PRIVACY IMPACT ASSESSMENT:
Department of Energy
Office of the Chief Information Officer – IM-62
PIA Template Version 5 – August 2017

Affects Members Of the Public? ☐

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: http://www.directives.doe.gov/pdfs/doe/doetext/neword/206/o2061.pdf

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	July 22, 2020
Departmental Element & Site	Office of the Chief Information Officer (OCIO); Department of Energy (DOE) Headquarters and other DOE locations
Name of Information System or IT Project	DOE Azure System/Environment (DOE Azure)
Exhibit Project UID	Not Applicable
New PIA ☐ **Update** X	Update triggered by personnel changes

	Name, Title	Contact Information Phone, Email
System Owner	Aaron Wisner Information Technology Specialist, IM-62	Room CA-322 19901 Germantown Road Germantown, MD 20874 (301) 903-5247 aaron.wisner@hq.doe.gov
Local Privacy Act Officer	Brooke Dickson Director of Privacy Management and Compliance	(202) 287-5786 Brooke.Dickson@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

	Office of the Chief Information Officer, IM-42	
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Henry Rivera Technical POC IM-63	301-903-0102 Henry.Rivera@hq.doe.gov
Person Completing this Document	Lawrence Orah Information Systems Security Officer (ISSO) IM-63	(240)-306-7671 Lawrence.Orah@hq.doe.gov
Purpose of Information System or IT Project	OCIO uses Microsoft Azure, a large scale enterprise cloud service capability, to provide Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as- a-Service (SaaS) capabilities to DOE customers as a virtual data center. Azure is a platform of interoperable cloud computing services including open-source, standards-based technologies, and proprietary solutions from Microsoft. OCIO utilizes Azure to support data center workload, improve efficiency, and lower costs. This PIA assesses internal DOE use of Microsoft Azure (Azure) cloud-based services as a host environment for DOE applications, systems, and other tools. Privacy assessments relating to DOE Information Technology (IT) systems and applications containing PII within DOE Azure shall be documented in application-specific PIAs. The only PII contained within DOE Azure (not including PII collected or maintained within applications hosted in the Azure environment) resides in Azure Active Directory (AAD) and is limited to basic contact information including name, e-mail address, and telephone number. This limited PII is used for administration of the Azure system including user authentication and directory services. PII within AAD is protected by a variety of administrative, technical, and physical controls overseen by the Cyber Security Expert cited herein (see question 25). DOE Azure is a Federal Risk and Authorization Management Program (FedRAMP)-approved cloud service which undergoes periodic reviews to ensure that all security controls are in place and operating as intended. DOE leverages Azure's multi-tenant public cloud service platform functionality to support SaaS, PaaS, and IaaS cloud service models in order to more efficiently stay up to date with its own security, risk management, and governance. Microsoft is responsible for additional DOE Azure infrastructure support, updates, and maintaining physical security at its data centers. Infrastructure-as-a-Service	

MODULE I – PRIVACY NEEDS ASSESSMENT

	Server hardware is rented along with the necessary software (the hypervisor) to host an application's virtual machine (VM). A hypervisor is a program that enables DOE to host several different VMs on a single server or other hardware. Each VM is able to run its own programs, effectively using the host hardware's processor, memory, and resources. A hypervisor allows DOE to have several VMs all working optimally on a single piece of computer hardware. The VM consists of the operating system, associated system software, and the associated application(s). The laaS deployment model consolidates VMs from their own on-site servers to the cloud servers. Platform-as-a-Service Microsoft maintains much of the system software. This enables DOE's IT & cybersecurity departments to focus on other goals and mandates. The PaaS deployment model enables DOE OCIO to focus on deploying its code on the PaaS machines while the cloud provider helps ensures that operating systems, database software, integration software, and other features are maintained and kept up to date. Software-as-a-Service DOE rents an application from a vendor. This model allows DOE IT departments to focus on provisioning users and data as well as integrating applications with single sign-on (SSO). Azure provides added levels of cloud security at the software layer that meet the security, privacy, and compliance needs of DOE. To manage privacy and security-related concerns, Microsoft has created a Microsoft Azure Trust Center, and Microsoft Azure has services In line with Federal compliance programs and DOE compliance goals. A full and current listing of these services can be found on the Microsoft Azure Trust Center Compliance page.
Type of Information Collected or Maintained by the System:	☐ NONE, N/A ☐ 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

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐ DoB, Place of Birth ☐ Employment Information ☐ Criminal History ☒ Name, Phone, Address ☒ Other –PII may be included in the data streams used by systems and applications within DOE Azure which require application-specific PIAs containing reference to this document.
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 exists in the system.
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?	No.
4. Is the information about DOE or contractor employees?	Yes. ☒ Federal Employees ☒ Contractor Employees

MODULE I – PRIVACY NEEDS ASSESSMENT

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), § 7101 et. seq. • Federal Information Security Modernization Act of 2014 (FISMA), 44 U.S.C. §§3551-3558 • National Defense Authorization Act for Fiscal Year 2015 (Public Law 113-291) § 831, Federal Information Technology Acquisition Reform ACT (FITARA) • 44 U.S.C. Chapter 35, The Paperwork Reduction Act.
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)?**	All systems on the network display a warning banner as required by DOE 0 205.1B, paragraph 4.c (11), which directs that SDM Risk Management Implementation Plans "[m]ust require DOE and NNSA NSS and Federal unclassified systems to display a system use notification (e.g. Warning Banner) at login and require users to electronically acknowledge the warning (such as clicking on 'OK' or 'I agree' button to proceed)." The warning banner requires users to agree before being allowed to proceed. This consent is required to access DOE Azure. A limited amount of credentialing is pulled from AAD for authentication purposes essential to the security of the system. Individuals who access Azure have consented to the Warning Banner and do not generally have the right to decline to provide this information.

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?**	Contractors are involved with the design, development, and maintenance of Microsoft Azure and are subject to the same limitations applicable to DOE officers and employees under the Privacy Act, 5 U.S.C. 552a. Contract language states that data covered by the Privacy Act may be disclosed to contractors. Any information that is obtained or viewed shall be on a need-to-know basis. Assigned contractors are required to safeguard all information they obtain in accordance with the provisions of the Privacy Act and requirements of DOE. The contractors shall ensure that all DOE documents and software processed, and the information contained therein, are protected from unauthorized use and mishandling.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	DOE Azure is 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. To mitigate the privacy risks, DOE has implemented a series of administrative, technical, and physical controls overseen by the Cyber Security Expert cited herein (see question 25). DOE Azure is a FedRAMP approved cloud service provider which undergoes periodic reviews to ensure that all security controls are in place and operating as intended. DOE Azure is rated as FISMA moderate and high baseline moderate based upon the type and sensitivity of data contained within the system. Should information contained within the Azure environment be compromised, the resulting breach could negatively impact the privacy interests of individuals and the trust between individuals whose information is compromised and the federal government. Compromise of the PII specific to Azure, i.e., contact information used for administrative and security purposes in AAD, would have a limited privacy impact, as the PII is limited to low sensitivity basic contact information. The impact of PII maintained in applications hosted within Azure shall be assessed in PIAs specific to those applications.

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.**	PII may potentially be retrieved by name, location, extension, or other personal identifiers through the application within Azure that is being used. Accordingly, applications hosted on Azure require their own PIAs containing reference to this document. Accordingely, data and site owners are responsible for the administration of their respective SORNs. PII stored in Azure Active Directory (AAD) may be searched and retrieved by basic contact information including name, e-mail address, telephone.
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*.**	• OPM/GOV-1 • DOE-5 Personnel Records of Former Contractor Employees • DOE-2 Supervisory Maintained Personnel Records • DOE-11 Emergency Locator Records • DOE-28 General Training Records
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?	AAD information is obtained from DOEInfo and on premises Active Directory servers from which AAD may obtain credentialing and authentication data. Individual Site and Data Owners are responsible for the individual information held in their applications, databases, or provisioned Azure services.
9. Will the information system derive new or meta data about an individual from the information collected?	DOE Azure does not derive new data or create previously unavailable data about an individual through aggregation from the information collected. However, metadata associated with user credentials may be linked to a specific user in order to manage related internal transactions for the security of the system.
10. Are the data elements described in detail and documented?	Yes.

MODULE II – PII SYSTEMS & PROJECTS

11. How will the PII be used?	Data from AAD is used for user authentication and directory services. Proper use of data contained in individual applications, databases, and services is the responsibility of the data owners and is discussed in the corresponding PIAs.
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?**	AAD creates metadata associated with user records which tracks logon and logoff dates and times and account status use to maintain system security and in authentication processes. Although the system does not derive new data or create previously unavailable data about an individual through aggregation from the information collected, new data may be input into the system to support the mission of the organization. Metadata associated with user credentials may be linked to a user.
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?	AAD produces reports for the administration of the Azure console which may contain information about user accounts. Audit trails contained in Azure may contain user identifiers for system security purposes.
15. What will be the use of these reports?	Audit monitoring and network protection. Any reports generated are for administrative and security purposes. The reports will be used for support of system content administration and security, such as incident response investigations.
16. Who will have access to these reports?	Only authorized DOE federal and contractor personnel with elevated privileges will have access.
MONITORING	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	This system does not track the physical identity or location of individuals, nor does it monitor their personal behavior. Azure only records actions taken during use of the system for audit log and security purposes.

MODULE II – PII SYSTEMS & PROJECTS	
18. What kinds of information are collected as a function of the monitoring of individuals?	User actions performed via the console or via application program interfaces (API) are logged. Individuals are not physically identified, located, or their personal actions monitored.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Yes. Access to DOE Azure is only accessible from within the DOE network. Access is limited to authorized federal and contractor employees and is controlled by the system administrator. Site access is controlled by the site administrator. Privileged accounts and tenant accounts are heavily partitioned with privileged account access restricted by role.
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.	Data within the Azure environment is provided by DOE system owners and data owners who are responsible for verifying the accuracy, completeness, and currency of the data.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	Data in AAD is maintained through a single interface which prevents data inconsistency even if the underling system stores data in multiple locations. Automated data replication and synchronization methods are employed. Data in individual applications, databases, and services must be maintained by theindividual data owners.
RECORDS MANAGEMENT	

22. Identify the record(s).	• Information System Security Records
	  ○ Audit/security logs
	  ○ Identity, credential, and access management records
	  ○ Administrative reports for system content administration and security, incident response investigation and user account lifecycle activities
	  ○ Azure active directory
	• DOE customers using Azure will need to identify records and schedules for the information and applications they will host on the cloud service

MODULE II – PII SYSTEMS & PROJECTS	
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	☐ Unscheduled ☒ Scheduled *(cite NARA authority(ies) below)* • GRS 3.2 item 020 - Computer security incident handling, reporting and follow-up records • GRS 3.2, item 030/031 - System access records
24. Records Contact	Maria Levesque; Maria.Levesque@hq.doe.gov; 202-586-9527 Kelly King; kelly.king@doe.gov; 301-903-8708
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	Technical and administrative controls are in place to prevent the misuse of data by individuals with access at both DOE and the cloud service provider. All system team members (federal and contractor) are required to annually complete the Department of Energy Headquarters Annual Cyber Security Refresher Briefing and the Annual Privacy Training as a requirement for access to the system. Administrative controls include separation of duties (so individuals have access only to appropriate personal information) and use of system audit logs (to monitor access and user activity in the system). System administrators have limited access to information, including PII, contained on the site. Site administrators and users may upload information, containing PII, to the site. Rules of behavior and consequences for violating the rules are displayed to the user each time the user logs onto the system.
26. Who will have access to PII data?	DOE federal and contractor personnel will have role-based access to PII in the system in accordance with the policies and controls established by the PII data owner/end user. System administrators have limited access to PII uploaded by data owner/end users.
27. How is access to PII data determined?	Role-based job functions determine an employee's or contractor's access to DOE Azure.

MODULE II – PII SYSTEMS & PROJECTS	
28. Do other information systems share data or have access to the data in the system? If yes, explain.	AAD pulls authentication data from DOEInfo and local Active Directories for the security and administration of Azure.
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?	Where required, there will be Interconnection Service Agreements/ Memorandums of Understanding/Agreements (MOUs/MOAs) between DOE and supporting offices utilizing the O365 instance.
30. Who is responsible for ensuring the authorized use of personal information?	The MS Azure Government Cloud Authorizing Official, as identified in the System Security Plan. Site and Data Owners are responsible for the information contained in their instances.
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	**Aaron Wisner** **(Signature)**	
Local Privacy Act Officer	**Brooke Dickson** Brooke J. Dickson Digitally signed by Brooke J. Dickson Date: 2021.04.08 16:38:12 -04'00' **(Signature)**	
Chief Privacy Officer	**William Ken Hunt** WILLIAM HUNT Digitally signed by WILLIAM HUNT Date: 2021.04.08 15:26:51 -04'00' **(Signature)**	