PRIVACY IMPACT ASSESSMENT
Office of the Chief Information Officer (OCIO), Cybersecurity Operations (IM-33)
Integrated Joint Cybersecurity Center (iJC3)
IM-30 Vendor Risk Management (VRM)

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

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	03/22/2021
Departmental Element & Site	Office of the Chief Information Officer (OCIO), Cybersecurity Operations (IM-33), Integrated Joint Cybersecurity Coordination Center (iJC3) DOE Germantown Campus, Room CA-007
Name of Information System or IT Project	Vendor Risk Management (VRM) FedRAMP Package ID F1305072116
Exhibit Project UID	N/A
New PIA [X] **Update** [ ]	New

	Name, Title	Contact Information Phone, Email
System Owner	Robert Knisely iJC3 Manager Office of the Chief Information Officer (OCIO) Cybersecurity Operations (IM33) Integrated Joint Cybersecurity Coordination Center (iJC3)	301-903-0988 robert.knisely@hq.doe.gov
Local Privacy Act Officer	Brooke Dickson Privacy Management and Compliance Officer / DOE IM-42	202-287-5786 brooke.dickson@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Paul Abulu (CTR) ISSO, iJC3	Office: 301-903-7701 paul.abulu@hq.doe.gov
Person Completing this Document	Robert Knisely iJC3 Manager	301-903-0988 Robert.Knisely@hq.doe.gov
Purpose of Information System or IT Project	The Department of Energy (DOE) has established and operationalized an Enterprise Supply Chain Risk Management (SCRM) program within the Office of the Chief Information Officer (OCIO) to help identify and reduce potential risks associated with DOE third party relationships that provide information technology services and/or products. The Vendor Risk Management (VRM) is an automated tool under a Software-as-a-Service (SaaS) deployment model that provides a risk assessment function on supply chains to DOE and other US Federal Agencies, which will have access to Likelihood findings but not Impact Evaluations (further explained below). DOE currently assesses vendor risks though a manual investigation process, obtaining the requisite information primarily via email and telephone. VRM automates the vendor risk assessment process, allowing for greater efficiency, uniformity, security, and information protection. VRM is a cloud-based web portal to support SCRM operations, which includes tracking, managing, and reporting of: • Requests for Service (RFS), Requests for Information (RFI), Vendor Risk Management; • Non-organizational Federal SCRM access to data within VRM Module. VRM is built on the FedRAMP-approved (SaaS) ServiceNow platform. The VRM module is the DOE SCRM system within IM-30 that manages, treats, and monitors risks and issues associated with existing or new suppliers to DOE and other U.S. Federal Agencies. The VRM Module has two portals for users to access. (1) VRM Portal: The VRM Portal is only accessible to authorized DOE and other Federal employees and contractors through role-based access to: • Provide name, phone number, e-mail, and program office/departmental element (DE) (program office; site; POC; email; name; phone); • Request for Information: Request an open source assessment of a supplier on cybersecurity, compliance, foreign interests, finance, and geopolitics. The open source assessment report will show risk scores and supporting details aligned to the five areas above for the program office/DE lead to decide to pursue or reject a vendor relationship; and	

MODULE I – PRIVACY NEEDS ASSESSMENT

- Request for Service: Request a deep dive assessment of supplier product of services requiring selection of questionnaires based on NIST 800-171 and North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), which is a set of requirements designed to secure the assets required for operating North America's bulk electric system. The deep dive assessment report will show risk scores and details based on the feedback provided within the questionnaires for program offices/DE to decide to procure product or service. This process does not seek or collect any PII, but rather focuses on collecting organization-level documents, e.g., as polices or lists of fourth party companies, to better understand how the supplier operates.
- Following the risk assessment process, vendors are assigned a risk rating from 1 to 5 (5 being the highest risk). VRM contains Impact Evaluations, which evaluate the potential impact of a compromise to the vendor software, and Likelihood findings, which evaluate vendor risk through multiple risk lenses (cybersecurity, compliance, foreign interests, finance, and geopolitics).

(2) Vendor Portal: A public-facing, generic log-in portal through ServiceNow for access by an authorized supplier representative according to role-based access permissions. This portal enables the supplier representative to:

- Provide name, phone number, e-mail, and company name and address;
- Provide feedback on questionnaires assigned to supplier. This consists of yes, no, or not applicable responses with ability to provide comments; and
- Upload supplier documentation to support responses to questionnaires (e.g., company plans and policies).

Both portals require authentication to be completed before gaining accesses to their respective sites. Authentication is supported via OneID, 3rd party multi-factor authentication (Microsoft Authenticator), or EITS RSA token. A PIV (HSPS-12) card will be required to use OneID. The VRM and Vendor web portals require identification and authentication for all users, and OneID further restricts login to those who have PIV cards. External U.S. Federal Agency users will be required to use Multi-Factor Authentication (MFA) but will not be required to go through OneID. VRM Team is receiving support from Public Key Infrastructure Team to use select U.S. Federal Agency persons' PIV authentication certificates for authentication.

The Vendor Portal also has chat functionality to enable communication between DOE SCRM Federal employees and contractors and supplier representatives. Full names of Federal employees and contractors are hidden from supplier representatives to protect their identities. Basic contact information will be collected from the submitter at the site level during initial request for an assessment on behalf of the site. The PII collected and maintained is low sensitivity and protected by administrative and technical controls.

MODULE I – PRIVACY NEEDS ASSESSMENT

Type of Information Collected or Maintained by the System:	☐ SSN ☐ Medical & Health Information ☐ Financial Information ☐ Clearance Information ☐ Biometric Information ☐ Mother's Maiden Name ☐ DoB, Place of Birth ☐ Employment Information ☒ Name, Phone, email address ☐ Criminal History ☐ Name, Phone, Address ☒ Other – Please Specify The information collected depends on the ticket type (Service Request, Request for Information, or Incident Report). For *Vendor assessment requests*: 1. Assessment Request information (type and description) 2. Requester Contact information (name, phone, and email) 3. Requester Office information (program office; site; POC; email; name; phone) 4. Vendor information (name, e-mail, phone, company address) 5. Vendor impact assessment information (open source information on cyber security, foreign interest, geopolitical, compliance, and finance) 6. Vendor deep dive assessment information (information provided by vendor on implemented policies and procedures)
Has there been any attempt to verify PII does not exist on the system?	PII exists on the system

MODULE I – PRIVACY NEEDS ASSESSMENT

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

Threshold Questions

1. Does the system contain (collect and/or maintain), or plan to contain any information about individuals?	Yes (see above).
2. Is the information in identifiable form?	Yes.
3. Is the information about individual Members of the Public?	Yes. A supplier representative provides name, phone number, e-mail, and company name and address.
4. Is the information about DOE or contractor employees?	[**X**] Federal Employees [**X**] 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?**	1. P.L. 106-65, "National Defense Authorization Act [Section 3212(d)], enacted October 1999. 2. Department of Energy Authorization Act, Title 42, United States Code (U.S.C), Section 7101 et. Seq. 3. Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. 4. The Cybersecurity Information Sharing Act of 2015 ("CISA").

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)?**	There are two relevant opportunities: 1) All visitors to the portal will see the following warning banner, which explicitly states that logging in is equivalent to providing consent. An individual, may, of course, choose not to log in to the system. ****WARNING**WARNING**WARNING**WARNING**** This is a Department of Energy (DOE) computer system. DOE computer systems are provided for the processing of official U.S. Government information only. All data contained within DOE computer systems is owned by the DOE, and may be audited, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may disclose any potential evidence of crime found on DOE computer systems to appropriate authorities. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS AUDITING, INTERCEPTION, RECORDING, READING, COPYING, CAPTURING, and DISCLOSURE OF COMPUTER ACTIVITY. ****WARNING**WARNING**WARNING**WARNING**** 2) On several screens (when inside VRM) users have the option to upload attachments (that would contain additional information). User uploads are not mandatory.
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, contractors are involved with the design, development, and maintenance of VRM. Privacy Act compliance clauses are included in all contractor agreements. These require contractors to safeguard all information that they may obtain in accordance with the provisions of the Privacy Act and DOE requirements.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	DOE has established and operationalized an Enterprise Supply Chain Risk Management (SCRM) program within the Office of the Chief Information Office (OCIO) to help identify and reduce potential risks associated with DOE third party relationships that provide information and communications technology. The system's purpose and use will be consistent with that of Incident Response and Security Coordination Teams. VRM is designed to utilize company-level information to better assess vendor risks. Accordingly, VRM is not focused on individuals. PII collected and maintained by VRM is limited to basic contact information for the administration of tickets and requests. Should this information be compromised, it could impact the trust between members of the public, Federal employees, contractors, and the Federal Government. The

MODULE II – PII SYSTEMS & PROJECTS

	potential privacy harm of such a breach is anticipated to be low in light of the low sensitivity of the PII contained in the system. In addition, PII in VRM is protected by a variety of technical and administrative controls and user access has been confirmed to be reliably siloed through penetration testing. The presence of vendor risk ratings within VRM increases the potential privacy harm by association to individuals designated as points of contact on tickets for vendor entities with high risk ratings. VRM does not contain a blacklist of high-risk vendors nor are discussions of risk findings or final decisions on whether to do business with vendors included on tickets containing risk ratings, thereby mitigating the privacy risk. In addition, high risk ratings do not preclude DOE from doing business with vendors and the information is used constructively in practice, as DOE elements may and do choose to provide risk information to vendors so that they may take measures to reduce their risk factors. Use of the vendor portal will be restricted to vendors seeking to do business with DOE who can authenticate via OneID or through a third-party authenticator, such as Authy, Google Authenticator, or Microsoft Authenticator. Users are required to have a verified e-mail address and use a third-party authenticator application for MFA. VRM requires all users to input a one-time pass code from the authenticator. The one-time pass code in the application refreshes every 60 seconds. No PII is collected during this process. The Vendor portal is restricted to authorized new or existing DOE suppliers. Authorized Federal employees and contractors within OCIO will be able to see users' information (name, e-mail, phone, company address). The authorized user from the supplier will be restricted to seeing only their user information. The VRM portal is restricted to authorized DOE and other Federal employees and contractors. Individuals outside of DOE and other Federal agencies will not be able to access the portal. The VRM portal will collect users' name, phone number, e-mail, and office information (program office; site; POC; email; name; phone). Authorized Federal employees and contractors within OCIO will be able to see users' information described above. Program Office and Departmental Elements will be restricted to users' information within their respective program office or departmental element. Authorized external Federal employees and contractors are restricted to their agency's user information. For example, a different Federal Agency will not be able to see DOE users' information.
5. SORNs	While tickets contain PII, they are indexed according to vendor company information, not information relating to individuals. PII is not tagged by an

MODULE II – PII SYSTEMS & PROJECTS

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.**	identifier, name, unique number, or symbol and cannot be routinely searched by any such element. Accordingly, deliberate, indexed retrieval of PII is not possible.
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*.**	N/A.
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?	1) OneID (https://oneid.yc.energy.gov/info/#/idm) and PIV cards will be used to authenticate. Any actual VRM user will need to supply their own PIV card. 2) Once inside the system, a user may enter basic contact information.
9. Will the information system derive new or metadata about an individual from the information collected?	No.
10. Are the data elements described in detail and documented?	Yes. They are described in the FIPS-199 Security Categorization.
DATA USE	
11. How will the PII be used?	The system may contain professional contact information about a Federal employee, contractor, or site employee who is requesting an assessment, requesting access (to the system), or requesting information as well as basic contact information for vendor personnel using the vendor portal. PII is used for administrative purposes and may be retained as part of monitoring logs and files as part of iJC3 security policy.

MODULE II – PII SYSTEMS & PROJECTS

12. If the system derives metadata, how will the new or metadata 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?	Other Federal agencies with whom DOE has entered into a contract will have limited access to Likelihood findings with risk scores within VRM. Individuals designated by vendors as points of contact will be attached to this information. These agencies will not have access to Impact Evaluations. Only SCRM personnel (including VRM system admins) and site-designated entity executives will be able to see tickets that have been submitted by people other than themselves. More specifically, site-designated entity executives will only be able to see tickets concerning their respective organization. Some users will need to be able to have visibility at the Program Office level (which encompasses multiple sites).
REPORTS	
14. What kinds of reports are produced about individuals or contain an individual's data?	Per NIST SP 800-53 / 800-37, VRM is also required to follow several auditing controls. As a result, audit logs are generated. These contain information such as user actions (login time, etc.). VRM hasn't been designed to report on individuals. Rather, its primary function is to document SCRM assessments. However, an individual must be associated with every ticket. It may be necessary to review VRM ticket history. These reports may contain professional contact information. The tickets do not contain PII beyond the name of the individuals submitting them.
15. What will be the use of these reports?	The audit logs will be used by authorized system administrators to review user activity within the VRM module for administrative and security purposes.
16. Who will have access to these reports?	Access is restricted based on role. 1) Authorized iJC3 system administrators and security personnel will have access to reports from all sites. 2) Site-designated entity executives and requesters will be able to view reports that cover only their (respective) sites. 3) Vendor end users will not have any report-viewing capability.

MODULE II – PII SYSTEMS & PROJECTS

MONITORING	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	VRM is not a monitoring or identification system. Certain user actions are required to be logged for security purposes.
18. What kinds of information are collected as a function of the monitoring of individuals?	Auditable user actions are logged, as VRM is required to meet NIST-defined security controls. The system must be capable of auditing based on a risk assessment and mission/business needs in the DOE Program Cyber Security Policy (PCSP). Audit events include successful and unsuccessful logon, account creation / deletion, changes in account profiles, and error conditions. Further details can be found in the VRM Security Plan.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Yes. Technical and administrative controls limit the users who can view audit logs.
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.	There is an annual audit review where the ISSO and other stakeholders will review the details included in system audit records.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	N/A. There is only one production instance of VRM, and it is hosted in the cloud. All system users, regardless of their geographic location, will be accessing this single instance.
RECORDS MANAGEMENT	
22. Identify the record(s).	VRM records will consists of: 1) Data described in Module 1: • Assessment Request information (type and description) • Requester Contact information (name, phone, and email) • Requester Office information (program office; site; POC; email; name; phone) • Vendor information (name, e-mail, phone, company address)

MODULE II – PII SYSTEMS & PROJECTS

	• Vendor impact assessment information (open source information on cyber security, foreign interest, geopolitical, compliance, and finance) • Vendor deep dive assessment information (information provided by vendor on implemented policies and procedures) • Chats between vendors and DOE 2) User actions recorded for system security and administration
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 below)* National Archives Records Administration (NARA) General Records Schedule (GRS) GRS 3.2 Information Systems Security Records, items 010 (Systems and data security records) and 030 (System access records). This schedule covers records created and maintained by Federal agencies related to protecting the security of information technology systems and data, and responding to computer security incidents. This schedule does not apply to system data or content. The Schedules may be found here: https://www.archives.gov/records-mgmt/grs.html https://www.archives.gov/files/records-mgmt/grs/grs03-2.pdf
24. Records Contact	Maria Levesque Supervisory Information Technology Specialist U.S. Department of Energy IM-41 Records Management Phone: 202-586-9527, 703-459-6322 maria.levesque@hq.doe.gov Shannon Hughes IM-30 Phone: 202-586-0089 shannon.hughes@hq.doe.gov
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 VRM and Vendor web portals require identification and authentication for all users. OneID further restricts login to those who have PIV cards. Upon login, privileges are determined by membership in role-based groups. To request privileged access, users are required to follow the iJC3 approval process. Implementation details are described in the system's Security Plan.
26. Who will have access to PII data?	The VRM portal is restricted to authorized DOE and other Federal employees and contractors. Individuals outside of DOE and other Federal agencies will not be able to access the portal. The VRM portal will collect user name, phone number, e-mail, and office information (program office; site; POC; email; name; phone). Authorized federal employees and contractors within OCIO will be able to see user information described above. Program Office and Departmental Elements will be restricted to user information within their respective program office or departmental element. Authorized external Federal employees and contractors are restricted to their agency's user information. For example, a different Federal Agency will not be able to see a DOE user's information. The Vendor portal is restricted to authorized new or existing DOE suppliers. Authorized Federal employees and contractors within OCIO will be able to see user information (name, e-mail, phone, company address). The authorized user from the supplier will be restricted to seeing only their information.
27. How is access to PII data determined?	Access to data in VRM is restricted and role-based. Access to VRM has to be approved by the SCRM Program Director for general user access. iJC3 approval is required for privileged access and to complete any privileged functions, e.g., audit logs.
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

MODULE II – PII SYSTEMS & PROJECTS

30. Who is responsible for ensuring the authorized use of personal information?	The VRM System Owner is responsible for ensuring authorized use of personal information. Access control lists are kept by iJC3 VRM System Administrators and audited according to policy.

END OF MODULE II

SIGNATURE PAGE

	Signature	Date (If not digitally signed)
System Owner	**Robert Knisely** **(Print Name)** Ashton M. Garrett Jr. Digitally signed by Ashton M. Garrett Jr. Date: 2022.01.18 13:11:02 -05'00' **(Signature)**	
Local Privacy Act Officer	**Brooke Dickson** **(Print Name)** Brooke J. Dickson Digitally signed by Brooke J. Dickson Date: 2021.12.21 11:14:19 -05'00' **(Signature)**	
Ken Hunt **Chief Privacy Officer**	**William K. Hunt** **(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2021.12.16 18:24:21 -05'00' **(Signature)**	