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	02/01/2022
Departmental Element & Site	The Department of Energy Environmental Management Los Alamos National Laboratory N3B Project
Name of Information System or IT Project	N3B EM Los Alamos Legacy Cleanup Contract Network (N3B EM-LA LLCC)
Exhibit Project UID	N3B EM Los Alamos Legacy Cleanup Contract
New PIA ☐ **Update** ☒	Name, Title and Contact Information were updated to current. Items 22 and 23 were updated with inputs from N3B records management.

	Name, Title	Contact Information Phone, Email
System Owner	Jason Moore, CIO	(505) 257-7155 Jason.Moore@em-la.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT		
Local Privacy Act Officer	John H. Evans	(240) 562-1125 John.H.Evans@em.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Frank Steves, ISSM	(505) 695-4569 Frank.Steves@em-la.doe.gov
Person Completing this Document	Adotey Acquaye, ISSO	(505) 709-7921 Adotey.Acquaye@em-la.doe.gov
Purpose of Information System or IT Project	The EM-LA LLCC network provides a means of storing and processing information during the execution of work performed by N3B in support of the Los Alamos Legacy Cleanup Contract (LLCC). The work to be performed involves a software suite form generating, profiling, characterizing, inventorying, processing, over packing, packaging, and shipping all waste streams. The EM-LA LLCC network encompasses a variety of engineering and administrative applications to enable execution of general business systems and functions, such as electronic mail, internet access, and office productivity applications. N3B generates drawings, reports, analyses, calculation packages, commercial contract documentation (work authorizations, POs, etc.) correspondence, computer software analysis package input and output, and emails both internal and external. The project utilizes a combination of on premise and FedRAMP approved cloud-based software. Applications supporting key business process which may contain PII include: • Payroll, benefits (maintained primarily via third-party cloud provider, but key personnel may download reports and records in the process of job duties • Environmental Safety and Health and/or Occupational health medical records • Human Resources • Procurement and Contracts • Project Controls • Security for processing badging and clearance related information • Information Technology (file systems and email accessed by authorized individuals)	
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"	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐ 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
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.*	No
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, previous employees and current/previous contractors, subcontractors, vendors, guests
4. Is the information about DOE or contractor employees?	YES (If Yes, select with an "X" in the boxes below) ☐ Federal Employees ☒ Contractor Employees

MODULE I – PRIVACY NEEDS ASSESSMENT

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?**	The U.S. Department of Energy Contract 89303318CEM000007 provides N3B with the authority to collect information required to manage the project including retention of personnel data. Federal and state labor and tax laws require employers to maintain information pertaining to employees, vendors. The Energy Employees Occupational Illness Compensation Program Act (EEOICPA) was enacted in October 2000. Part B of the EEOICPA, effective July 31, 2001, compensates current or former employees (or their survivors) of the DOE, its predecessor agencies, and certain of its vendors, contractors, and subcontractors, who were diagnosed with a radiogenic cancer, chronic beryllium disease, beryllium sensitivity, or silica while employed at covered facilities. 20 CFR Parts 1-30, Title 42, Chapter 84 Federal Record, and 10 CFR 835 for Radiological Records also apply. Authority to maintain records associated with DHS facility and perimeter access control, including visitor management can be found in 5 U.S.C. § 301; the Federal Records Act, 6 U.S.C., the Homeland Security Act; 44 U.S.C. § 3101; and Executive Order 9397, as amended; Executive Order 12968, Federal Property Regulations, issued July 2002.
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)?**	Consent to provide information for the intended purpose is a part of the application process. By providing the information, consent is provided by the individual. Information is only utilized for its intended purpose.
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. Contracts issued by N3B contain required contract flow down clauses.

MODULE II – PII SYSTEMS & PROJECTS	
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	DOE has assessed N3B as a moderate risk system for confidentiality, integrity, and availability according to the criteria set forth in Federal Information Processing Standard (FIPS) 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. Safeguards exist to reduce the risk of compromise. N3B 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 • Firewalls, and application security features. N3B contains some PII, the ensuing risk to the privacy of individuals is generally moderate given the type of information that is retrieved. A compromise of privacy information could subject an individual to malicious activities such as identity theft.
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.**	Retrieval methods are based on the business needs of the organization. Typically, information is retrieved via searchable names or another unique identifier.

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*.**	N3B does have records that fall under some of DOE's, which are listed below. N3B does not have a published SORN, as we are a private company. DOE-5 Personnel Records of Former Contractor Employees (includes all former workers) DOE-10 Energy Employees Occupational Illness Compensation Program Act Files DOE-11 Emergency Operations Notification Call List DOE-14 Report of Compensation DOE-15 Intelligence Related Access Authorization DOE-28 General Training Records DOE-33 Personnel Medical Records (present and former DOE employees and Contractor employees) DOE-35 Personnel Radiation Exposure Records DOE-38 Occupational and Industrial Accident Records DOE-43 Personnel Security Clearance Files DOE-48 Security Education and/or Infraction Reports DOE-51 Employee and Visitor Access Control Records DOE-52 Access Control Records of International Visits, Assignments, and Employment at DOE Facilities and Contractor Sites DOE-53 Access Authorization for ADP Equipment DOE-81 Counterintelligence Administrative and Analytical Records and Reports DOE-84 Counterintelligence Investigative Records DOE-88 Epidemiologic and Other Health Studies, Surveys, and Surveillances
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?	Information is provided by the individual. Medical records or requests for background information may be additionally obtained via a third-party vendor or medical facility.

MODULE II – PII SYSTEMS & PROJECTS	
9. Will the information system derive new or meta data about an individual from the information collected?	It is possible that the information system will derive new meta data based on information aggregation and reporting.
10. Are the data elements described in detail and documented?	Database schemas, configuration baseline documentation, and vendor provided documentation provide detail data elements.
DATA USE	
11. How will the PII be used?	Badging, tax-related usage, payroll/payment information (i.e. direct deposit or checks) and reimbursement of expenses. Additionally, reporting is utilized. Information may be provided to DOE upon request. Health related information is utilized as part of compliance requirements.
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?**	Reporting. For example, IRS reporting requirements, financial reports, and compliance reports.
13. With what other agencies or entities will an individual's information be shared?	Applicable Federal, State, and Local Tax agencies, Department of Energy.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	Employee/contractor expense data is used to manage reimbursement of expenses. Vendor reports are used to track expenses. Tax related reports are used to provide tax form information. Health, incident, and/or safety-related reports may be created for compliance, oversight submittal, and for quality improvement statistics. Badge Request Forms are used to provide badges to employees, contractors, sub-contractors, and guests to give them physical access to the N3B property. During onboarding, information is collected manually for timecards, taxes, payroll, insurance, etc. Clearance information may also be collected based on the position of the individual.
15. What will be the use of these reports?	Expense reimbursement, payment information, expense reports, tax and payroll data, compliance requirements, oversight reporting to DOE, and process improvement.

MODULE II – PII SYSTEMS & PROJECTS	
16. Who will have access to these reports?	Access to reports containing PII is provided based on the Least User Privilege model. Key personnel in the following areas have roles that are applicable: Human Resources, Project Controls, Finance, Cost Account Managers, Procurement, Safety, Environmental Health, IT Staff with Privileged access accounts, Senior Management, and Security. N3B also shares PII with Los Alamos National Lab (LANL) for badging purposes.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	The information systems do not locate or monitor individuals, except for log aggregation for cyber compliance which does not include PII. Mobile devices may be location enabled; however, the users can disable that feature at any time. Information is obtained in health related forms, HR forms during the onboarding process and payroll/benefits processing, and in the procurement system for the purpose of identification of vendors. Information is also collected as part of processing badges and/or clearances.
18. What kinds of information are collected as a function of the monitoring of individuals?	Social Security Number, Tax ID, banking ACH information, name, address, medical data, Date of Birth.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Network monitoring, firewalls, portable device encryption, and access, control.
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.	The Information System data is protected via Access Control and Multi-factor authentication to protect against modification. Backups occur regularly. Date/time stamps on files are logged and aggregated. The individual application owner and/or device owner is responsible for ensuring that relevant processes are in place to ensure that accuracy, relevance, and completeness has been considered.

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?	System Owners and information owners are responsible for ensuring information is used and managed consistently for its stated purpose in support of the organization. Records are centralized in a record, management system.
Records Management	
22. Identify the record(s).	• Payroll records • Personnel Records • Medical records • Procurement and Contracts • Project Controls • Security for processing badging and clearance related information • Information Technology (file systems and email accessed by authorized individuals)

23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Check appropriately and cite as required. □ Unscheduled ■ Scheduled (cite NARA authority(ies) below) • Records Used to Calculate Payroll, Arrange Paycheck Deposit, and Change Previously Issued Paychecks | GRS 2.4-010 (DAA-GRS-2019-0004-0001) • Time and Attendance Records | GRS 2.4 • Official Personnel Files of Contractor Employees | DOE RDS ADM 1.1 EPI (N1-434-89-1(1)) • Occupational Injury and Illness Files | DOE 2.7, item 100 • Contractor Employee Medical Folder | DOE RDS ADM 1.21.1.a EPI (N1-434-89-1, item 4a) • Financial Transaction Records Related to Procuring Goods and Services, Paying bills, Collecting Debts, and Accounting | GRS 1.1-010 (DAA-GRS-2013-0003-0001) • Issuance Documenting Substantive Functions | DOE ADM 16.1.1 (N1-434-98-19, item 1.1) • Baseline Management | DOE 1.3, item 030 • Personnel Security and Access Clearances | GRS 5.6-181 (DAA-GRS-2017-0006-0025) • Information Technology Development Project Records: Infrastructure Project Records | GRS 3.1-010 (DAA-GRS-2013-0005-0006) • Information Technology Development Project Records: System Development Records | GRS 3.1-011 (DAA-GRS-2013-0005-0007) • Information Technology Operations and Maintenance Records | GRS 3.1-020 (DAA-GRS-2013-0005-0004) • Configuration and Change Management Records | GRS 3.1-030 (DAA-GRS-2013-0005-0005) • Data Administration Records: All Documentation for Temporary Electronic Records and Documentation not Necessary for Preservation of Permanent Records | GRS 3.1-051 (DAA-GRS-2013-0005-0003) • Systems and Data Security Records | GRS 3.2-010 (DAA-GRS-2013-0006-0001) • System Access Records | GRS 3.2-030 (DAA-GRS-2013-0006-0003) • System Access Records | GRS 3.2-031 (DAA-GRS-2013-0006-0004) • Public Key Infrastructure (PKI) Administrative Records: Federal Bridge Certification Authority (FBCA) CAs | GRS 3.2-060 N1-GRS-07-3, item 13a1) • PKI Administrative Records: Other (non-FBCA et. al.) CAs | GRS 3.2-061 (N1-GRS-07-3, item 13a2)

MODULE II – PII SYSTEMS & PROJECTS	
	• Email of Non-Capstone Officials | GRS 6.1-011 (DAA-GRS-2014-0001- 0002) • Access and Disclosure Request Files | GRS 4.2-020 (DAA-GRS-2016-0002-0001) • Privacy Act Accounting of Disclosure Files | GRS 4.2-050 (NC1-64-77-1 item 27) • Erroneous Release Records | GRS 4.2-060 (DAA-GRS-2015-0002-0001) • Telework/Alternate Worksite Program Case Files | GRS 2.3-040 (DAA-GRS-2018-0002-0004) • Employee Relations Programs' Administrative Records | GRS 2.3-010 (DAA-GRS-2018-0002-0001) • Tracking and Control Records | GRS 4.1-010 (DAA-GRS-2013-002-0016)
24. Records Contact	Clifford Anglim clifford.anglim@em-la.doe.gov (505) 309-1347 Dixon Wolf dixon.wolf@em-la.doe.gov (505) 470-0445
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	The Information System is categorized per FIPS-199 as a "Moderate" system. The system implements moderate level controls as defined by NIST SP 800-53 rev 4, Security and Privacy Controls for Federal Information Systems and Organizations. The system is currently in the certification and accreditation process.
26. Who will have access to PII data?	Access to PII is provided based on the Least User Privilege model. Key personnel in the following areas have roles that are applicable: Human Resources, Project Controls, Finance, Cost Account Managers, Procurement, Safety, Environmental Health, IT Staff with Privileged access accounts, and Los Alamos National Lab (LANL) badging office staff will have access to badge-related PII.
27. How is access to PII data determined?	Users access PII data via security group policy and discretionary access controls regulate access based on the user's job function and an established need-to-know based on the job position responsibilities. Application-level access controls may additionally be utilized.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	Data may be pulled from one application into another application/tool for reporting. Specific data, such as timekeeping and payroll, may also be downloaded from an external vendor.

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?	Currently, no ISA's are in place.
30. Who is responsible for ensuring the authorized use of personal information?	Application owner or information system owner is responsible for ensuring the authorized use of personal information. Collectors of PII, such as HR, Procurement, Contracts, etc. are responsible for accurately identifying what information constitutes PII and protecting it in accordance with NIST 800-122.
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	_____ (Print Name) X Jason B. Moore Digitally signed by Jason B. Moore Date: 2022.06.29 16:51:11 -06'00'	_____
Local Privacy Act Officer	_____ (Print Name) X John H. Evans Digitally signed by John H. Evans Date: 2022.06.28 18:08:29 -06'00'	_____
Chief Privacy Officer	_____ (Print Name) X William K. Hunt Digitally signed by William K. Hunt Date: 2022.06.24 13:27:12 -04'00'	_____