Affects Members Of the Public?	X

Department of Energy

Privacy Impact Assessment (PIA)

Guidance is provided in the template. See DOE Order 206.1, Department of Energy Privacy Program, Appendix A, Privacy Impact Assessments, for requirements and additional guidance for conducting a PIA: ***https://www.directives.doe.gov/directives-documents/200-series/0206.1-BOrder/@@images/file***

Please complete form and return via email to Privacy@hq.doe.gov

No hand-written submissions will be accepted.

This template may not be modified.

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	03/11/2022
Departmental Element & Site	ITData Center BPA Headquarters, 905 NE 11th Ave, Portland OR
Name of Information System or IT Project	NetBackup, a subsystem of the GSS.
Exhibit Project UID	Contract number: BPA-21-D-87157
New PIA ☐ **Update** ☒	This is an update to the Netbackup PIA signed 5.9.17. This update reflects the additional explanation on How the system supports the BPA mission, What information the system collects and What PII information the system collects.

	Name, Title	Contact Information Phone, Email
Information System Owner	Paul Dickson, JN Supervisory IT Specialist, JN	503-230-4075 prdickson@bpa.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Information Owner	Benjamin Berry, J Chief Information Officer	503-230-4072 blberry@bpa.gov
Local Privacy Act Officer	Candice Palen Privacy Act Officer	503-230-5602 cdpalen@bpa.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Earl Evans Information Systems Security Engineer	503-230-3019 erevans@bpa.gov
Person Completing this Document	Pete Albert	503-230-4228 pjalbert@bpa.gov
Purpose of Information System or IT Project	**The purpose of the system** The NetBackup system provides backup and restore services to various systems and services within the Agency. It is a component of the General Computing Environment General Support System (GCE GSS). Veritas NetBackup is the core solution for the backup systems. The Netbackup system is currently deployed in and managed by Data Center Services (JND). The project supports both disaster recovery and eDiscovery strategies. **How the system supports the BPA mission** It provides data protection (backup/restore capabilities) for components of GCE GSS. **What information the system collects** It collects production data stored on GCE GSS components. **What PII information the system collects** PII information is collected only when backing up systems which collect that data. It is not a primary function of this application.	

MODULE I – PRIVACY NEEDS ASSESSMENT

Type of Information Collected or Maintained by the System:	☒ SSN Social Security number ☒ Medical & Health Information e.g. blood test results ☒ Financial Information e.g. credit card number ☒ Clearance Information e.g. "Q" ☒ Biometric Information e.g. finger print, retinal scan ☒ Mother's Maiden Name ☒ DoB, Place of Birth ☒ Employment Information ☒ Criminal History ☒ Name, Phone, Address ☐ Other – Please Specify
Has there been any attempt to verify PII does not exist on the system? **DOE Order 206.1, *Department of Energy Privacy Program,* defines PII as** *any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.*	N/A, as PII is known to exist on the systems that are being backed up.
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

MODULE I – PRIVACY NEEDS ASSESSMENT

4. Is the information about DOE or contractor employees?	YES or NO (If Yes, select with an "X" in the boxes below) ☒ 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.

The goal of the threshold questions is to legitimately and efficiently determine whether additional assessment is necessary. If there is doubt, it is in the System Owner's best interest to complete Module II.

PIAs affecting Members of the Public are posted on the DOE Privacy website. For this reason, PIAs affecting Members of the Public should be written in plain language and at a high level so they are easily understandable and do not disclose sensitive information.

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

MODULE II – PII SYSTEMS & PROJECTS	
1. AUTHORITY **What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?**	40 U.S.C. §101, et seq. Federal Property and Administrative Services Act of 1949; and 41 CFR 109 Department of Energy Property Management Regulations.
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)?**	The backup system uses software (Veritas NetBackup) to copy images of all systems on the network for disaster recovery, system failure or human error. By using network assets, users are consenting to enlist in backup services.
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, this system uses contractors. Yes, all BPA's contracts involving contractor access to BPA records contain a clause that requires contractors to comply with the Privacy Act per BPA Purchasing Instructions..

4. IMPACT ANALYSIS:

How does this project or information system impact privacy?

The compromise of data contained in Netbackup software could result in HIGH impact. The loss of confidentiality, integrity or availability of data could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

The system presents a potentially HIGH privacy impact due to sensitive PII contained including SSN, financial data, and health data. Should sensitive PII in the system be compromised it could cause serious harm to individuals including professional and financial harm as well as personal and reputational harm should health data be compromised.

The system detects a number of protections to protect privacy and via the Fair Information Practice Principles (FIPPs). The system sereves as backup support and will maintain the minimum PII necessary for its business purpose to mitigate privacy harm. The system was certified and accredited and found to have mitigated risk to an acceptable level.

Netbackup is designed to protect PII and mitigate privacy risk via the following administrative, technical, and physical controls:

- Strict access control enforcement based on need-to-know
- Security Control testing
- Biweekly vulnerability updates

	Impact Level		
Confidentiality Factors	Low	Moderate	High
Identifiability			x
Quantity of PII		X	
Date Field Sensitivity			x
Context of Use		X	
Obligation to Protect Confidentiality			x
Access to and Location of PII		X	
Overall PII Confidentiality Level			x

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.**	Data is not retrieved by personal identifier. Data can only be restored (retrieved from the backup system and made available) to the information owner. Restore requests are submitted via Customer Relationship Management (CRM). Data is restored to its original location to ensure that file permissions remain intact.
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?	Data is backed up into the backup system from a variety of sources including: work group drives, user home drives, database exports, email systems, operating system files, application source code, email system data. The only information that provides demarcation of data is between the server hosting the data and the drive letter that it resides on. In some cases, folder names are specified.
9. Will the information system derive new or meta data about an individual from the information collected?	No

MODULE II – PII SYSTEMS & PROJECTS	
10. Are the data elements described in detail and documented?	N/A
DATA USE	
11. How will the PII be used?	Any data backed up by the NetBackup system is available for restore. Data can be restored to the originator, or to another requestor with approval of the ISO. The Backup System administrators have no oversight into how the information will be used, or whether PII is included.
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 The system does not create meta data. It only creates backup of data stored on systems on GCE GSS.
13. With what other agencies or entities will an individual's information be shared?	Information from the Backup System will not be shared with other agencies or entities. Information from systems being backed up will be shared according to current business practices. See PIAs for those systems for details.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	N/A
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?	No

MODULE II – PII SYSTEMS & PROJECTS	
18. What kinds of information are collected as a function of the monitoring of individuals?	None
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.	The information on the system is kept current by virtue of the backup function with the source systems.
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
Records Management	
22. Identify the record(s).	No records are stored in this system, only images of records from other systems.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	N/A
24. Records Contact	IGLM@bpa.gov
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	The System Owner has implemented and tested all baseline security controls appropriate to its FIPS categorization in accordance with the Senior DOE Management PCSP and DOE Directives. The system was certified and accredited and found to have mitigated risk to an acceptable level. The systems are enrolled in bi-weekly vulnerability updates.

MODULE II – PII SYSTEMS & PROJECTS	
26. Who will have access to PII data?	Members of the group roleEPUServerOperationsBackup have access to the application.
27. How is access to PII data determined?	Data is restored to the originating owner and location upon request. Exceptions to this include: legal requests, AG Audit requests, Cyber Security requests, requests with authorization of Information owner.
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
30. Who is responsible for ensuring the authorized use of personal information?	The original information owners of the backed-up data are responsible for ensuring authorized use.
END OF MODULE II	

SIGNATURE PAGE		
	Signature	**Date**
Information System Owner	PAUL DICKSON (Print Name) Digitally signed by PAUL DICKSON Date: 2023.01.18 13:07:59 -08'00' (Signature)	
Information Owner	Benjamin L Berry (Print Name) Digitally signed by Benjamin L Berry Date: 2023.01.18 14:12:35 -08'00' (Signature)	
Local Privacy Act Officer	Candice Palen (Print Name) Digitally signed by Candice Palen Date: 2023.01.19 09:38:44 -08'00' (Signature)	
DOE Chief Privacy Officer	William K. Hunt (Print Name) Digitally signed by William K. Hunt Date: 2023.01.17 08:58:06 -05'00' (Signature)	