Affects Members Of the Public?	X

Department of Energy

Privacy Impact Assessment (PIA)

Guidance is provided in the template. See DOE Order 206.1, Department of Energy Privacy Program, Appendix A, Privacy Impact Assessments, for requirements and additional guidance for conducting a PIA: ***https://www.directives.doe.gov/directives-documents/200-series/0206.1-BOrder/@@images/file***

Please complete form and return via email to Privacy@hq.doe.gov

No hand-written submissions will be accepted.

This template may not be modified.

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	10/12/2021
Departmental Element & Site	Department of Energy Bonneville Power Administration (BPA) Portland, Oregon
Name of Information System or IT Project	DocuSign
Exhibit Project UID	BPA is a self-funded Federal agency and is exempt from Exhibit 300 submissions
New PIA ☐ **Update** X	This is an update to the existing PIA

	Name, Title	Contact Information Phone, Email
System Owner	Yvette Gill, JL Supervisory IT specialist	503-230-3947 yrgill@bpa.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Information Owner	Scott Hampton, NSP Manager Supplemental Labor Office	360-418-8293 srhampton@bpa.gov
Local Privacy Act Officer	Candice Palen, CGI CGI Supervisor	503-230-3602 cdpalen@bpa.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Nick Choi, JLS IT Specialist	503-230-5397 hccchoi@bpa.gov
Person Completing this Document	Scott Hampton, NSP Supervisory Contract Specialist	360-418-8293 srhampton@bpa.gov
Purpose of Information System or IT Project	DocuSign is a FedRAMP certified, cloud-based SaaS that provides communication and electronic signature capability used to expedite and improve the quality and efficiency of document processing. BPA's Supplemental Labor Management Office (SLMO), Human Resources (HR), Office of Personnel Security (PerSec) and Non-Government Employee Processing group (Non-Gov) will use DocuSign to enhance the audit trail for documents needed in the onboarding and oversight of BPA's workforce. Update September 2021: Use of DocuSign has expanded to include the following use cases: • Onboarding paperwork for BFTE*, CFTE, Service Contractors and student volunteers (SLMO, HR, PERSEC, Non-Gov) • Background Investigation Upgrades (PERSEC) • Foreign National Paperwork (PERSEC – not using in DS yet but may in the future) • Annual Hard Copy Training for contractors who don't have network access (SLMO) • Energized Facility Key Audit (SLMO, TOZ) • Energized Access Attestations (TOZ) • General Counsel Letters - Signatures (Legal) • Management Representation Letters for Auditors - Signatures (Finance) • Approval Letter to Release Quarterly/Annual Reports (Finance) *Note: BFTE onboarding paperwork is transitioning to USA Staffing, but HR will continue to use DS in special situations like student volunteer onboarding.	

MODULE I – PRIVACY NEEDS ASSESSMENT

	Documents are signed and then extracted and moved to the appropriate Office of Record or location based on the business process the document is supporting. Copies of the documents are stored in DocuSign for one year (365 days) and then purged automatically. Docusign contains SSNs, financial information, DOB, employment information, criminal history, name and contact information.
Type of Information Collected or Maintained by the System:	☒ SSN Social Security number (Onboarding records) ☐ Medical & Health Information e.g. blood test results ☒ Financial Information e.g. credit card number (Onboarding forms ask about federal debt delinquency) ☐ Clearance Information e.g. "Q" ☐ Biometric Information e.g. finger print, retinal scan ☐ Mother's Maiden Name ☒ DoB, Place of Birth (Onboarding forms) ☒ Employment Information (Onboarding forms ask if they have left a job under unfavorable circumstances in the last 5 yrs.) ☒ Criminal History (Onboarding forms ask about criminal history for the last 7 years) ☒ Name, Phone, Address ☒ Other – Please Specify – other information necessary for onboarding such as citizenship status, Selective Service registration status, military service, relatives that work at BPA, federal retirement status, work at other federal agencies.
Has there been any attempt to verify PII does not exist on the system? **DOE Order 206.1, *Department of Energy Privacy Program,* defines PII as** *any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to*	N/A. The above-listed PII is captured on forms that are processed in DocuSign

MODULE I – PRIVACY NEEDS ASSESSMENT

distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.	
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	N/A

Threshold Questions

1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?	Yes
2. Is the information in identifiable form?	Yes
3. Is the information about individual Members of the Public?	Yes
4. Is the information about DOE or contractor employees?	☒ Federal Employees ☒ Contractor Employees

If the answer to **all** four (4) Threshold Questions is "**No**," you may **proceed to the signature page** of the PIA. Submit the completed PNA with signature page to the CPO.

Module II must be completed for all systems if the answer to any of the four (4) threshold questions is "Yes." All questions must be completed. If appropriate, an answer of N/A may be entered.

The goal of the threshold questions is to legitimately and efficiently determine whether additional assessment is necessary. If there is doubt, it is in the System Owner's best interest to complete Module II.

PIAs affecting Members of the Public are posted on the DOE Privacy website. For this reason, PIAs affecting Members of the Public should be written in plain language and at a high level so they are easily understandable and do not disclose sensitive information.

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

1. AUTHORITY **What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?**	Department of Energy Authorization Act, Title 42 United States Code (U.S.C.) section 7101, et. seq. The Bonneville Power Project: *Administrative Authority to Contract* (16 U.S.C. §§ 832a(f), 839f(a)) grants BPA authority to procure contracts to advance the agency's mission. DocuSign allows BPA to more effectively and efficiently on-board contractors hired in line with BPA's mission.
2. CONSENT **What opportunities do individuals have to decline to provide information (e.g. where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?**	The DocuSign system is used to complete onboarding documentation and attestations of task completion, such as required training, key audits and energized access requirements. When a signer opens an "envelope" in the system, a message displays that says "Please read the Electronic Record and Signature Disclosure." The signer must mark "I agree to use electronic records and signatures" to continue. If they elect not to check the box and continue, they may select "Decline to Sign" which will void the envelope. Users can complete hard-copy forms instead, following the instructions of the relevant office – typically their employer or the Supplemental Labor Office, Personnel Security, or Human Capital Management.
3. CONTRACTS **Are contractors involved with the design, development and maintenance of the system? If yes, was the Privacy Order CRD or Privacy Act clauses included in their contracts?**	Yes, supplemental labor contractors (CFTE) access the system and data in the course of their regular jobs. All supplemental labor CFTE operate under master agreements with Privacy Act clauses and non-disclosure attestations. The relevant Privacy Act clauses were included in the contract.

MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS:

How does this project or information system impact privacy?

The privacy impact of DocuSign is assessed as high because of the volume and sensitive nature of PII (including Social Security numbers). The risk rating is used to determine the effect to the individuals should the system's confidentiality, integrity, or availability be compromised.

Confidentiality Factors	Low	Moderate	High
Identifiability			X
Quantity of PII			X
Data Field Sensitivity			X
Context of Use		X	
Obligation to Protect Confidentiality			X
Access to and Location of PII		X	
Overall Privacy Risk			X

Docusign is designed to protect PII and mitigate privacy risk via the following administrative, technical, and physical controls:

• Strict access control enforcement based on need-to-know

5. SORNs

How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?

If yes, explain, and list the identifiers that will be used to retrieve information on the individual.

Data may be retrieved by an identifier, including name.

MODULE II – PII SYSTEMS & PROJECTS	
6. SORNs **Has a Privacy Act System of Records Notice (SORN) been published in the *Federal Register*?** **If "Yes," provide name of SORN and location in the *Federal Register*.**	Yes. The following SORNs are applicable. OPM/GOVT-1: General Personnel Records DOE-28: General Traning Records DOE-43: Personnel Security Files DOE-52: Access Control Records of International Visits, Assignments, and Employment DOE-63: Personal Identify Verification Files
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	No
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	Personal information passed through DocuSign is entered directly by the individual subject.
9. Will the information system derive new or meta data about an individual from the information collected?	No. This system is automating manual paper processes. There will be no additional data gathered or generated, as users will be electronically completing BPA, DOE and OPM forms, rather than manually.
10. Are the data elements described in detail and documented?	Yes. The data gathered is identical to the manual paper process this system replaced. Fields are identified in the system and can be given names to facilitate editing and error-checking.
DATA USE	

MODULE II – PII SYSTEMS & PROJECTS	
11. How will the PII be used?	The PII collected by the system is PII that is: - required by the Personnel Security office and OPM to conduct background checks for BPA badging, - Required for foreign national visit and assignment processing, - Required for annual contractor training, - Required for conducting facility key audits, - Required for conducting energized access authorization requests, - Used for facilitating General Council letters for signature, - Used for facilitating management representation letters for auditors, - Used for approval letters to release financial reports.
12. If the system derives meta data, how will the new or meta data be used? **Will the new or meta data be part of an individual's record?**	No new or meta data is used or derived.
13. With what other agencies or entities will an individual's information be shared?	The PII captured in DocuSign is shared with the National Background Investigation Bureau (NBIB) via Electronic Questionnaire for Investigation Processing (e-QIP), a secure website designed to automate the common security questionnaires used to process Federal background investigations. As part of the DocuSign workflow, onboarding envelopes flow to the contract worker's employer (BPA's supplier) for review and signatures after the contract worker has completed their portion of the onboarding forms. Prior to DocuSign the supplier would hand deliver completed forms to SLMO.
Reports	

MODULE II – PII SYSTEMS & PROJECTS	
14. What kinds of reports are produced about individuals or contain an individual's data?	The DocuSign system has reporting around system usage and metrics (number of envelopes, time and speed of viewing by participating users, reports on who has signed an envelope, etc.). DocuSign cannot generate reports using the data input into the forms.
15. What will be the use of these reports?	BPA's contract with DocuSign provides for an allotment of electronic "envelopes". The reports are used to track the number of envelopes used, so administrators know when to purchase additional envelopes. Additional reporting may include analysis of who is sending envelopes, the speed at which envelopes are being completed, etc.
16. Who will have access to these reports?	All administrators of the system and users who have been granted reporting permissions may run reports on all account-level activity. Users may run reports on their own account activity only.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	N/A, the system cannot locate or monitor individuals.
18. What kinds of information are collected as a function of the monitoring of individuals?	N/A, individuals are not monitored in DocuSign.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	N/A, individuals are not monitored in DocuSign.
DATA MANAGEMENT & MAINTENANCE	
20. How will records about individuals be kept current and verified for accuracy, relevance and completeness? Include PII data collected from sources other than DOE records.	The forms in the system are completed by individuals about themselves. After completion, forms are locked and maintained in an uneditable format.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	N/A - DocuSign system is a cloud based software as a service.

MODULE II – PII SYSTEMS & PROJECTS	
Records Management	
22. Identify the record(s).	DocuSign contains copies of documents that BPA has sent for signing. This includes onboarding documents for BFTE, CFTE, Service Contractors and student volunteers; documents for background investigation upgrades, annual hard copy required training attestations; Energized Facility Key Audits; Energized Facility Attestations; General Counsel letters; Management Representation Letters; Approval letters to release quarterly/annual reports.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	GRS 3.2, Item 030 - System Access Records GRS 5.2 item 020 - Intermediary Records
24. Records Contact	IGLM@bpa.gov
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	The SaaS has implemented role-based access: Administrator, Sender, and Viewer. Access is determined by role and need to know. Individuals who have Sender access can view all envelopes they send and any envelopes the Administrator has given them access to. Viewers may view the envelopes they have access to (typically those envelopes they have been copied on). Viewers may not send envelopes.
26. Who will have access to PII data?	Administrator Sender (limited to the data to which they have access) Viewer (limited to the data to which they have access)
27. How is access to PII data determined?	User access will be restricted. Individuals who need to fill out the forms in order to start work at BPA or maintain their work status at BPA will only be able to access the forms and information they input. BPA personnel who access the information in order to facilitate onboarding and maintenance of personnel will have access to all documents in the system that they have been granted access to. They will be accessing the same information they currently have access to on the paper forms.

MODULE II – PII SYSTEMS & PROJECTS	
28. Do other information systems share data or have access to the data in the system? If yes, explain.	No
29. For connecting information systems, is there an Interconnection Security Agreement (ISA) or other agreement between System Owners to ensure the privacy of individuals is protected?	N/A
30. Who is responsible for ensuring the authorized use of personal information?	The Information Owner
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	YVETTE GILL (Print Name) Digitally signed by YVETTE GILL Date: 2022.11.07 10:41:58 -08'00' (Signature)	
Information Owner	JAMES LONGFELLOW (Print Name) Digitally signed by JAMES LONGFELLOW Date: 2022.11.08 08:16:12 -08'00' (Signature)	
Local Privacy Act Officer	CANDICE PALEN (Print Name) Digitally signed by CANDICE PALEN Date: 2022.11.08 13:59:15 -08'00' (Signature)	
Ken Hunt **Chief Privacy Officer**	William K. Hunt (Print Name) Digitally signed by William K. Hunt Date: 2022.11.03 12:05:50 -04'00' (Signature)	