Affects Members Of the Public? ☒

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	08/09/2022	
Departmental Element & Site	Bonneville Power Administration Portland, OR	
Name of Information System or IT Project	TeamMate BAS-GSS	
Exhibit Project UID	BPA is a self-funded Federal agency and is exempt from Exhibit 300 submissions.	
New PIA □ **Update** ☒	This is an updated PIA. Previous update 05/28/2015.	
	Name, Title	**Contact Information Phone, Email**
Information System Owner	Yvette R Gill, JL	yrgill@bpa.gov 503-230-3947

MODULE I – PRIVACY NEEDS ASSESSMENT

Information Owner	Melissa Gallagher-Reiter Supervisory Internal Auditor (CNV)	360-418-2820 mgreiter@bpa.gov
Local Privacy Act Officer	Candice Palen Privacy Act Officer	503-230-5602 cdpalen@bpa.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Nick Choi Software Development & Ops	503-230-5397 hcchoi@bpa.gov
Person Completing this Document	Reilley Boquist Internal Auditor (CNH)	503-230-5356 rmboquist.bap.gov
Purpose of Information System or IT Project	TeamMate is a repository for supporting documentation (including PII) obtained during an internal review or investigation. The system allows for Internal Audit (IA) to obtain any necessary support without compromising the integrity or privacy of the data. It is utilized solely within IA and external party access is only granted in two cases: (1) requests from the DOE Inspector General and (2) External Quality Review. External Quality Review is an external quality review of IA activity. This review is conducted once every five years by a private auditing firm, with view-only access and a contract and nondisclosure agreement in place. The types of data collected is dependent on the type of review being conducted. Any manner of data *could be* obtained from the audit client and there is the potential for PII. If the PII is absolutely necessary for the review, it will be thoroughly documented and identified within the project. In the event that unnecessary PII is obtained, the auditor will scrub the data to remove any unnessesary information. The most common type of PII collected that will not be scrubbed are unique identifiers within systems (SSN, account numbers, birthdate, etc). Audit makes every attempt to not collect PII but rather just review it within the source system and not keep the data within TeamMate. PII is not retrieved by identifier in the system.	
Type of Information Collected or Maintained by the System:	☒ SSN Social Security number ☒ Medical & Health Information e.g. drug test results ☒ Financial Information e.g. purchase card account numbers	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☒ Clearance Information e.g. "Q"/"L"/"Secret", Position Risk, BI Type (Public Trust, NACI) – We don't store any actual "Q"/"L"/"Secret" data, just a listing of people who have those designations. ☐ Biometric Information e.g. finger print, retinal scan ☐ Mother's Maiden Name ☒ DoB, Place of Birth ☒ Employment Information ☐ Criminal History ☒ Name, Phone, Address ☐ Other – Please Specify
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 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.*	N/A
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?	YES ☒ Federal Employees ☒ Contractor Employees

MODULE I – PRIVACY NEEDS ASSESSMENT

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?**	GAO Government Auditing Standards ("Yellow Book") Section 8.32 states that "auditors must prepare audit documentation related to planning, conducting, and reporting for each audit." Additionally, it is required in Section 8.140 that "auditor should make appropriate individuals and audit documentation available upon request and in a timely manger to other auditors and reviewers."

MODULE II – PII SYSTEMS & PROJECTS	
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)?**	Individuals do not consent specifically with the collection of their information in this system. Consent is derived via collection at source systems.
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?**	This system is housed at BPA. The relevant Privacy Act clauses are included in the contracts for contractors who access the system.

MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS:

How does this project or information system impact privacy?

The unauthorized disclosure of information contained in this system is expected to have a serious adverse effect on individuals' privacy. The system contains highly sensitive PII. Should sensitive PII in the system be compromised, it would result in significant privacy harm to individuals potentially including financial harm, professional harm, embarrassment, harm to personal relationships, and it would damage the trust between individuals and the Federal Government.

The system observes a number of protections to protect privacy and via the Fair Information Practice Principles (FIPPs). The system maintains the minimum PII necessary for its business purpose to mitigate privacy harm. In addition, use of the PII in is limited to clearly defined business purposes.

The focus of TeamMate is to be a repository for supporting documentation (including PII) obtained during an internal review or investigation. This requires requires collection of sensitive PII. Security controls have been implemented and processes are in place to ensure that access is restricted.

TeamMate 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
- System Audits

The ensuing risk to the privacy of individuals is HIGH.

Confidentiality Factors	Low	Moderate	High
Identifiability			x
Quantity of PII		x	
Date Field Sensitivity			x
Context of Use			x
Obligation to Protect Confidentiality			x
Access to and Location of PII		x	
Overall PII Confidentiality Level			x

MODULE II – PII SYSTEMS & PROJECTS

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.**	The data is retrieved by project/audit name. It is not routinely retrieved by a personal identifier. Because records in this system are not routinely retrieved by personal identifier, the Privacy Act does not apply to this system and there is no applicable System of Records. A System of Records Notice is not required.
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*.**	N/A
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	N/A
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	The sources of information vary depending on the objectives of the audit and the issues identified. In circumstances in which PII is collected during an audit, it would typically be found in records that Internal Audit has obtained in a report form a BPA department or organization being audited, and/or potentially any outside entitied containing relevant information.
9. Will the information system derive new or meta data about an individual from the information collected?	No
10. Are the data elements described in detail and documented?	YES, in the System Security Plan

MODULE II – PII SYSTEMS & PROJECTS

DATA USE	
11. How will the PII be used?	PII is not routinely used in the system, as there is no intent to collect any PII. If PII is collected, it is used to perform audit procedures and to potentially support conclusions derived from the information. Internal audit asks that PII not be provided and, whenever possible, attempts to remove or obfuscate the PII before storing it in TeamMate. If unnecessary PII is collected in the course of an audit, Internal Audit will not use it.
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?**	N/A
13. With what other agencies or entities will an individual's information be shared?	None
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	No reports are produced containing PII.
15. What will be the use of these reports?	N/A
16. Who will have access to these reports?	N/A
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	No
18. What kinds of information are collected as a function of the monitoring of individuals?	N/A

MODULE II – PII SYSTEMS & PROJECTS

19. Are controls implemented to prevent unauthorized monitoring of individuals?	N/A
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.	There is no process in place to verify records for accuracy. All records should be verified before entering the TeamMate system, as the records collected are used only in the support of the audit.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	The Information system is on-site
Records Management	
22. Identify the record(s).	The system contains any type of documentation necessary to complete each review. This includes, but is not limited to: word documents, excel files, PDF copies of documents, Power BI Data Analytics, and Visio Process Maps.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	N1-305-07-001-5b, GRS 5.7, item 050 MP-1200 - (Review/Investigation supporting documentation - workpapers) Destroy 6 years after the records are closed. DW-1153 - (A123 testing/reporting) - Destroy 6 years after report submission or oversight entity notice of approval, as appropriate, but longer retention is authorized if required for business use.
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?	A system security plan (SSP) is in place identifying all of the security controls necessary to ensure protection of the information. The SSP and controls were assessed in FY2014 by the Office of Cyber Security. The system received an Authority to Operate in March of 2014.

MODULE II – PII SYSTEMS & PROJECTS

26. Who will have access to PII data?	For each project, the Chief Audit Executive, the CN Management Associate, one to two supervisory auditors, and one to three auditors assigned to the specific audit (access is limited to CN individuals only), will have access to the project and any associated documents which may contain PII. All auditors within Internal Audit may potentially be given access to a project if dictated by business needs. Further the TeamMate Champion and Information Owner have administrative access to view all information within TeamMate (both reside in CN).
27. How is access to PII data determined?	Access to PII data in TeamMate is determined by the specific project or audit, and only those individuals working on a specific audit are gien access to PII data.
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	(Print Name) YVETTE GILL Digitally signed by YVETTE GILL Date: 2023.04.06 10:43:39 -07'00' (Signature)	
Information Owner	(Print Name) MELISSA GALLAGHER-REITER Digitally signed by MELISSA GALLAGHER-REITER Date: 2023.04.25 10:10:21 -07'00' (Signature)	
Local Privacy Act Officer	(Print Name) Candice Palen Digitally signed by Candice Palen Date: 2023.04.25 11:53:03 -07'00' (Signature)	
DOE **Chief Privacy Officer**	(Print Name) Brooke J. Dickson Digitally signed by Brooke J. Dickson Date: 2023.04.06 11:09:16 -04'00' (Signature)	