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	September 8, 2023
Departmental Element & Site	Office of Inspector General
Name of Information System or IT Project	TeamMate AM / Audit and Inspection Management System (TeamMate/AIMS)
Exhibit Project UID	019-000001322
New PIA ☐ **Update** X	

	Name, Title	Contact Information Phone, Email
System Owner	Todd Wisniewski Deputy Assistant Inspector General Office of Cyber Assessments and Data Analytics (CADA)	(412) 386-4157 Todd.Wisniewski@netl.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Alexander Borman Attorney Advisor Office of Counsel to the Inspector General	(202) 586-1653 Alexander.Borman@hq.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Janel Ellison Information System Security Officer Office of Cyber Assessments and Data Analytics (CADA), Technical Support Team	(865) 241-3468 Janel.Ellison@hq.doe.gov
Person Completing this Document	Janel Ellison Information System Security Officer Office of Cyber Assessments and Data Analytics (CADA), Technical Support Team	(865) 241-3468 Janel.Ellison@hq.doe.gov
Purpose of Information System or IT Project	TeamMate/AIMS (often referred to as simply "TeamMate") is used by the Department of Energy (DOE) Office of Inspector General (OIG) to support the OIG's mission as mandated by the Inspector General Act of 1978 of identifying opportunities for cost savings and operational efficiencies in DOE's programs and operations, including the National Nuclear Security Administration, Energy Information Administration, Power Marketing Administrations, and the Federal Energy Regulatory Commission. This is accomplished through audits, inspections, evaluations and allegation-based oversight activities designed to detect, identify, and prevent fraud, waste, abuse, mismanagement and violations of law, regulation, and policy. TeamMate serves as the primary method for the creation of centralized electronic project files, organization of work papers and evidence, and accessibility and retention of information in a manner that satisfies Generally Accepted Government Auditing Standards (GAGAS) of the Government Accountability Office, the standards provided by the Council of the Inspectors General on Integrity and Efficiency (CIGIE), and other requirements. TeamMate streamlines and automates the entire workflow process pertaining to audits, inspections, evaluations and allegation-based oversight activities including: (1) risk assessment; (2) scheduling; (3) planning; (4) execution; (5) review; (6) report generation; (7) trend analysis; (8) committee reporting; (9) records retention; and (10) promoting collaboration among managers and staff. Criminal investigators do not have access to TeamMate. Rather, criminal referrals derived from audits, inspections, evaluations and allegation-based oversight	

MODULE I – PRIVACY NEEDS ASSESSMENT

	activities will be separately predicated and processed in the OIG's iPrism system. Information Flow: The accreditation boundary is within the Office of the Chief Information Officer's (OCIO) Energy IT Services (EITS) managed infrastructure supporting the TeamMate system, including network, servers, database files, as well as TeamMate Suite desktop client applications and web-based applications. The OCIO EITS provides wide area network (WAN) connectivity for DOE. OIG users at 13 DOE offices nationwide leverage this infrastructure to connect to TeamMate centrally. Users establish secure network connections directly from each DOE site's local area network (LAN) or remotely using a virtual private network.
Type of Information Collected or Maintained by the System:	☒ SSN Social Security number ☒ Medical & Health Information e.g. blood test results ☒ Financial Information e.g. credit card number ☒ Clearance Information e.g. "Q" ☒ 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 Any information incidental to audit and inspection fact gathering work. For example, a project file may contain scanned images of government-issued identifications if necessary during an inspection.
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*	PII exists on the system.

MODULE I – PRIVACY NEEDS ASSESSMENT

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

MODULE II – PII SYSTEMS & PROJECTS

1. AUTHORITY **What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?**	• Public Law (PL) 95-452, the Inspector General Act of 1978, as amended [Title 5 United States Code (U.S.C.), Sections 401-424], sets forth authority and functions of the Inspector General and provides authorization to collect and maintain personal information to uncover fraud, waste, abuse, misuse, corruption, criminal acts, or mismanagement relating to DOE programs, operations, facilities, contracts, and information technology systems. • In accordance with DOE O 221.2A, *Cooperation with the Office of Inspector General*, during the courses of audits, inspections, or investigations all DOE employees and contractors must: ○ Cooperate fully and promptly with requests from the OIG for information and data relating to DOE programs and operations; ○ Comply with requests for interviews and briefings and must provide affidavits or sworn statements, if so requested by an employee of the OIG so designated to take affidavits or sworn statements; and ○ Not impede or hinder other employees' cooperation with the OIG. • Additionally, in accordance with DOE O 221.2B, Reporting Fraud, Waste and Abuse to the Office of Inspector General: ○ Employees and contractors must report allegations and/or actual instances of fraud, waste, abuse, misuse, corruption, criminal acts, or mismanagement relating to DOE programs to the OIG; and ○ Supervisors must not impede, discourage, or prohibit employees from reporting such matters directly to the OIG.

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)?**	To effectuate the OIG's mission under the Inspector General Act of 1978, as amended, opportunities are not provided to individuals wishing to withhold or place limitations on investigatory information in the system. This information system is exempt from certain requirements under 10 CFR § 1008.12(a), which provides for an exemption for Investigative Files of the Inspector General (DOE-54). Moreover, 10 CFR § 1008.12(b)(2) provides a broad exemption for investigatory material compiled for law enforcement purposes, including with respect to Allegation-Based Inspections Files of the Office of Inspector General (DOE–83). These exemptions enable the OIG to avoid notifying an individual at the individual's request of the existence of records in an investigative file pertaining to such individual or granting access to an investigative file in certain circumstances.
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. TeamMate is a commercial-off-the-shelf system. However, the OIG pays the vendor for the software and an annual maintenance fee.

MODULE II – PII SYSTEMS & PROJECTS	
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	The compromise of TeamMate's system could have a serious adverse effect on individuals in light of the highly sensitive information the system contains relating to oversight activities of individuals. TeamMate contains sensitive personal information (e.g., SSN, personal financial information, personal health information) as well as negative personal information (e.g., criminal and noncriminal investigatory information). Given the highly sensitive information in this system, if the system is compromised it could create significant harm and embarrassment for individuals including, but not related to, potentially significant reputational harm, professional harm, financial harm, embarrassment relating to the disclosure of personal health information, identity harm, and damage to trust between individuals and the Federal Government. The data in the system is relevant and necessary for the OIG to perform its statutory responsibilities. The OIG has mitigated the risk of a data breach by encrypting data. There are no connecting systems with direct access to the information within the system, which will lower the risk of an indirect data breach from other system. Internally, the system will be strictly controlled, and authorized access to data is strictly limited to the administrator(s) for the system and the individuals assigned to the respective audit, inspection, evaluation, etc. PII will be maintained in accordance with the Privacy Act and DOE requirements, and within applicable Federal records management requirements.
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.**	No, PII cannot be retrieved by an identifier because the information is not indexed or referenced based on unique or identifiable information. Specifically, there are no defined fields or unique identifiers to input or retrieve names and PII data elements (e.g., SSN, DOB, etc). Although PII may be present in the project files, it is not the primary source of data in the system.

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*.**	• Investigative Files of the Inspector General (DOE-54) • Allegation-Based Inspection Files of the Office of Inspector General (DOE-83)
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 are derived from a number of different means. The information is often derived directly from the Department, including its subagencies and components, as well as entities with a relationship with the Department as a contractor/subcontractor and grantee/subgrantee. Additionally, the system could contain information from another federal agency that referred a matter to the OIG, a complaint received through the OIG's Hotline, and information gathered during an investigation. A person or entity may provide their own or another subject's 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?	No
DATA USE	

MODULE II – PII SYSTEMS & PROJECTS	
11. How will the PII be used?	Generally, the PII collected is incidental or generally outside the subject matter in question and is only maintained to support any conclusion reached during the course of an audit or inspection assignment. For example, an inspection of Department hiring practices could result in the OIG collecting records containing sensitive personnel information. While the sensitive personnel information is not the focus of the inspection, such information may be necessary to examine to support any conclusions and recommendations. PII data is not trackable or searchable from within the system and is not captured for that purpose. On an internal level, the identified PII of OIG employees (First and Last name, Email Address) will be used to associate user accounts for system use.
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?	Other Federal agencies may be granted read-only access during the triennial CIGIE peer review process or if required by GAO, DOJ, or FBI, such as during the course of an engagement, investigative matter, or subpoena.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	There are no automated reports produced about individuals. Only in the event an individual was the subject of a review would a summary report be derived from that person's personal data.
15. What will be the use of these reports?	A narrative report would be used only in the event an individual was the subject of a review.
16. Who will have access to these reports?	Access is restricted to OIG management and staff by assigned role on a per project basis determined by the project owners and their respective management. Other Federal agencies may be granted read-only access during the triennial CIGIE peer review process or if required by GAO, DOJ, or FBI, such as during the course of an engagement, investigative matter, or subpoena.
Monitoring	

MODULE II – PII SYSTEMS & PROJECTS	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	No, there is no formal mechanism to collect or track PII for identifying, locating, or monitoring individuals.
18. What kinds of information are collected as a function of the monitoring of individuals?	N/A
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.	In accordance with the standards provided under GAGAS and CIGIE, all information gathered and that is used to support conclusions are to be corroborated with sufficient and reliable sources to ensure that the data is complete, accurate, relevant and balanced. Additionally, prior to publication, all OIG reports and underlying support are reviewed by multiple levels of management and verified by an independent reviewer during a factual accuracy process.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	In order to provide uniformity in the use of information and processes, users access TeamMate information from their DOE provisioned desktops by connecting from the corporate network to the servers residing in the DOE-OCIO managed environment. Consistent use is achieved through recurring user training.
Records Management	
22. Identify the record(s).	Types of OIG records: 1. Audit Records 2. Inspection Records 3. Investigative Records

MODULE II – PII SYSTEMS & PROJECTS	
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	☐ Unscheduled ☒ Scheduled *(cite NARA authority(ies) below)* The OIG follows DOE Records Management Program Administrative Records Schedule 22: Audit/Investigative Records, October 2021, Revision 4 (Authorization Number: N1-434-98-24). Section II governs OIG Records: • Audit Records. (N1-434-00-1, Item 2) • Inspection Records. (N1-434-00-1, Item 3) • Investigative Records. (N1-434-00-1, Item 4) Generally, an initiated project is maintained for 10 years.
24. Records Contact	Alexander Borman (Records Liaison Officer) 202-586-1653 Alexander.Borman@hq.doe.gov
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	Management, technical, and administrative controls are in place to protect the data from unauthorized access, modification, or use. Two-factor authentication is required for access. Remote access is available only through the corporate network through a VPN. After a user successfully logs into a DOE provisioned laptop with full disk encryption using Windows authentication, a connection must be established to the corporate network and then users authenticate to TeamMate to access their assigned projects.
26. Who will have access to PII data?	Access is restricted to OIG management and staff by assigned role on a per project basis determined by the project owners and their respective management. Other Federal agencies may be granted read-only access during the triennial CIGIE peer review process or if required by GAO, DOJ, or FBI, such as during the course of an engagement, investigative matter, or subpoena.
27. How is access to PII data determined?	User access is controlled by assigned role on a per project basis determined by the project owners and their respective management.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	No

MODULE II – PII SYSTEMS & PROJECTS	
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?	Project owners and their respective management are responsible for ensuring proper marking and authorized use of PII.
END OF MODULE II	

SIGNATURE PAGE		
	Signature	**Date**
System Owner	**Todd Wisniewski** **(Print Name)** TODD WISNIEWSKI Digitally signed by TODD WISNIEWSKI Date: 2023.09.22 11:31:38 -04'00' **(Signature)**	
Local Privacy Act Officer	**Alexander Borman** **(Print Name)** Alexander J. Borman Digitally signed by Alexander J. Borman Date: 2023.09.22 11:13:06 -04'00' **(Signature)**	

Chief Privacy Officer	**William K Hunt** **(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2023.09.22 10:45:54 -04'00' **(Signature)**	