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	06/27/2023	
Departmental Element & Site	Fossil Energy and Carbon Management/National Energy Technology Laboratory	
Name of Information System or IT Project	NETL Microsoft Office 365	
Exhibit Project UID		
New PIA X **Update**		
	Name, Title	**Contact Information Phone, Email**
System Owner	Martin Andrews	(O) 412-386-5391 martin.andrews@netl.doe.gov
Local Privacy Act Officer	Ann Guy	(M) (202) 555-1212 ann.guy@netl.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Justin Woodford	(O) (541) 918-4508 justin.woodford@netl.doe.gov
Person Completing this Document	James Kessler	(O) (304)285-4129 james.kessler@netl.doe.gov
Purpose of Information System or IT Project	Microsoft Office 365 is a Software as a Service (SaaS) solution that includes Microsoft Office and other services, such as email and collaboration, from Microsoft's cloud server. Microsoft Office 365 provides desktop functionalities and is available by subscription. Microsoft Outlook is a collaboration tool that may share Personally Identifiable Information for necessary employment functions such as personnel actions, security clearances, and medical actions. Microsoft Office houses the file formats necessary to create and maintain employee information such as Word, Excel, and PowerPoint.	
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	

MODULE I – PRIVACY NEEDS ASSESSMENT

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.*	PII exists on the system.
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, both ☒ 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.

MODULE I – PRIVACY NEEDS ASSESSMENT

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.
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)?**	Personnel Tracking System (PTS) contains personnel information provided by employees to HR. Should prospective or current employees decline to provide PII needed by HR, it may affect their ability to obtain or maintain employment. Employee information in Office 365 will be for official use only by authorized users.

MODULE II – PII SYSTEMS & PROJECTS	
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?**	Contractors are onboarded to assist with the design, development and maintenance of PTS and Occupational Health Management (OHM). Privacy Act clauses are included in the contracts. Depending upon the type of contract awarded, one or more of the clauses listed below is included: • Compliance with Applicable Federal, State, and Local Requirements; • Confidentiality of Information; • Security and Personnel Requirements; • Government Provided Services; • Automatic Data Processing Equipment (ADPE) Usage; • Automatic Data Processing Equipment (ADPE) Leasing; • Limitation of Software; • 52.224-1 Privacy Act Notification (Apr 1984); • 52.224-2 Privacy Act (Apr 1984); • 52.239-1 Privacy or Security Safeguards (Aug 1996); • 952.204-77 Computer Security (Aug 2006).

MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	DOE has assessed Office 365 as a moderate-risk systems according to the criteria set forth in Federal Information Processing Standard 199 established by the National Institute of Standards and Technology (NIST). The risk rating is used to determine the effect to the agency should the system's confidentiality, integrity or availability be compromised. The unauthorized disclosure of information contained in the 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, and it would damage the trust between individuals and the Federal Government. Authorized users of Office 365 are the subject of a favorably adjudicated background investigation and receive extensive training on the use and protection of PII. 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. Security controls have been implemented and processes are in place to ensure that access is restricted. The Office 365 system 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 reviews • Encryption of data at rest and data in transit
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.**	Yes. Searches would show full name, work address, phone number, email address, and business affiliation.

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*.**	• DOE–2 DOE-Personnel Supervisor Maintained Personnel Records • DOE–3 Employee Concerns Program Records • DOE–8 Intergovernmental Personnel Act (IPA) Agreements • DOE–23 Property Accountability System • DOE–28 General Training Records • DOE–60 General Correspondence Files
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?	NETL on-premises Active Directory populated by PTS
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
DATA USE	
11. How will the PII be used?	To create/manage user accounts, to assign roles, to find individuals in the Global Address List, and to collaborate/communicate.
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

MODULE II – PII SYSTEMS & PROJECTS	
13. With what other agencies or entities will an individual's information be shared?	DOE Headquarters and other National Laboratories that subscribe to the Energy IT Services (EITS) tenant.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	Authentication logs, system scans
15. What will be the use of these reports?	NIST mandated security logging
16. Who will have access to these reports?	NETL Cyber Security Team
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	Yes, via logging and NETL's enterprise SIEM system (Splunk) and Microsoft's Security and Compliance Center
18. What kinds of information are collected as a function of the monitoring of individuals?	Username, date/time stamp, IP address, ports/protocols, system name.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Role based, with only administrator access to system logs.
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.	Full name, email address, phone, and organization are replicated from Active Directory via PTS.

MODULE II – PII SYSTEMS & PROJECTS	
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	Microsoft Office 365 ensures real-time replication of its data.
Records Management	
22. Identify the record(s).	Email, Chats, Teams sites, Calendar, Calls/voicemail, Files/documents Information System Security Records
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	☐ Unscheduled X Scheduled *(cite NARA authority(ies) below)* Email, chat, calendar, calls/voicemail (Exchange, Teams): GRS 6.1, Item 010 & 011 Files/Documents (SharePoint, OneDrive) GRS 5.2, Item 020, DOE ADM 23, Item 5.1, Program specific retention schedules. Information System Security Records: GRS 3.2, Items 020, 030, 031
24. Records Contact	Ryan Morrone, ryan.morrone@netl.doe.gov (O) (412) 386-4693
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	O365 uses role-based security. Additionally, NETL implements a Zero trust model enforcing principal of least privilege and phishing-resistant MFA. Information containing PII will be encrypted in transit.
26. Who will have access to PII data?	Full Name is accessible to all users. Email, Phone, Occupation, and Organization are visible from the Global Address List. Other forms of PII may be transmitted through messages in an encrypted fashion.
27. How is access to PII data determined?	It's what would be visible in the Global Address List (GAL)

MODULE II – PII SYSTEMS & PROJECTS	
28. Do other information systems share data or have access to the data in the system? If yes, explain.	Any system that uses Lightweight Directory Access Protocol to authenticate to it would have the same information replicated from Active Directory.
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?	Yes
30. Who is responsible for ensuring the authorized use of personal information?	NETL Privacy Officer NETL Authorizing Official
END OF MODULE II	

SIGNATURE PAGE		
	Signature	**Date**
System Owner	**Martin Andrews** **(Print Name)** Digitally signed by MARTIN ANDREWS Date: 2023.06.27 17:01:33 -04'00' **(Signature)**	
Local Privacy Act Officer	**Ann Guy** **(Print Name)** ANN GUY Digitally signed by ANN GUY Date: 2023.06.28 05:44:27 -04'00' **(Signature)**	
Chief Privacy Officer	**Ken Hunt** **(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2023.06.27 16:34:29 -04'00' **(Signature)**	