



PRIVACY IMPACT ASSESSMENT: ANL - RAMP
PIA Template Version 5 – August 2017

Affects Members Of the Public?

Department of Energy

Privacy Impact Assessment (PIA)

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	April 15, 2021	
Departmental Element & Site	Office of Intelligence and Counterintelligence / Argonne National Laboratory	
Name of Information System or IT Project	Resume Analysis Meta-data Project	
Exhibit Project UID	U.S. Department of Energy Contract DE-AC02-06CH11357	
New PIA <input checked="" type="checkbox"/>	New PIA	
Update <input type="checkbox"/>		
	Name, Title	Contact Information Phone, Email
System Owner	Dan Schabacker, Scientist	630-252-5191 dschabacker@anl.gov
Local Privacy Act Officer	Miriam Bartos Privacy Act Officer (DOE-SC) (Argonne/Low)	miriam.bartos@science.doe.gov
	AndraLeigh (Andy) Rodini Civil Liberties, Privacy, and Professional Integrity Officer (DOE-IN) (Argonne/High)	andraleigh.rodini@doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	John Volmer, Cybersecurity Program Office, Argonne National Laboratory, Department of Energy	630-252-5449 volmer@anl.gov



MODULE I – PRIVACY NEEDS ASSESSMENT

Person Completing this Document	Dan Schabacker, Principle Investigator, Argonne National Laboratory, Department of Energy	630-252-5191 dschabacker@anl.gov
Purpose of Information System or IT Project	The purpose of the Resume Analysis Meta-data Project (RAMP) is to document, track, manage, analyze, and/or report on foreign visits and assignments across DOE facilities as required under DOE Order 142.3A: Unclassified Foreign Visits and Assignments Program, which requires all foreign nationals to present sufficient documentation of immigrant or nonimmigrant status to verify their identity and authorization for a visit or assignment. RAMP collects Visa Type, I-94 number and expiration date, passport number, expiration date, and country of issue, and proof of Lawful Permanent Resident (LPR) status and expiration date.	
Type of Information Collected or Maintained by the System:	<input type="checkbox"/> SSN <input type="checkbox"/> Medical & Health Information <input type="checkbox"/> Financial Information <input checked="" type="checkbox"/> Clearance Information <input type="checkbox"/> Biometric Information <input checked="" type="checkbox"/> Mother's Maiden Name <input checked="" type="checkbox"/> DoB, Place of Birth <input checked="" type="checkbox"/> Employment Information <input type="checkbox"/> Criminal History <input checked="" type="checkbox"/> Name, Phone, Address <input checked="" type="checkbox"/> Other – Please Specify - Visa Type, I-94 Number and expiration date, Passport Number, expiration date, and country of issue, proof of Lawful Permanent Residency (LPR) and expiration date.	
Has there been any attempt to verify PII does not exist on the system? DOE Order 206.1, <i>Department of Energy Privacy Program</i> , 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	PII exists within the system	



MODULE I – PRIVACY NEEDS ASSESSMENT

<i>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.</i>	
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 <input checked="" type="checkbox"/> Federal Employees <input checked="" type="checkbox"/> Contractor Employees

END OF PRIVACY NEEDS ASSESSMENT



MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

<p>1. AUTHORITY</p> <p>What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?</p>	<ul style="list-style-type: none"> • Department of Energy Authorization Act, Title 42, United States Code (U.S.C.), Section 7101 et seq.; 50 U.S.C. 2401 et seq. • Presidential Decision Directive (PDD) 61, <i>U.S. Department of Energy Counterintelligence Program</i>. • Executive Order (E.O.) 12333, United States Intelligence Activities, as amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008).
<p>2. CONSENT</p> <p>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)?</p>	<p>Information is submitted by individuals to DOE sites voluntarily to gain access to the site or for employment. DOE Order 142.3A requires all foreign nationals, including legal permanent residents, present sufficient documentation of immigrant or nonimmigrant status to verify their identity and authorization for a visit or assignment. Valid documentation is required for access to DOE Laboratory space. Should individuals decline to provide the requisite information, they may be denied access to DOE sites.</p>
<p>3. CONTRACTS</p> <p>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?</p>	<p>Yes. Contractors are primarily responsible for designing, developing, and maintaining the system. Personal information from the system may be disclosed to these contractors and their officers and employees in performance of their contracts, and those individuals who are provided this information are subject to the same limitations applicable to DOE officers and employees under the Privacy Act of 1974, 5 U.S.C. 552a.</p> <p>Privacy Act clauses are included in the appropriate contracts. Contract language states that the contractor is subject to the requirements of the Privacy Act and DOE O 206.1, including requirements for access to the information on a need-to-know basis and requirements to safeguard all information they may obtain in accordance with the provisions of the Privacy Act. The contractor also must ensure that all DOE documents and software processed, and the information contained therein, are protected from unauthorized use and mishandling by assigned personnel.</p>



MODULE II – PII SYSTEMS & PROJECTS

<p>4. IMPACT ANALYSIS:</p> <p>How does this project or information system impact privacy?</p>	<p>DOE has assessed RAMP as a moderate-risk system 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.</p> <p>RAMP contains PII relating to individuals' immigration status. Should this information be compromised, it could result in embarrassment and social or professional harm to individuals. In addition, a compromise of this information could potentially harm the reputation of the United States Government abroad.</p> <p>Security controls have been implemented and processes are in place to ensure that controls are operating effectively to mitigate the risk of RAMP from being compromised. All baseline security controls have been implemented and tested as appropriate to its FIPS categorization in accordance with the Senior DOE Management Program Cyber Security Plan (PCSP) and DOE directives. Technical and administrative controls are in place to prevent the misuse of data by individuals with access.</p>
<p>5. SORNs</p> <p>How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?</p> <p>If yes, explain, and list the identifiers that will be used to retrieve information on the individual.</p>	<p>Databases are queried and information is retrieved by last name, first name, and/or visitor number issued to foreign nationals upon their request to visit or work with DOE sites. Foreign nationals may include LPRs.</p>
<p>6. SORNs</p> <p>Has a Privacy Act System of Records Notice (SORN) been published in the <i>Federal Register</i>?</p> <p>If "Yes," provide name of SORN and location in the <i>Federal Register</i>.</p>	<ul style="list-style-type: none"> • DOE-52: Access Control Records of International Visits, Assignments, and Employment at DOE Facilities and Contractor Sites. Federal Register Vol. 74, No.6, Friday, January 9, 2009. Page 1055. • DOE-81: Counterintelligence Administrative and Analytical Records and Reports. Federal Register Vol. 74, No.6, Friday, January 9, 2009. Page 1080.



MODULE II – PII SYSTEMS & PROJECTS

<p>7. SORNs</p> <p>If the information system is being modified, will the SORN(s) require amendment or revision?</p>	<p>N/A</p>
<p>DATA SOURCES</p>	
<p>8. What are the sources of information about individuals in the information system or project?</p>	<p>Foreign Access Central Tracking System (FACTS), which obtains the information directly from foreign nationals seeking access to DOE sites, and similar foreign visit and assignments systems used by DOE National Laboratories which do not participate in FACTS. See FACTS PIA for more information.</p>
<p>9. Will the information system derive new or meta data about an individual from the information collected?</p>	<p>No.</p>
<p>10. Are the data elements described in detail and documented?</p>	<p>Data elements are defined in the system design documents and in user guides.</p>
<p>DATA USE</p>	
<p>11. How will the PII be used?</p>	<p>Data is used to document, track, manage, analyze, and/or report on foreign visits and assignments across DOE facilities. In addition, data will be used in accordance with counterintelligence policies, EO 12333, and DOE Intelligence Activities Procedures.</p>
<p>12. If the system derives meta data, how will the new or meta data be used?</p> <p>Will the new or meta data be part of an individual's record?</p>	<p>N/A. System does not derive meta data.</p>
<p>13. With what other agencies or entities will an individual's information be shared?</p>	<p>Information from the system will be shared with other federal agencies for both Counterintelligence and Intelligence purposes when appropriate. However, no U.S. Persons Information (USPI) will be shared outside of DOE.</p>
<p>REPORTS</p>	



MODULE II – PII SYSTEMS & PROJECTS

<p>14. What kinds of reports are produced about individuals or contain an individual's data?</p>	<p>The system may produce reports containing information on foreign visitors to DOE laboratories including visa type, education, start date and end date of visit/access, country of citizenship, and birth country.</p>
<p>15. What will be the use of these reports?</p>	<p>To document, track, manage, analyze, and/or report on foreign visit and assignment across DOE facilities.</p>
<p>16. Who will have access to these reports?</p>	<p>Federal and contractor Counterintelligence personnel with a valid need to know.</p>
<p>MONITORING</p>	
<p>17. Will this information system provide the capability to identify, locate, and monitor individuals?</p>	<p>No, though the system contains information on access granted to specific DOE sites which may be used to suggest location.</p>
<p>18. What kinds of information are collected as a function of the monitoring of individuals?</p>	<p>N/A. System does not monitor individuals.</p>
<p>19. Are controls implemented to prevent unauthorized monitoring of individuals?</p>	<p>System does not monitor individuals. Security controls have been implemented and processes are in place to ensure that controls are operating effectively to mitigate the risk of RAMP from being compromised. All baseline security controls have been implemented and tested as appropriate to its FIPS categorization in accordance with the Senior DOE Management Program Cyber Security Plan (PCSP) and DOE directives. Technical and administrative controls are in place to prevent the misuse of data by individuals with access.</p>
<p>DATA MANAGEMENT & MAINTENANCE</p>	
<p>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.</p>	<p>All DOE facilities are responsible for providing accurate and current data to FACTS. RAMP pulls data directly from FACTS. As data is updated in FACTS it will be pulled into RAMP.</p> <p>RAMP will not generate new data. If a record is updated within FACTS, the next data update would receive that update. For example, if an individual has a new residence, FACTS would get updated and then RAMP would be updated. RAMP would closely mirror what is stored within the FACTS database. See FACTS PIA for more information.</p>



MODULE II – PII SYSTEMS & PROJECTS

<p>21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?</p>	<p>Argonne is hosting this system within two environments. The first network is a protected enclave wherein the data is structured and organized before exporting to the other Argonne network. The other network is a secured environment requiring user accounts based on their Public Key Infrastructure (PKI) authentication and approval from (DOE-HQ/DOE-IN). Users would use their respective computer systems to utilize the web application and are subject to the same use restrictions and policies across sites.</p>
<p>RECORDS MANAGEMENT</p>	
<p>22. Identify the record(s).</p>	<p>Visitor Access Control Records.</p>
<p>23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.</p>	<ul style="list-style-type: none"> • N1-434-98-21 • N1-434-05-02
<p>24. Records Contact</p>	<p>Roberto Herrera Jr bherrera@anl.gov 630-252-8672</p>
<p>ACCESS, SAFEGUARDS & SECURITY</p>	
<p>25. What controls are in place to protect the data from unauthorized access, modification or use?</p>	<p>Security controls have been implemented and processes are in place to ensure that controls are operating effectively to mitigate the risk of RAMP from being compromised. All baseline security controls have been implemented and tested as appropriate to its FIPS categorization in accordance with the Senior DOE Management Program Cyber Security Plan (PCSP) and DOE directives. Technical and administrative controls are in place to prevent the misuse of data by individuals with access. The system will meet at least a minimum framework of “NIST 800-53 Moderate”.</p> <p>Only Counterintelligence personnel with a valid need-to-know have access to PII. Upon access to the system the user will be presented with a banner acknowledging that the system contains USPI and PII and that such information should be handled and protected in accordance with legal authorities. The banner will be reviewed by legal before the system is enabled for use. The system will be periodically reviewed with the contractor’s cybersecurity office for compliance and validation.</p>
<p>26. Who will have access to PII data?</p>	<p>Only Counterintelligence personnel with a valid need-to-know have access to PII.</p>

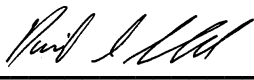


MODULE II – PII SYSTEMS & PROJECTS

<p>27. How is access to PII data determined?</p>	<p>Only individuals needing the information to effectively execute the Counterintelligence duties based on their roles are granted access to the system and the PII contained therein.</p>
<p>28. Do other information systems share data or have access to the data in the system? If yes, explain.</p>	<p>No, but the system does have a user accessible application programming interface (API), so a user could use different toolsets to access the data. If the user logs off the RAMP system, the connection would break and they would have to re-authenticate again using their PKI certificate. This type of access via API would not be a standard activity and would require justification and approval by the Federal project sponsor.</p>
<p>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?</p>	<p>There are no interconnections with other information systems. Data sets are securely exported, assessed for completeness, prepared for ingest and imported to the platform.</p>
<p>30. Who is responsible for ensuring the authorized use of personal information?</p>	<p>Senior Counterintelligence Officer.</p>

END OF MODULE II



SIGNATURE PAGE		
	Signature	Date
Dan Schabacker ANL System Owner	<u> Daniel Schabacker </u> (Print Name)  <u> </u> (Signature)	<u> 04/15/2021 </u>
John Volmer ANL Information Security Manager	<u> </u> (Print Name) <u> </u> (Signature)	<u> </u>
Miriam Bartos DOE-SC Privacy Officer	<u> </u> (Print Name) <u> </u> (Signature)	<u> </u>
Ken Hunt Chief Privacy Officer	<u> </u> (Print Name) <u> </u> (Signature)	<u> </u>