Affects Members Of the Public? ☐

**Department of Energy**

# Privacy Impact Assessment (PIA)

## MODULE I – PRIVACY NEEDS ASSESSMENT

| | |
|---|---|
| **Date** | March 9, 2023 |
| **Departmental Element & Site** | Office of Environment, Health, Safety and Security<br>Office of Resource Management<br>Office of Information Management<br>Microsoft Azure |
| **Name of Information System or IT Project** | Reporting and Analytical SharePoint (RASP) |
| **Exhibit Project UID** | |
| **New PIA** [X]<br>**Update** [ ] | |

| | Name, Title | Contact Information Phone, Email |
|---|---|---|
| **System Owner** | Helen Heupel, Office of Information Management | 301-903-9031;<br>Helen.Heupel@hq.doe.gov |
| **Local Privacy Act Officer** | Raymond Holmer<br>Office of Environment, Health, Safety & Security, EHSS-72, | 301-903-7325<br>Raymond.Holmer@hq.doe.gov |
| **Cyber Security Expert** reviewing this document (e.g. ISSM, CSSM, ISSO, etc.) | Krystal Harne<br>EHSS ISSO<br>Office of Environment, Health, Safety and Security | 301-903-8283;<br>Krystal.Harne@hq.doe.gov |
| **Person Completing this Document** | Andrew Snow<br>EHSS Cyber Security Point of Contact<br>EHSS-72 | 703-789-6385;<br>Andrew.Snow@hq.doe.gov |

# MODULE I – PRIVACY NEEDS ASSESSMENT

| | | |
|---|---|---|
| | Contractor to DOE<br>Edgewater Technology Services | |
| **Purpose of Information System or IT Project** | The Reporting and Analytical SharePoint (RASP) supports EHSS initiatives by housing three applications that collect, organize, analyze, and report on data. RASP is made up of three SharePoint sites. These sites collect PII from both external contractors and Federal employees. All three applications are EHSS-21 but each has a separate application owner. RASP acts as a document repository that users can share and retrieve files for the ongoing efforts of the EHSS programs that it supports. Low sensitivity administrative PII is stored within these three applications including contact information for the auditors, which are found in their respective audits. The PII is purely contact information, containing names, work titles, work addresses, work phone numbers, and/or work email addresses used to tie reports back to the individual or team who completed them.<br><br><u>DOE Consolidated Audit Program (DOECAP)</u><br><br>DOECAP conducts audits on commercial laboratories that have a contract with DOE to perform tests of air, soil, and water samples. These laboratories need to follow standard government guidelines in their testing procedures. DOECAP is the Federal agency that verifies that these guidelines are being followed. Audits are also conducted on commercial disposal facilities. The DOECAP SharePoint site houses checklists and other resources for auditors to be able to access so that they are using the most up-to-date guidelines during these audits.<br><br>The DOECAP SharePoint consists of document libraries that contain the necessary checklists and documents needed while the auditors are in the field. The checklists are used as references for audits and contain no PII themselves. Administrative PII - including job position and work phone - is contained with the reports and audits that are uploaded by employees to identify who completed/is responsible for the document.<br><br><u>Sustainable Acquisition</u><br><br>The Sustainable Acquisition SharePoint environment contains working documents for collaboration between DOE employees and external contractors. Low sensitivity administrative PII including name and email address is contained within this system for contact purposes.<br><br><u>Sustainable Environmental Stewardship</u><br><br>The Sustainable Environmental Stewardship SharePoint contains public information being maintained by EHSS-21 personnel for use by DOE employees and external contractors. Low sensitivity administrative PII is contained within this system for contact purposes. | |
| | Name, work title, work contact information. | |

# MODULE I – PRIVACY NEEDS ASSESSMENT

| | |
|---|---|
| **Type of Information Collected or Maintained by the System:** | |
| **Has there been any attempt to verify PII does not exist on the system?**<br>**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.* | The system contains administrative PII. |
| **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?** | NO |
| **4. Is the information about DOE or contractor employees?** | YES<br>☒ Federal Employees<br>☒ Contractor Employees |

# END OF PRIVACY NEEDS ASSESSMENT

# MODULE II – PII SYSTEMS & PROJECTS

## AUTHORITY, IMPACT & NOTICE

| | |
|---|---|
| **1. AUTHORITY**<br>**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 |
| **2. CONSENT**<br>**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)?** | Users give consent to be placed on the list as the contact person before the document is placed in SharePoint. Individuals who conduct the audits voluntarily include PII on the document. When a search in done in the SharePoint, the search is of a specific audit or document, not by identifiable attributes. Additionally, consent to have PII in one of the applications does not give consent in regard to the other two. Within the SharePoint, there is no email or chat function. The PII must be used outside of the SharePoint. |
| **3. CONTRACTS**<br>**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. The contracts contain the relevant privacy information and contractors are required to sign Confidentiality Agreements or Non-Disclosure Agreements (NDA). |
| **4. IMPACT ANALYSIS:**<br>**How does this project or information system impact privacy?** | PII such as name, phone, and email will be used for communication purposes only. Having current information in a centralized shareable secure location is essential for the success of projects contained in this system. Not having contact information readily accessible in the system will cause an undue burden on users to store and maintain that information elsewhere. All PII is business contact information. The low sensitivity and purely administrative use and nature of this PII result in a low privacy risk. Should this information be compromised, it would cause minimal harm to individuals.<br><br>A series of technical, administrative, and physical controls are implemented to restrict access based on role and to safeguard data within the system. The system leans heavily on data minimization to protect individuals' privacy by containing only work contact information. |

## MODULE II – PII SYSTEMS & PROJECTS

| | |
|---|---|
| **5. SORNs**<br>**How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?**<br>**If yes, explain, and list the identifiers that will be used to retrieve information on the individual.** | PII within the Sustainable Acquisition and Sustainable Environmental Stewardship is not retrievable to the users any sort of searchable identifier. PII located within the DOECAP application is attached to reports and audits and although identifiers are used to retrieve these documents, there would be no way to know what PII would be contained within the report or audit until it was opened. Moreover, the system contains exclusively administrative PII used for administrative purposes. |
| **6. SORNs**<br>**Has a Privacy Act System of Records Notice (SORN) been published in the *Federal Register*?**<br>**If "Yes," provide name of SORN and location in the *Federal Register*.** | N/A. The system contains administrative PII. |
| **7. SORNs**<br>**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?** | Individual-provided. DOE employees and contractors. |
| **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?** | See system security plan. |
| **DATA USE** | |

| MODULE II – PII SYSTEMS & PROJECTS | |
|---|---|
| **11. How will the PII be used?** | PII such as name, phone, and work email will be used for communication purposes and referral to who is responsible for each audit. |
| **12. If the system derives meta data, how will the new or meta data be used?**<br>**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?** | Audit reports contain business contact information. |
| **15. What will be the use of these reports?** | Audit reports are used to verify that laboratories are compliant with government guidelines respecting air, soil, and water testing. |
| **16. Who will have access to these reports?** | Only Department of Energy Authorized Federal Employees and Contractors will have access to the files. Only Administrators and/or Authorized users of the individual system will be able to access the files. Each application has separate access. An individual given access to one application does not automatically receive access to the other two applications. Access is given on a "need-to-know" basis. The permissions are set individually by the application owner. |
| **MONITORING** | |
| **17. Will this information system provide the capability to identify, locate, and monitor individuals?** | Identify and locate only, no tracking or monitoring will be used. The ability to locate is limited to the provided work contact information. |
| **18. What kinds of information are collected as a function of the monitoring of individuals?** | There is no tracking or monitoring information collected. |

## MODULE II – PII SYSTEMS & PROJECTS

| | |
|---|---|
| **19. Are controls implemented to prevent unauthorized monitoring of individuals?** | There is no tracking or monitoring information collected. |
| **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.** | It is the responsibility of the Application Owner to provide current and accurate lists. This information is provided by the respective individuals. PII within DOECAP is attached to reports and audits that identify who completed the document. The PII is not updated within these as they are a snapshot in time do not require updating. |
| **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 system will not be used at more than one site. It is a centralized system that all valid users can access. |
| **RECORDS MANAGEMENT** | |
| **22. Identify the record(s).** | SharePoint (RASP) provides document libraries for organization and collaboration of documents. Files that have been uploaded to the document libraries are copies of files that reside on the EHSS LAN. The files on the SharePoint server would not fall under Records Management. |
| **23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.** | N/A |
| **24. Records Contact** | Baldev Dhillon, 301-903-0990 |
| **ACCESS, SAFEGUARDS & SECURITY** | |
| **25. What controls are in place to protect the data from unauthorized access, modification or use?** | FEDRAMP High Level using Microsoft Azure Cloud SharePoint and DOE EITS Low Control Baseline controls. These include a series of technical, administrative, and physical controls used to restrict access based on role and to safeguard data within the system. |

| MODULE II – PII SYSTEMS & PROJECTS | |
|---|---|
| **26. Who will have access to PII data?** | Administrators of the system who are designated by the Federal Program/Project Managers. Users of the systems will have access to PII data on an as needed basis. Administrators have full control of the SharePoint structure, privileged users have read/write privileges and be able to make Team Site changes, and general users are limited to either read only or read/write privileges (These users are not allowed to make Team Site changes.) One must have an account (login information) to access the SharePoint. |
| **27. How is access to PII data determined?** | Administrators of the system who are designated by the Federal Program/Project Managers. Users of the systems will have access to PII data on an as needed basis. |
| **28. Do other information systems share data or have access to the data in the system? If yes, explain.** | There are no connecting Information Systems. |
| **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?** | There are no connecting Information Systems. |
| **30. Who is responsible for ensuring the authorized use of personal information?** | Administrators of the system who are designated by the Federal Program/Project Managers.<br><br>Developers, Network Administrators, System Owners, Third Party Network Support Personal |
| **END OF MODULE II** | |

# SIGNATURE PAGE

| | Signature | Date |
|---|---|---|
| **System Owner** | **Helen Heupel**<br>**(Print Name)**<br>Helen Heupel Digitally signed by Helen Heupel Date: 2023.03.31 09:21:06 -04'00'<br>**(Signature)** | |
| **Local Privacy Act Officer** | **Raymond C. Holmer**<br>**(Print Name)**<br>RAYMOND HOLMER Digitally signed by RAYMOND HOLMER Date: 2023.03.31 10:19:56 -04'00'<br>**(Signature)** | |
| ***Ken Hunt***<br>**Chief Privacy Officer** | **(Print Name)**<br>William K. Hunt Digitally signed by William K. Hunt Date: 2023.03.30 12:00:40 -04'00'<br>**(Signature)** | |