Affects Members Of the Public? ☐

Department of Energy

Privacy Impact Assessment (PIA)

MODULE I – PRIVACY NEEDS ASSESSMENT		
Date	10-05-22	
Departmental Element & Site	Southwestern Power Administration (SWPA)	
Name of Information System or IT Project	Southwestern General Support System (GSS) – Includes File Servers (Pluto/Pegasus) and Microsoft SharePoint, ORACLE, and Commvault applications.	
Exhibit Project UID	SWPA GSS (formerly Infrastructure and Office Automation) – 019-60-02-00-01-5000-04	
New PIA ☐ **Update** X		
	Name, Title	**Contact Information Phone, Email**
System Owner	Francis Romans, IT Specialist (IT Lead)	918.595.6638 francis.romans@swpa.gov
Local Privacy Act Officer	Lona Smith, Management and Program Analyst	(918) 595-6649 lona.smith@swpa.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Allan Reid, Chief Information Security Officer (CISO)	(417) 891-2652 allan.reid@swpa.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Person Completing this Document	Dawn Rodriguez, Information Security Officer (ISO)	(918) 595-6717 dawn.rodriguez@swpa.gov
Purpose of Information System or IT Project	SWPA GSS is a Wide Area Network (WAN). This network is comprised of six Local Area Networks (LANs) within offices located in Tulsa, Gore, OK; Jonesboro, AR; Springfield, Table Rock; and Nixa, MO. The GSS provides SWPA personnel with email, internet access, file storage, and backup/restoration (Commvault). The GSS supports the Financial Management System (FMS) or Oracle, and Microsoft SharePoint applications. Oracle is used by Southwestern to process and record financial transactions related to purchasing, projects, assets, inventory, accounts payable, accounts receivable, and general ledger activities. Activities include but are not limited to payroll, payment of suppliers, project cost, customer revenues and collections, etc. The system contains SSN, TIN, Bank Account Information, Credit Card Information, Name, Phone, and Address information. Microsoft SharePoint, File servers (Pegasus/Pluto), and Commvault are authorized document storage locations for sensitive information. The following department and SharePoint folders may contain PII: • Dept_Finance: Social Security Number (SSN), Employee Name, Cash Management (Financial Information) • CM1: LDS SSN, Employee Name, Cash Management (Financial Information) • QUAD: Financial Information – temporary storage declaration until consolidation of information to Dept_Finance. • E-Discovery: All types of PII. • Dept_Security: DoB, Place of Birth, SSN, Criminal History, Clearance Information, Mother's Maiden Name, Name, Phone, Address • Dept_HR: SSN, Medical & Health Information, DoB, Place of Birth, Employment Information, Criminal History, Name, Phone, Address • Dept_IT/Bearskin_HR: SSN, Birth Dates, Name, Phone, Address, Employment Information • Dept_IT/Wyandotte_HR: SSN, Birth Dates, Name, Phone, Address, Employment Information • Dept_Legal: SSN, Medical Information, Financial Disclosures, Name, Phone, Address • Dept_HealthSafety: Accident Reports, Name, Birth Dates	
Type of Information Collected or	☒ Social Security number - Microsoft SharePoint/File servers (Pegasus/Pluto), Oracle, and Commvault are authorized document storage locations for sensitive information.	

MODULE I – PRIVACY NEEDS ASSESSMENT

Maintained by the System:	☒ Medical & Health Information – Microsoft SharePoint/File servers (Pegasus/Pluto) and Commvault are authorized document storage locations for sensitive information. ☒ Financial Information – Oracle/Microsoft SharePoint/File servers (Pegasus/Pluto)/Commvault are authorized document storage locations for sensitive information. ☒ Clearance Information - Microsoft SharePoint/File servers (Pegasus/Pluto)//Commvault are authorized document storage locations for sensitive information. ☐ Biometric Information ☒ Mother's Maiden Name - Microsoft SharePoint/File servers (Pegasus/Pluto)/Oracle/Commvault are authorized document storage locations for sensitive information. ☒ DoB, Place of Birth - Microsoft SharePoint/File servers (Pegasus/Pluto)/Oracle/Commvault are authorized document storage locations for sensitive information. ☒ Employment Information - Microsoft SharePoint/File servers (Pegasus/Pluto)/Oracle/Commvault are authorized document storage locations for sensitive information. ☒ Criminal History - Microsoft SharePoint/File servers (Pegasus/Pluto) are authorized document storage locations for sensitive information. ☒ Name, Phone, Address - Microsoft SharePoint/File servers (Pegasus/Pluto)/Oracle/Commvault are authorized document storage locations for sensitive information. ☒ Other – Accident Reports - Microsoft SharePoint/File servers (Pegasus/Pluto)/Commvault are authorized document storage locations for sensitive information.
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*	PII does exist on the system. Southwestern employs software tools to scan content (information or data) to search for types of data such as Social Security numbers.

MODULE I – PRIVACY NEEDS ASSESSMENT

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.	
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	System scan

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?	NO ☐ Federal Employees ☐ 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.
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)?**	The information is a requisite of access to SWPA sites or systems. Should an individual decline to provide required information, access may be denied.
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. SWPA's procurement processes ensure that the requisite Privacy Act clauses are included in these contracts.

MODULE II – PII SYSTEMS & PROJECTS	
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	SWPA has assessed GSS as a moderate-risk system 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. Applications within the system contain highly sensitive PII including but not limited to SSN, health data, and financial data. 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). Applications containing PII maintain 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 according to role and that controls are operating effectively to mitigate the risk of GSS from being compromised. Physical access is controlled with a Physical Access Control System (PACS). Access is restricted based on job function and electronic access permissions are controlled through username, password, and/or PIV cards. Log management procedures provide monitoring of system use to ensure the integrity and security of the data in the system. The system undergoes bi-annual system scans for PII as an added layer of data protection to ensure that no unaccounted for or unnecessary data is contained as well as to help ensure the accuracy of PII.
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.**	Some data can be retrieved by name, address, and SSN. Physical security electronic access records can be retrieved by name only.

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*.**	• Dept_Finance - Payroll, employee reimbursements, and non-cash fringe benefits reporting; Full SSN (DOE-18, 74 FR 1020; DOE-26, 74 FR 1026) • Dept_Security – Personnel Risk Assessments; Full SSN (DOE-43, 74 FR 1044; DOE-51, 74 FR 1053; DOE-52, 74 FR, 1055; DOE-63, 74 FR 1068) • Dept_Legal – Federal Tort Claim forms; Full SSN (DOE-1, 74 FR 998; DOE-41, 74 FR 1042; DOE-55, 74 FR 1059) • Dept_System Protection and Communications – Accident/Injury Forms; Partial SSN (DOE-38, 74 FR 1039; DOE-2, 74 FR 999, DOE-7, 74 FR 1005) • Dept_HR – Human Resources forms; Full SSN (DOE-13, 74 FR 1012; DOE-28, 74 FR 1029; DOE-33, 74 FR 1032; DOE-43, 74 FR 1044)
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?	• Individuals – HR and financial information (e.g., bank account, credit card number, SSN, TIN, address, name) is provided by employees, customers, vendors, and landowners/tenants. • Systems maintained by Federal agencies – ATAAPS, CAIRS(Computerized Accident/Incident Reporting System), CHRIS (PeopleSoft), DFAS interface for payroll, DOE Info, eComp (DOL system) for workers compensation, eOPF (OPM), eVerify (USCIS), PIPS/CVS (OPM system), USA Staffing (OPM), and USACCESS. • Tribal, state, or local government entity (County Records - courthouse records, tax records, other public records) • Named and other third-party sources (background checks, neighbors or friends).
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.

MODULE II – PII SYSTEMS & PROJECTS	
DATA USE	
11. How will the PII be used?	• The HR Division uses PII to create personnel files. SWPA will not use contractor HR personnel information. • The Financial Management division uses PII for payment and/or reimbursement purposes. • The Safety division uses PII provided by DOE CAIRS. Although this is a DOE system, CAIRS reports are stored locally on SWPA file servers and SharePoint. The CAIRS program is used to analyze accident trends and store accident investigation data for the purposes of accident reporting. • The General Counsel division uses PII to request treasury checks to pay tort claims. • Physical Security uses PII to adjudicate suitability for access to sites or systems.
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?	PII is generally shared internally within DOE, and PII housed in HR systems which are accessed through the DOE portal cannot be queried by other agencies or entities. Some PII may be queried and potentially shared with the Treasury Department, Office of Personnel Management, Justifacts, and other third-party background investigation providers as permitted in the corresponding SORNs.
REPORTS	
14. What kinds of reports are produced about individuals or contain an individual's data?	Reports containing PII include: 1099, Payroll, Employee, Vendor and Customer Payment, Non-Cash Fringe Benefit Reports, ccident reports, travel vouchers, DOE HR portal reports, incident reports (physical/cyber), background investigation reports, and 450 financial disclosures.
15. What will be the use of these reports?	SWPA uses the PII reports from item 14 for accident reporting and recordkeeping, reporting of Physical Security Incidents, reporting counterintelligence leads and concerns to appropriate agency resources, determination of suitability for access, and to respond to authorized data requests.

MODULE II – PII SYSTEMS & PROJECTS	
16. Who will have access to these reports?	• 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?	Access is restricted based on job function and electronic access permissions are controlled through username, password, and/or PIV cards. Log management procedures provide monitoring of system use to ensure the integrity and security of the data in the system.

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.	Financial information is updated with current information provided by employees, vendors, HR, and Legal; new Wyandotte contractor HR forms would be requested from the individual; the Procurement division 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 the time data is provided and is confirmed upon receipt of the 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?	System Owners and information owners are responsible for ensuring information is used and managed in a consistent manner. In accordance with the Federal Managers' Financial Integrity Act, SWPA is required to review, assess, and establish effective internal controls over their programs, financial reporting, and financial management systems.
RECORDS MANAGEMENT	
22. Identify the record(s).	• General Counsel retains Federal Tort claims and financial disclosures for 6 years. • FOIA requests for 6 years. • Physical security data is maintained for 5 years after next investigation.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	☐ Unscheduled ☒ Scheduled *(cite NARA authority(ies) below)* Procedures are documented in the Records Retention Schedule and established in accordance with approved DOE records schedules. Upon conversion to electronic format, paper copies are destroyed using a crosscut shredder. Electronic files are deleted from their network locations. SWPA SF115 NI-387-09-1 is the disposition authority for all items that have SWPA specific retention schedules. • General Counsel & Finance records: SWPA SF115 NI-387-09-1 • FOIA - General Records Schedule 4.2, approved-3 years; denied-6 years. • Physical Security records: General Records Schedule 5.6, individuals cleared-5 years; individuals denied-1 year after consideration.
24. Records Contact	Jason DeFrain, jason.defrain@swpa.gov; 918-218-3465

ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	Physical access is controlled with a Physical Access Control System (PACS). Access is restricted based on job function and electronic access permissions are controlled through username, password, and/or PIV cards. Log management procedures provide monitoring of system use to ensure the integrity and security of the data in the system. SWPA's *Cyber Security Program Plan (CSPP)* and GSS Security plan document information security policy, procedures and security controls implemented to protect data from unauthorized access, modification, or use. The System Owner has implemented and tested all baseline security controls appropriate to Moderate FIPS categorization in accordance with DOE Directives. The system was certified and accredited by by Marshall Boyken on 02/01/2021.
26. Who will have access to PII data?	• 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 who have 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; for example, supervisors or management will request access using the access request process. Each user must use his or her individual account and password to access the data.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	No – data is only shared internally within the GSS System.

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?	For external interconnections, SWPA maintains ISAs outlining the responsibilities and expectations for system interconnections with DOENet, but that is for access to their systems, not access to the GSS.
30. Who is responsible for ensuring the authorized use of personal information?	• Information Owners • Information Security Officers • Security Officer/Security Specialist/Personnel Security Contractor • System Administrators • Wyandotte Program Manager/IT Project Manager/Admin Assistant • Realty Specialists • Environmental Specialist • Field Personnel • DOE site coordinator for CAIRS • Accounting Officer
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	**Doug Hart** **FMS "Oracle" System Owner** Francis L. Romans Digitally signed by FRANCIS ROMANS Date: 2022.11.28 15:49:59 -06'00' **Francis Romans** **GSS System Owner**	
Local Privacy Act Officer	Lona Smith Digitally signed by Lona Smith Date: 2022.11.28 16:07:28 -06'00' **Lona Smith** **Privacy Act Officer**	
DOE HQ Chief Privacy Officer	Brooke J. Dickson Digitally signed by Brooke J. Dickson Date: 2022.11.23 14:09:36 -05'00' **Ken Hunt** **Chief Privacy Officer**	