



PRIVACY IMPACT ASSESSMENT
Office of Chief Financial Officer
Vendor Invoicing Portal and Electronic Reporting System (VIPERS)

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-chg1-minchg/@@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	July 1, 2024	
Departmental Element & Site	Office of the Chief Financial Officer, Headquarters - Office of the Chief Information Officer (OCIO) EITS Data Center and Cloud Services (DCCS) environment	
Name of Information System or IT Project	Vendor Invoicing Portal and Electronic Reporting System (VIPERS)	
Exhibit Project UID	019-000000122	
New PIA Update	<input type="checkbox"/> <input checked="" type="checkbox"/>	This is an annual update for the PIA. An updated PIA for this system will be submitted to the Chief Privacy Officer for review within twelve (12) months.
Name, Title		Contact Information Phone, Email
System Owner	Katie Shular Office of Corporate Business Systems (CF-40) Office of the Chief Financial Officer (CF) U.S. Department of Energy	240-562-1879 Katie.Shular@hq.doe.gov



PRIVACY IMPACT ASSESSMENT
 Office of Chief Financial Officer
 Vendor Invoicing Portal and Electronic Reporting System (VIPERS)

MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Ana Manchester Office of Corporate Business Systems (CF-40) Office of the Chief Financial Officer (CF) U.S. Department of Energy	301-903-9360 Ana.Manchester@hq.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Ana Manchester, ISSM Office of Corporate Business Systems (CF-40) Office of the Chief Financial Officer (CF) U.S. Department of Energy	301-903-9360 Ana.Manchester@hq.doe.gov
Person Completing this Document	Katie Shular Office of Corporate Business Systems (CF-40) Office of the Chief Financial Officer (CF) U.S. Department of Energy	240-562-1879 Katie.Shular@hq.doe.gov
Purpose of Information System or IT Project	<p>VIPERS is a web-based system that allows government vendors to submit invoices electronically to DOE through a secure portal.</p> <p>VIPERS allows vendors to check the status (received, paid, etc.) of their invoices by logging into the system with email address and password. Under the Actions tab, the vendor then chooses Invoice Status/Funding to see all invoices submitted and a status in the Status column. The Vendor TIN is visible on the VIPERS invoice.</p> <p>DOE Federal employees can use VIPERS to submit invoices for training reimbursements. Federal employees check their status using MFA to log into the system. Under the Actions tab, the federal employee then chooses Invoice Status/Funding to see all invoices submitted and a status in the Status column.</p> <p>Administrators can see the last four of the SSN, banking information, and TIN on an employee invoice.</p> <p>Normal users do NOT see the SSN, banking information, or TIN on an invoice in VIPERS.</p>	
Type of Information	Social Security Number (SSN) – SSN and Tax Identification Number (TIN) <input type="checkbox"/> Medical & Health Information	



PRIVACY IMPACT ASSESSMENT
 Office of Chief Financial Officer
 Vendor Invoicing Portal and Electronic Reporting System (VIPERS)

MODULE I – PRIVACY NEEDS ASSESSMENT

Collected or Maintained by the System:	<input checked="" type="checkbox"/> Financial Information - Personnel events actual or planned that affect compensation or benefits <input type="checkbox"/> Clearance Information <input type="checkbox"/> Biometric Information <input type="checkbox"/> Mother’s Maiden Name <input type="checkbox"/> Date of Birth and Place of Birth <input type="checkbox"/> Employment Information <input type="checkbox"/> Criminal History <input checked="" type="checkbox"/> Name, Phone, Address <input checked="" type="checkbox"/> Other – DOE Employee ID (a 5-digit unique identifier used only within DOE)
-----------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Has there been any attempt to verify PII does not exist on the system? <i>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.</i>	N/A
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----

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



PRIVACY IMPACT ASSESSMENT
Office of Chief Financial Officer
Vendor Invoicing Portal and Electronic Reporting System (VIPERS)

MODULE I – PRIVACY NEEDS ASSESSMENT

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

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.

There are no other additional sources of authority for this system.



PRIVACY IMPACT ASSESSMENT
Office of Chief Financial Officer
Vendor Invoicing Portal and Electronic Reporting System (VIPERS)

MODULE II – PII SYSTEMS & PROJECTS

<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>If the individual declines to provide the requested information, they will not be able to register in VIPERS to process their invoice electronically. New contracts may require vendors to submit invoices via VIPERS. If their contract does not stipulate that they are required to use VIPERS, they can submit a paper copy of the invoice. Use of VIPERS is required for all vendor contracts with very few exceptions.</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>Contractors are involved in the design, development, and maintenance of the system. Contractor roles include both system administration and information administration and processing. Personal information may be disclosed to these contractors and their officers and employees in performance of their contracts. The individuals provided this type of information are subject to the same limitations applicable to DOE officers and employees under the Privacy Act, 5 U.S.C. 552a.</p> <p>Contract language states that data covered by the Privacy Act may be disclosed to contractors and their officers and employees. Any information that is obtained or viewed shall be on a need-to-know basis. Contractors are required to safeguard all information that they may obtain in accordance with the provisions of the Privacy Act and the requirements of the DOE. The contractor shall ensure that all DOE documents and software processed, and the information contained therein, are protected from unauthorized use and mishandling by assigned personnel.</p>



PRIVACY IMPACT ASSESSMENT
 Office of Chief Financial Officer
 Vendor Invoicing Portal and Electronic Reporting System (VIPERS)

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 VIPERS as a moderate-risk systems 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.</p> <p>The unauthorized disclosure of information is expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. Security controls have been implemented and processes are in place to ensure that controls are operating effectively to mitigate the risk of VIPERS being compromised. These include role-based access, further restricted to only the data authorized for their organizations use with the exception of system administrators, and display of the SSNs are limited to only the last four digits.</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>Data is retrieved via the vendor's tax-id number or DOE employee's CHRIS ID.</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>	<p>The system operates in accordance with the following DOE Systems of Records (SORs):</p> <p>DOE-18 Financial Accounting System</p>



PRIVACY IMPACT ASSESSMENT
Office of Chief Financial Officer
Vendor Invoicing Portal and Electronic Reporting System (VIPERS)

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>The system is not collecting new or additional information. The current Systems of Records do not require amendment or revision.</p>
DATA SOURCES	
<p>8. What are the sources of information about individuals in the information system or project?</p>	<p>During invoice submittal, VIPERS accesses DOE’s Standard Accounting and Reporting System (STARS) to retrieve invoice and vendor information to display to the user. When vendors check status of invoices already submitted, VIPERS accesses STARS to retrieve invoice information to display to the user. STARS also contains vendor information obtained from the GSA System for Award Management (SAM) - SAM does not interface directly with VIPERS. The information in SAM is provided by the Vendors.</p>
<p>9. Will the information system derive new or meta data about an individual from the information collected?</p>	<p>No</p>



PRIVACY IMPACT ASSESSMENT
Office of Chief Financial Officer
Vendor Invoicing Portal and Electronic Reporting System (VIPERS)

MODULE II – PII SYSTEMS & PROJECTS

10. Are the data elements described in detail and documented?

Yes.

VIPERS PII data include the following vendor data elements: TIN/SSN, bank account numbers, routing numbers, the name of the vendor, and the address of the vendor.

Banking information is pulled from SAM and displayed on the screen. Our invoices use SAM banking for payment. If the banking is incorrect, the vendor should update SAM before submitting an invoice.

TIN/SSN is from STARS.

Vendor name and address is from STARS. A change of address can be requested via VIPERS.

The vendor is required one time only to submit their contract number and tax ID when registering in VIPERS. This is done for validation. We need to prove that they are the organization that they claim to be.

When the VIPERS vendor submits an invoice, they only submit the amount requested, description, and attach proof of services performed. They do not enter any PII when submitting an invoice. The vendor does verify their banking information on the “verify banking screen”. Any corrections to banking information must be made in SAM.GOV. No corrections to PII data can be made in VIPERS.

DATA USE



PRIVACY IMPACT ASSESSMENT
 Office of Chief Financial Officer
 Vendor Invoicing Portal and Electronic Reporting System (VIPERS)

MODULE II – PII SYSTEMS & PROJECTS

11. How will the PII be used?	<p>The required data elements from the Prompt Payment Act are populated onto the vendor’s invoice based on SAM.gov information. The elements required to constitute a proper invoice include legal business name, tax ID number, address, and banking information.</p> <p>Vendor invoice information is displayed to the vendor for their verification. Certain fields are required for submitting invoices electronically (TIN, banking info, etc.). Changes made will be compared to authoritative sources, and an email sent to the responsible field office site for follow-up.</p>
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?	None
Reports	
14. What kinds of reports are produced about individuals or contain an individual’s data?	None
15. What will be the use of these reports?	N/A
16. Who will have access to these reports?	N/A
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	Yes, but only for the limited use of security purposes system audit logs are maintained to record system activity and user activity.



PRIVACY IMPACT ASSESSMENT
 Office of Chief Financial Officer
 Vendor Invoicing Portal and Electronic Reporting System (VIPERS)

MODULE II – PII SYSTEMS & PROJECTS

18. What kinds of information are collected as a function of the monitoring of individuals?	<p>For security purposes, system audit logs are maintained to record system activity and user activity. This activity includes invalid logon attempts and access and modification to data in the system.</p> <p>The Operating System/Server logs maintained by the EITS environment contains IP information; this is separate from the application/database logging specific to VIPERS.</p>
19. Are controls implemented to prevent unauthorized monitoring of individuals?	<p>VIPERS established policies and procedures for controlling and monitoring access to the system. These are defined in the Security Plan and are compliant with privacy controls in NIST 800-53, rev 4.</p>
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.	<p>VIPERS provides the vendor with a comparison of vendor information between the DOE accounting system and System of Award Management (SAM). The vendor is responsible for reviewing this information. Any changes other than banking changes are captured and emailed to the Payment Center. Banking changes MUST be changed in SAM.</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>The system is only maintained at DOE HQ in the Energy Information Technology Services Data Center and System Services (EITS DC&SS), though it may be accessed by authorized users directly from the internet.</p> <p>Privileged access to the database is only available within DOENET, using 2 factor authentication.</p>
Records Management	
22. Identify the record(s).	<p>Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting.</p>
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	<p>The records in VIPERS have not yet been scheduled electronically but would fall under:</p> <p>Financial Management and Reporting Records: GRS 1.1, items 010, 011, 030, 040, and 050.</p>



PRIVACY IMPACT ASSESSMENT
Office of Chief Financial Officer
Vendor Invoicing Portal and Electronic Reporting System (VIPERS)

MODULE II – PII SYSTEMS & PROJECTS

24. Records Contact

Sean Kennedy, Records Manager

Sean.Kennedy@hq.doe.gov

240-315-6772

ACCESS, SAFEGUARDS & SECURITY

25. What controls are in place to protect the data from unauthorized access, modification or use?

Through the Office of the Chief Financial Officer’s (CF) Assessment and Accreditation program and annual assessment processes, all baseline security controls have been implemented and tested as appropriate to its Federal Information Processing (FIPS) categorization in accordance with the Senior DOE Management Program Cyber Security Plan (PCSP) and DOE Directives. The system was certified and accredited with full Authority To Operate and found to have mitigated risk to an acceptable level.

Technical and administrative controls are in place to prevent the misuse of data by individuals with access. The technical controls include restricted access via MFA based on user responsibility and job function. These access controls are defined in the system security plan. All system team members (Federal and contractor) are required to take the DOE standard cyber security certification course as a necessary prerequisite for the system access. Rules of behavior and consequences for violating the rules are displayed to the user each time the user logs onto the system. Administrative controls include non- disclosure agreements, role-based access so individuals only have access to appropriate personal information, and use of system audit logs to monitor access and user activity in the system.

26. Who will have access to PII data?

Vendors and federal employees will have access to their own information.

Access to PII of others in the system will be strictly controlled based on job responsibility and function. System Administrators and help desk staff will have access to all data in the system. Personnel in the Office of the Chief Financial Officer area will have access to data for payments they are responsible to for.



PRIVACY IMPACT ASSESSMENT
 Office of Chief Financial Officer
 Vendor Invoicing Portal and Electronic Reporting System (VIPERS)

MODULE II – PII SYSTEMS & PROJECTS

27. How is access to PII data determined?	<p>VIPERS users request their access via a dedicated portal (available at https://vipers.doe.gov). VIPERS users register using a TIN/CHRIS ID and Purchase Order (PO) Number which is verified against the STARS PO record, although the access is logged, the system does not save the registration information to the database.</p> <p>Privileged access to the database is role-based and is available only to CF staff.</p>
28. Do other information systems share data or have access to the data in the system? If yes, explain.	<p>Relevant invoice and payment information is retrieved from STARS for verification by the Vendor.</p> <p>There is a data transfer to STARS.</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>There is an Interconnection Security Agreement (ISA) with STARS.</p>
30. Who is responsible for ensuring the authorized use of personal information?	<p>System Owner, the Chief Financial Officer, and the Director for Corporate Information Systems</p>

END OF MODULE II



PRIVACY IMPACT ASSESSMENT
Office of Chief Financial Officer
Vendor Invoicing Portal and Electronic Reporting System (VIPERS)

SIGNATURE PAGE		
	Signature	Date
System Owner	Katie Shular _____ (Print Name) _____ (Signature)	_____ _____
Local Privacy Act Officer	Ana Manchester _____ (Print Name) _____ (Signature)	_____ _____
Chief Privacy Officer	William K. Hunt _____ (Print Name) _____ (Signature)	_____ _____