Affects Members Of the Public? X

Department of Energy

Privacy Impact Assessment (PIA)

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	03-09-2021
Departmental Element & Site	Southwestern Power Administration
Name of Information System or IT Project	Southwestern Microsoft Office 365 (O365)
Exhibit Project UID	SWPA GSS (formerly Infrastructure and Office Automation) – 019-60-02-00-01-5000-04
New PIA [X] **Update** [ ]	N/A

	Name, Title	Contact Information Phone, Email
System Owner	Francis Romans	918.595.6638 francis.romans@swpa.gov
Local Privacy Act Officer	Laurence J. Yadon	918.595.6607 laurence.yadon@swpa.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Dawn Rodriguez, Information Security Officer (ISO)	918.859.8589 dawn.rodriguez@swpa.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Person Completing this Document	Dawn Rodriguez, Information Security Officer (ISO)	918.859.8589 dawn.rodriguez@swpa.gov
Purpose of Information System or IT Project	Southwestern's Microsoft Office 365 Multitenant is a cloud computing environment offered by Microsoft as a Software-as-a-Service (SaaS) subscription. Southwestern's primary use of this SaaS is for cloud-based email. Depending on what end-users choose to email, information stored in email and attachments (such as spreadsheets, word processing documents, and other Portable Document Format (PDF) documents) may contain PII. This PIA discusses the relevant categories of PII anticipated to be included as per Southwestern's common business purposes. Microsoft Skype for Business, Teams, SharePoint Online, and OneDrive for Business are not authorized to contain PII beyond the minimal user information required for the administration of the systems as per *Rules of Behavior* and *Information Protection Management.* This system may contain the following PII maintained by Southwestern Divisions: • Financial Management – SSN, Employee Name, Financial Information; • Human Resources Management - SSN, Medical & Health Information, Date of Birth (DoB), Place of Birth, Employment Information, Criminal History, Name, Phone, Address; • Wyandotte Technologies - SSN, Birth Dates, Name, Phone, Address, and Employment Information; • Acquisition and Facilities Services - Landowner names and addresses • General Counsel - SSN, Medical Information, Financial Disclosures, Name, Phone, and Address; • Environmental, Health, Safety - Accident Reports, Name, and Birth Dates & Security - DoB, Place of Birth, SSN, Criminal History, Clearance Information, Mother's Maiden Name, Name, Phone, and Address.	
Type of Information Collected or Maintained by the System:	☒ SSN Social Security number ☒ Medical & Health Information ☒ Financial Information ☒ Clearance Information ☐ Biometric Information ☒ Mother's Maiden Name ☒ DoB, Place of Birth	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☒ Employment Information ☒ Criminal History ☒ Name, Phone, Address ☒ Other – Accident Reports
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 *Member of the Public* refers to individuals in a non-employee or DOE contractor context. *Members of the Public* includes individuals for whom DOE maintains information, as required by law, who were previously employed or contracted by DOE.
4. Is the information about DOE or contractor employees?	YES ☒ Federal Employees

MODULE I – PRIVACY NEEDS ASSESSMENT

	☒ Contractor Employees

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. • 44 U.S.C. Chapter 35, The Paperwork Reduction Act.
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 who require access to Southwestern sites or systems must provide the requested information or they are not allowed to access those sites or systems. Consent is given when a user provides information to Southwestern on Federal Tort Claim form SF95. Consent is not required for public information (e.g., land sales and any related information available in local and state offices).
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?**	Wyandotte support services contractor is involved in the maintenance of systems containing PII. Southwestern's procurement processes ensure that the required privacy clauses exist in these contracts.

MODULE II – PII SYSTEMS & PROJECTS	
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	Southwestern has reviewed the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB) Approved Security Authorization Package: Microsoft - Office 365 Multi-Tenant & Supporting Services (Microsoft Office 365 multitenant, MSO365MT). Microsoft Office 365 multitenant has been categorized and assessed using methods and procedures consistent with Federal guidance including FIPS 199 and NIST 800-53. A security categorization of "Moderate" (Confidentiality=Moderate, Integrity=Moderate, Availability=Moderate) was provided as part of the package and independently confirmed by Southwestern. The unauthorized disclosure of information is expected to have a serious adverse effect on Southwestern operations, assets, or individuals. Because the information included in emails is determined by users, there is a wide range of potential harm should this information be compromised. Should an email containing sensitive PII (e.g., SSN, personal health information) be compromised, the breach may result in significant harm to the affected individual(s) potentially including embarrassment, harm to professional reputation, social harm, financial harm, and could damage the trust between individuals and their employer. Security controls have been implemented and processes are in place to ensure that controls are operating effectively to mitigate the risk of O365 from being compromised. Role-based controls are used to determine access to systems and cannot be released without appropriate authorization or required access.
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.**	PII data within O365 is only authorized in email form. Retrieval is dependent on the mailbox user and may or may not be retrieved by an identifier. Depending on the application used (Outlook or mobile device), Southwestern end-users can retrieve information (e.g., information contained in email messages in the user's inbox or archive) by name or other identifiers using a full-text search capability.

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*.**	• Financial Management - Payroll, employee reimbursements, and non-cash fringe benefits reporting; Full SSN (DOE-18; DOE-26) • General Counsel – Federal Tort Claim forms; Full SSN (DOE-1; DOE-41; DOE-54) • Environmental, Health, Safety & Security [Personnel Risk Assessments; Full SSN (DOE-43; DOE-51; DOE-52; DOE-63)] and System Protection and Communications – Accident/Injury Forms; Partial SSN (DOE-38; DOE-2, DOE-7) • Human Resources Management – Human Resources forms; Full SSN (DOE-13; DOE-28; DOE-33; DOE-43)
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?	The source of an email message and the information contained therein is the sender of the message. This may include a Southwestern end-user (Federal and Contractor), an employee of another Federal agency (DOE HQ, USACCESS, Landowner names and addresses), an employee of a tribal, state, or local government agency (County Records - courthouse records, tax records, other public records), an employee of a private company or law firm, a member of the public, or some other category of individual corresponding with a user.
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. *Restricted Information ID (BCSI, ITSI, PII, CEII)*
DATA USE	

MODULE II – PII SYSTEMS & PROJECTS	
11. How will the PII be used?	O365 is utilized to transmit email messages (Outlook/Mobile devices) that might contain PII. The end user determines the use of PII. Anticipated uses include the following: • HR uses PII to create personnel files. Southwestern will not use contractor HR personnel information. • Financial Management uses PII for payment and/or reimbursement purposes. • Acquisition and Facilities Services uses PII to identify landowners. • Environmental, Health, Safety & Security uses PII provided by DOE HQ's CAIRS (Computerized Accident/Incident Reporting System). Although this is a DOE system, CAIRS reports are stored locally on Southwestern's file servers and SharePoint. The CAIRS program is used to analyze accident trends and store accident investigation data for the purposes of accident reporting. Security uses PII to adjudicate suitability for access to sites or systems. • General Counsel uses PII to request treasury checks to pay tort claims.
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?	The end user determines with whom to share PII. Southwestern PII may be shared internally within Southwestern divisions to other authorized personnel (Finance/General Counsel) and with the Department of Energy, Department of Energy Counterintelligence upon request or requirement, the Treasury Department, Office of Personnel Management, Justifacts and other third-party background investigation providers, and/or Freedom of Information request.
REPORTS	
14. What kinds of reports are produced about individuals or contain an individual's data?	The end-user determines PII report requirements. O365 may contain email messages containing the following Southwestern PII reports: 1099, Payroll, Employee, Vendor and Customer Payment, Non-Cash Fringe Benefit Reports, list of landowner names and addresses, accident reports, travel vouchers, DOE HR portal reports, incident reports (physical/cyber), background investigation reports, 450 financial disclosures, and land-related reports. However, most PII is maintained for retention purposes only.

MODULE II – PII SYSTEMS & PROJECTS	
15. What will be the use of these reports?	The end user determines the use of PII reports. Southwestern uses the PII reports from item 14 for contacting land-owners for property issues, accident reporting and recordkeeping, reporting of Physical Security Incidents, reporting counterintelligence leads and concerns to appropriate agency resources, determination of suitability for access and are used to respond to required data requested.
16. Who will have access to these reports?	Authorized PII end users have access to select reports depending on user role. End-users include: • Security Officer/Security Specialist/Personnel Security Contractor • Human Resources Specialists • Human Resources support contractor. • DOE Counterintelligence, upon request • IT personnel with administrative access to all folders • Realty Specialists • Environmental Specialist • Field personnel • Safety Office Manager • Director, Division of Environmental, Health, Safety & Security • Contractor safety specialist • GC Attorneys and Paralegals • Financial Management personnel • Supervisors/Management personnel, as needed
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?	None
19. Are controls implemented to prevent unauthorized monitoring of individuals?	All electronic access permissions are controlled through username, password, and/or PIV cards. Access is limited based on job functions. Log management procedures provide monitoring of system use.
DATA MANAGEMENT & MAINTENANCE	

MODULE II – PII SYSTEMS & PROJECTS	
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 content of official records is maintained by the Divisions who own the information. System Owners and information owners are responsible for ensuring information is used and managed consistently for its stated purpose in support of Southwestern. The end user maintains the content of official PII records. Financial information is updated with current information provided by employees, vendors, and other sources such as HR and Legal; new Wyandotte contractor HR forms would be requested of the individual; Acquisition and Facilities Services updates records when real property owners change, and physical security records only contain data which was derived or provided at time of investigation. This is periodic for long term employees or contractors. Completeness is determined at time of investigation. Accuracy for provided information is determined at time data is provided and is confirmed upon receipt of investigation report.
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 content of official records is maintained by the Divisions who own the information. System Owners and information owners are responsible for ensuring information is used and managed consistently for its stated purpose in support of Southwestern.
RECORDS MANAGEMENT	
22. Identify the record(s).	Records include emails of high level officials and non-high level officials.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	HLO email scheduled under GRS 6.1, item 010 (DAA-GRS2014-0001-0001); non-HLO email scheduled under GRS 6.1, item 011 (DAA-GRS2014-0001- 0002). See SWPA Capstone form for listing of HLO email accounts. This email schedule has been adopted enterprise-wide by DOE.
24. Records Contact	Jason DeFrain, jason.defrain@swpa.gov, 918.218.3465
ACCESS, SAFEGUARDS & SECURITY	

MODULE II – PII SYSTEMS & PROJECTS	
25. What controls are in place to protect the data from unauthorized access, modification or use?	The system is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements. Southwestern's Cyber Security Program Plan (CSPP) documents information security policy, procedures and security controls implemented to protect data from unauthorized access, modification, or use. The O365 system is FEDRAMP authorized at a Moderate FIPS categorization accredited by John Porter on 08-30-18. Monitoring, testing, and evaluating the system and applied controls is implemented through the FEDRAMP process. Security controls have been implemented and processes are in place to ensure that controls are operating effectively to mitigate the risk of O365 from being compromised. Role-based controls are used to determine access to systems and cannot be released without appropriate authorization or required access. O365's email function utilizes Entrust encryption to protect PII in transit. Users are required to participate in an annual cyber security training as well as review and sign Rules of Behavior.
26. Who will have access to PII data?	Access to O365 is restricted to authorized Southwestern end-users (employees and contractors). All end-users who access O365 must adhere to the Rules of Behavior. Non-Southwestern individuals may have access to PII only to the extent that users send these individuals email messages. Specific roles with PII access include: • Wyandotte Program Manager/IT Project Manager/Admin Assistant • Realty Specialists • Environmental Specialist • Field personnel • Safety Manager, Director of Safety, Contractor Safety Specialist • General Counsel Staff • Security Officer/Security Specialist/Personnel Security Contractor • Human Resource Specialists, Human Resources support contractor. • DOE Counterintelligence upon request • IT Personnel - administrative access • Financial Management employees • Supervisors/Management personnel, as needed
27. How is access to PII data determined?	Access is determined on a need-to-know basis due to role/responsibility. Supervisors or management request access using the access request process. Each user will use his or her individual account and password to access the data.

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?	System Security for PII: ○ Information owners ○ Information Security Officers ○ System Administrators
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	**Francis Romans**	
Local Privacy Act Officer	**Laurence Yadon**	
DOE HQ Chief Privacy Officer	William K. Hunt Digitally signed by William K. Hunt Date: 2021.07.20 08:52:54 -04'00' **Ken Hunt**	