Affects Members Of the Public? Mark if Applicable w/ an 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	March 4, 2024
Departmental Element & Site	Office of International Affairs
Name of Information System or IT Project	DOE Research, Technology, and Economic Security Open Source Tools for Risk Assessments – evaluation pilot
Exhibit Project UID	
New PIA [X] **Update** [ ]	This PIA describes RTES's programmatic effort as well as a pilot use of technologies intended to assist RTES to vet applicants to various financial assistance programs managed by the Department of Energy. Some vetting will be undertaken by DOE and some will be conducted on DOE's behalf by a commercial service provider under contract with DOE. As the program intends to use commercially available data to undertake its risk assessments, the privacy impacts of this activity are likely to be consequential. We are publishing this PIA as a pilot, however, because some of the program's foundational questions are still under review in ways that will impact the privacy interests of individuals and organizations wishing to do business with the department.

MODULE I – PRIVACY NEEDS ASSESSMENT

	For instance, although there is support for the conclusion that existing Privacy Act System of Records Notices (SORNs) cover the intended activities and information collection and uses, the program is currently working with the privacy compliance team to draft and publish a dedicated Privacy Act System of Records Notice that gives greater transparency into their intended uses of PII. Additionally, the program is still learning about the capabilities of the tools they plan to assess during this pilot period, and we anticipate some refinement of the data elements they will use as the program matures. This makes a full examination of privacy impacts premature. Accordingly, we are publishing this impact assessment to address their piloted use of these tools—both in-house and through a commercial contractor—to conduct their risk assessments. The privacy team will remain engaged with the program during this period and revisit this PIA once their SORN publishes and the program participants become more familiar with the data and tools they intend to rely on.

	Name, Title	Contact Information Phone, Email
System Owner	Julie Anderson Margaux Murali Kristen Cadigan Jeannette Singsen	Julie.Anderson@hq.doe.gov Margaux.Murali@hq.doe.gov Kristen.Cadigan@hq.doe.gov Jeannette.Singsen@hq.doe.gov
Local Privacy Act Officer	Audrey Blackwell	audrey.blackwell@hq.doe.gov 202-586-3138
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)		
Person Completing this Document	Kristen Cadigan, Deputy Director, IA-63 Margaux Murali, Deputy Director, IA-63	Kristen.Cadigan@hq.doe.gov 720-356-1789 Margaux.murali@hq.doe.gov 202-586-3698
Purpose of Information System or IT Project	**Background** The United States and our allies continue to face serious evolving research, technology, and economic security threats, as some foreign governments are	

MODULE I – PRIVACY NEEDS ASSESSMENT

working aggressively to acquire our most advanced technologies and dominate strategic supply chains. There have been executive and legislative actions to address some of these threats. In 2021, the White House issued the *Presidential Memorandum on United States Government-Supported Research and Development National Security Policy -- National Security Presidential Memorandum-33* (NSPM-33), which directed a series of actions research agencies must take, "to strengthen the protections of United States government-supported research and development (R&D) against foreign interference and exploitation." Recent legislation, such as the CHIPS and Science Act, directed Federal research agencies to implement research security measures including prohibiting all Federal personnel from participating in any foreign talent programs and prohibiting researchers working on Federal awards from participating in malign foreign talent recruitment programs. Newly established or recently amended DOE programmatic authorities now also prohibit support for "entities of concern" for certain programs. Moreover, as DOE implements the Bipartisan Infrastructure Law (BIL) and the Inflation Reduction Act, even programs that do not have explicit statutory directives must consider RTES risks to ensure proper stewardship of funds and benefits for the American taxpayer.

To ensure a comprehensive RTES approach, DOE is taking two major actions to address the many forms of RTES risks. First, as the Department announced in a memorandum dated March 1, 2023, the Secretary established a RTES Vetting Center (now, the RTES Office in the Office of International Affairs) that will support programs in due diligence reviews and risk mitigation to ensure our national security, economic competitiveness, and technological leadership imperatives are duly incorporated in our financial assistance, loan, and similar activities regardless of the funding source. The RTES Office is responsible for implementing DOE's RTES financial assistance policies to be informed by the RTES Policy Working Group, building RTES awareness within DOE, and engaging with external stakeholders on RTES matters.

DOE Research, Technology, and Economic Security Open Source Tools for Risk Assessments

DOE is implementing risk-based reviews of all DOE-funded projects as part of the broader U.S. Government effort to combat undue foreign influence in Federally funded scientific research. The RTES Office uses publicly and commercially available information to inform its risk assessments.

Tools Supporting the RTES Risk Assessments

The RTES Office will utilize tools directly as well as contract to have a third-party conduct assessments using commercially available tools and report its findings (to include information on foreign ownership, control, and influence) back to the RTES Office.

MODULE I – PRIVACY NEEDS ASSESSMENT

	The RTES Office, and their contractor(s), uses several tools directly and indirectly to complete risk assessments of applications for DOE-funded projects. These include the use of at least four commercially available products offered by aggregators of publicly and commercially available data. Data in these products includes some combination of open-source situational awareness and intelligence on global topics of interest; open-source intelligence; financial data about companies, investments, funds, financials, valuations, and contact information; and information on technology and advice related to preventing compliance breaches, responding to risk, and monitoring ongoing business activities. The information from these data sources will be combined with other information in DOE's holdings to develop a comprehensive risk assessment relevant to the mission of the RTES Program. Under the pilot, RTES will work with the privacy program to evaluate and refine their use of the tools. Over time, we will update this PIA to reflect particular privacy issues that arise from their use or the addition of other tools RTES may use to accomplish its mission.
Type of Information Collected or Maintained by the System:	☐ SSN Social Security number ☐ Medical & Health Information e.g. blood test results X 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 X Employment Information ☐ Criminal History X Name, Phone, Address ☒ Other – Please Specify

MODULE I – PRIVACY NEEDS ASSESSMENT

	The program will use the tools described in this PIA to conduct risk-based assessment of applicants. We expect these tools to provide information about applicant companies' and/or individuals' foreign ownership, control, and influence. This may include financial publicly available financial. We will describe these data elements in more detail in follow-on PIAs.
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 will exist in the system
If "Yes," what method was used to verify the system did not contain PII? (e.g. 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?	Yes
4. Is the information about DOE or contractor employees?	☐ 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.

MODULE I – PRIVACY NEEDS ASSESSMENT

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

1. AUTHORITY **What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?**	The software tools will inform DOE's due diligence reviews, which are authorized by: Presidential Memorandum on United States Government-Supported Research and Development National Security Policy (NSPM-33); Research and Development, Competition, and Innovation Act, Div. B of the CHIPS and Science Act (42 USC 18912, 19231-19237; Public Law 117-167); National Defense Authorization Act for Fiscal Year 2021 (42 USC 6605; Public Law 116-283); National Defense Authorization Act for Fiscal Year 2020 (42 USC 6601 note; Public Law 116-92); DOE Order 486.1A, *Foreign Government Sponsored or Affiliated Activities*.

MODULE II – PII SYSTEMS & PROJECTS

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)?**	Entities and individuals are electing to apply to DOE financial assistance and loans. The Funding Opportunity Announcement (FOA) includes language regarding the required risk review/assessment as applicable to research, technology and economic security (RTES) prior to selection. Failure to provide required information will result in a forfeit of the application. **"Risk Assessment"** Pursuant to 2 CFR 200.206, DOE will conduct an additional review of the risk posed by applications submitted under this FOA. Such risk assessment will consider: **1.** Financial stability; **2.** Quality of management systems and ability to meet the management standards prescribed in 2 CFR 200 as amended and adopted by 2 CFR 910; **3.** History of performance; **4.** Audit reports and findings; and **5.** The applicant's ability to effectively implement statutory, regulatory, or other requirements imposed on non-federal entities. DOE may make use of other publicly available information and the history of an applicant's performance under DOE or other federal agency awards. Depending on the severity of the findings and whether the findings were resolved, DOE may elect not to fund the applicant. In addition to this review, DOE must comply with the guidelines on government-wide suspension and debarment in 2 CFR 180 and must require non-federal entities to comply with these provisions. These provisions restrict federal awards, subawards and contracts with certain parties that are debarred, suspended, or otherwise excluded from or ineligible for participation in federal programs or activities. Further, as DOE invests in critical infrastructure and funds critical and emerging technology areas, DOE also considers possible vectors of undue foreign influence in evaluating risk. If high risks are identified and cannot be sufficiently mitigated, DOE may elect not to fund the applicant. As part of the research, technology, and economic security risk review, DOE may contact the applicant and/or proposed project team members for additional information to inform the review."

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?**	There are three relevant but distinct contract types: 1. Commercial tools acquired by RTES for use in-house: Since these are Commercial-off-the-Shelf products, there is no need for privacy clauses in the acquisition contracts. 2. Contractors supporting RTES in-house: Contractors supporting RTES and the development of its risk-based assessments are subject to Privacy Act requirements as well as DOE Privacy Order, 206.1A. 3. Private companies under contract to conduct external assessments on behalf of RTES: The companies that utilize the tools on DOE's behalf will be bound via contract to adhere to Privacy Act Requirements. As the contract is not yet in place, we will revisit this requirement in future PIAs.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	The use of commercial data is the most significant driver of potential privacy impacts. Each of the tools described in this pilot rely on the use of data that may be subject to data quality issues that are difficult to assess. In some instances, certain data may be more reliable if taken from public or regulatorily-required filings. However, it is difficult to assess the data quality of all the data sources, especially as the particular data sources are still under review. The best way to mitigate this concern is to examine the sources carefully for each intended data element and consider not relying on data that does not meet a reasonableness standard for use. Additionally, consistent with the Privacy Act, giving covered individuals an opportunity to review and correct any incorrect information that may have led to the negative assessment is another important mitigation effort. We will continue to evaluate this process and how it can improved as the pilot develops and report any concrete steps to mitigate identified concerns.

MODULE II – PII SYSTEMS & PROJECTS	
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.**	The information will be retrieved by individual or company name, application number, program office, or control number.
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*.**	As an initial matter, many of the activities in this pilot will not implicate a strict reading of the Privacy Act, as many of the risk assessments will focus on companies and organizations rather than on individuals. This does not mean, however, that there will not be impacts on privacy interests of individuals; nor does it mean that some assessments will be on individuals and therefore implicate the Privacy Act. Accordingly, at the outset of this pilot, DOE will rely on DOE Privacy Act System of Records (SORN) 82, *Grant and Contract Records for Research Projects, Science Education, and Related Activities*, which permits collection of information including, "… financial data… and any other pertinent information needed for the tracking or approval of a grant or contract." More importantly, the Privacy Team and RTES are committed to publishing a Privacy Act SORN specific to the program and its use of data about individuals, which will be additionally informed and refined by this pilot.
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	For transparency, the Privacy Team and RTES are committed to publishing a Privacy Act SORN specific to the program and its use of data about individuals, which will be additionally informed and refined by this pilot.
DATA SOURCES	

MODULE II – PII SYSTEMS & PROJECTS	
8. What are the sources of information about individuals in the information system or project?	Information on the financial assistance or loan application will be provided by the individual or company making the request. Additional information to conduct the assessments will be derived from a variety or other publicly available sources. This information will be aggregated by the tool providers and either accessed directly by DOE or by contractors operating on behalf of DOE.
9. Will the information system derive new or meta data about an individual from the information collected?	Yes, the software tools will be used to generate a consolidated report of the entity and/or individual based on open sources to inform the risk review/assessment.
10. Are the data elements described in detail and documented?	No comprehensive list currently exists. This is a substantial reason this effort is being offered as a pilot. Each of the tools maintains a finite number of data sources, of course, each of which is open-source and/or publicly available. But the RTES program needs to familiarize itself with the tools before a final set is documented. This section will be updated as the PIA is revised.
DATA USE	
11. How will the PII be used?	The names of entities and individuals will be used to conduct open-source risk reviews, either directly by RTES or through a contractor operating on RTES's behalf. The RTES Office uses the results to inform our overall risk assessments and make recommendations to DOE funding offices.
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?**	The new and/or meta data will inform the DOE RTES risk assessments. We complete a new review each time an entity or individual is applying for DOE financial assistance.

MODULE II – PII SYSTEMS & PROJECTS	
13. With what other agencies or entities will an individual's information be shared?	It is worth repeating here that certain assessments will apply to companies and organizations that are not subject to Privacy Act protections, though other limitations may apply. Accordingly, the limits placed on sharing discussed in this section are limited to information about individuals who are subject are afforded protections under the Privacy Act. Currently, information will only be shared in a manner consistent with the Routine Uses described in DOE-82. However, we anticipate expanding permissible sharing in the RTES-specific SORN currently being drafted. This will likely include sharing under a routine use to appropriate federal agencies to demonstrate an inconsistency with DOE's RTES requirements (*e.g.*, disclosure requirements, participation in malign foreign talent recruitment programs contrary to policies issued by DOE, or activities that threaten research, technology, and economic security) to inform efforts related to national and research, technology, and economic security. This includes law enforcement, security, and intelligence agencies, or relevant agency components (i.e., OIG, FBI, CIA, DOD, DOJ, DHS, FDA, NSA, DIA, NRO, and ODNI). This also includes other Federal funding agencies to the to the extent that such sharing is consistent with privacy laws and other legal restrictions and does not interfere with law enforcement or intelligence activities. For purpose of this routine use, sharing with federal agencies will be done in coordination with Office of General Counsel.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	DOE will use the results from the use of DOE acquired tools as well as the risk assessments provided by third parties to compile a single comprehensive DOE risk assessment, based on a variety of risk indicators, including: ultimate ownership, foreign ownership, control, and influence, solvency, reputational issues, export control issues, sanctions, foreign associations/collaborations/connections, foreign patent information, etc.
15. What will be the use of these reports?	Assessments will be used by program officials, in part, to make risk-based recommendations and proposed mitigations to funding offices regarding the projects they intend to select/fund.

MODULE II – PII SYSTEMS & PROJECTS	
16. Who will have access to these reports?	DOE RTES: 1) Risk Analysts 2) Deputy Directors 3) Director 4) Senior Advisor 5) DOE Leadership
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?	N/A
19. Are controls implemented to prevent unauthorized monitoring of individuals?	N/A
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.	As noted above, data quality is a concern when used to make impactful decision about individuals. RTES will conduct risk assessments in a timely manner after the application is received. This gives the best chance that the publicly available information is as relevant and up-to-date as possible. A new application that includes similar individuals who were subject to past reviews will receive a de novo assessment. This will, once again, lead to the most recent data being used.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	This information will be used solely by the RTES team.
Records Management	
22. Identify the record(s).	• Applications, checklists, determinations • internal SOPs, checklists, process documents

MODULE II – PII SYSTEMS & PROJECTS	
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Check appropriately and cite as required. ☐ Unscheduled X Scheduled *(cite NARA authority(ies) below)* DAA-0434-2015-0013-0001 Foreign Ownership, Control, or Influence (FOCI) Files, reports and determinations-successful DAA-0434-2015-0013-0002 Foreign Ownership, Control, or Influence (FOCI) Files, reports and determinations - unsuccessful
24. Records Contact	Clarke, Denise <denise.clarke@hq.doe.gov>
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	Internally there is a small team of federal employees and contractors who will have access to this information, bound by physical, administrative, and technical controls. Third party contractors will sign an NDA and make the identifiers and risk assessments known only to those with a need and authority to know. They will make no other use of the information.
26. Who will have access to PII data?	RTES program officials, third party vendors conducting assessments on DOE's behalf and individuals listed above as being authorized to receive reports.
27. How is access to PII data determined?	On a "need to know" basis outside of the RTES Office. Once the system of record is in place, the results of the risk review, recommended mitigations and final decisions will be included in the system. System access will only include the RTES Office (Management and Risk Analysts). The RTES Office will limit the sharing of information related to the risk reviews, and when there is a need to know, will share with DOE decision makers, as needed to make selection decisions and review recommended mitigations.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	No

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?	N/A
30. Who is responsible for ensuring the authorized use of personal information?	The RTES Office is responsible for providing the entity/individual names to the contractor and then the contractor inputs the names into the software tool to generate the reports which are then provided back to the RTES Office to inform the risk assessments. The RTES Office (Risk Analysts, Deputy Directors, Director) have access to the applications and are responsible for sharing the appropriate information with the contractor (entity/individual name only). RTES will only initiate a risk assessment of individuals and/or entities that have applied to DOE for financial assistance and, thereby, consented to the assessment process.
END OF MODULE II	

SIGNATURE PAGE		
	Signature	**Date**
System Owner	_____ **(Print Name)** KRISTEN CADIGAN Digitally signed by KRISTEN CADIGAN Date: 2024.03.22 13:01:03 -06'00' _____ **(Signature)**	_____
Local Privacy Act Officer	— **(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2024.03.21 16:54:56 -04'00' _____ **(Signature)**	_____
Ken Hunt **Chief Privacy Officer**	**Ken Hunt** _____ **(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2024.03.21 16:55:18 -04'00' _____ **(Signature)**	_____