide in spring 2021 to minimize the collection of PII and safeguard the data in compliance with Department guidelines that required sign off by each Deputy Assistant Secretary. As forms are onboarded into the tool our team conducts an internal review to ensure there is a current Privacy Statement and discuss candidacy for automation or possible alternative solutions.

5. Use of information

(a) What is/are the intended use(s) for the PII?

Information is used to fulfill various business processes across ECA to include exchange programs. Fulfillment of these processes commonly requires the name and contact information (name, e-mail address, phone number). The primary purpose of the PII is for the creation and maintenance of system user accounts. For additional assurance about the identity of the individual, the system uses PII to authenticate recipients before they are able to sign an agreement/document.

(b) Is the use of the PII relevant to the purpose for which the system was designed or for which it is being designed?

Yes. ECA has a business need to improve document signing and workflows, and to implement a solution that supports a heavily telework environment. The information is solely used for requesting and fulfilling information collection as requested by the ECA office.

(c) Does the system analyze the PII stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the PII?

(2) Does the analysis result in new information?

(3) Will the new information be placed in the individual's record? ☐Yes ☐No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?
☐Yes ☐No

(d) If the system will use test data, will it include real PII?

☐Yes ☒No ☐N/A

If yes, please provide additional details.

6. Sharing of PII

(a) With whom will the PII be shared internally and/or externally? Please identify the recipients of the information.

Internal:
No information is shared internally.

External:
No information is shared externally.

(b) What information will be shared?

Internal:
No information is shared internally.

External:
No information is shared externally.

(c) What is the purpose for sharing the information?

Internal:
No information is shared internally.

External:
No information is shared externally.

(d) The information to be shared is transmitted or disclosed by what methods?

Internal:
No information is shared internally.

External:
No information is shared externally.

(e) What safeguards are in place for each internal or external sharing arrangement?

Internal:
No information is shared internally.

External:
No information is shared externally.

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

Pursuant to the Privacy Act, individuals who agree to participate in a Department program are provided with an approved Privacy Act Statement on the form they complete which serves as a notification. The System of Records Notice (SORN) that governs the collection of this provides individuals additional information about how their PII will be utilized.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?

☒Yes ☐No

If yes, how do record subjects grant consent?

The record subject grants their consent by selecting "I consent" in the form and by initialing or signing their name for ECA program or a contract/job offer with the Department.

If no, why are record subjects not allowed to provide consent?

(c) What procedures allow record subjects to gain access to their information?

There are procedures for access and amendment laid out in the covering SORNs, which are cited in the Privacy Act Statement.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

Every ECA project has an assigned Program Officer (PO) with responsibility to update their program and participant information as required when notified by the participant and/or cooperating partners, This may occur via email or even in person at the project kickoff meeting. Additionally, there are procedures for correcting inaccurate information laid out in the covering SORNs.

If no, explain why not.

(e) By what means are record subjects notified of the procedures to correct their information?

Pursuant to the Privacy Act, individuals who agree to participate in a Departmental program are provided with a SORN that outlines procedures on how to correct their information. Program Officers work with the participant to verify and validate PII information if any corrections are necessary.

8. Security Controls

(a) How is all of the information in the system secured?

DocuSign is accessed over a secure HTTPS connection. Completed electronically-signed documents are accessible to the relevant ECA program staff on a need-to-know basis.
Information in the DocuSign Federal cloud is secured at many levels.
1. DocuSign Federal is housed within heavily access-restricted datacenter cages within each facility, with multiple layers of physical access control, authentication, and authorization before personnel or information system components are permitted access. Further, DocuSign Federal has dedicated multi-tenant security appliances and network area storage units to segregate Federal Agency data from other DocuSign customers.
2. Users are validated before they gain access through Single-Sign-On (SSO) via Microsoft Azure AD.
3. Access is limited on the need-to-know basis. The DocuSign Envelope (eDocument) transaction record is only accessible by DocuSign customer support staff who is given the eDocument Transaction ID by the agency customer.
4. All DocuSign data at rest and in-transit are encrypted using FIPS 140-2 validated Microsoft Crypto API with AES 256 encryption.

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

System Administrators - are ECA technical team members that have access to the information to create/delete and change/reset accounts.

Business Process Owner - are users that create, manage, and send eDocuments to end users for signature.

General Users – are end users that receive DocuSign forms for signature.

ECA offices that own the business process of the automated documents/templates will have access to relevant completed documents on a need-to-know basis.

(c) Describe the procedures established to limit system and data access to only those individuals who have an "official" need to access the information in their work capacity.

In addition to the security controls listed in question 8(a), DocuSign Federal has roles and responsibilities assigned to every user that limit the information that can be viewed and only users who have administrative privilege and can access the information to create/delete accounts, envelopes and change/reset roles and responsibilities among other capabilities. Access to the completed signed documents will be determined by the business process owner.

(d) How is access to data in the system determined for each role identified above?

System Administrators – Access is determined by the ECA/EX/IT Division Chief. Access to the data on the completed documents are determined by the user.

Business Process Owner - Access is determined by the various ECA Office Divisional Heads. A form is completed, uploaded into the system, emailed and approved by ECA office Divisional Head.

General Users – Access is determined as necessary when DocuSign is utilized to gain signature from general user.

(e) What monitoring, recording, auditing safeguards, and other controls are in place to prevent the misuse of the information?

All PII is encrypted. To prevent the misuse of the information, role-based access is used to ensure that the levels of access are restricted to specific job functions. Privileges are assigned on a need-to-know basis and follow the principle of least privilege.

(f) Are procedures, controls, or responsibilities regarding access to data in the system documented?

☒Yes ☐No

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

Department employees and contractors must complete mandatory Cybersecurity Awareness training (PS800) each year as well as complete Protecting Personally Identifiable Information (PA318) every two years. Similarly, DocuSign Federal requires all personnel and contractors to undergo annual awareness security and privacy trainings upon hire before personnel and contractors are granted access to the DocuSign Federal system.