Affects Members Of the Public? ☐

Department of Energy

Privacy Impact Assessment (PIA)

MODULE I – PRIVACY NEEDS ASSESSMENT		
Date	03/08/2021	
Departmental Element & Site	IM-50	
Name of Information System or IT Project	Google Cloud Broker Platform Services	
Exhibit Project UID	N/A	
New PIA **Update** ☐	New PIA	
	Name, Title	**Contact Information Phone, Email**
System Owner	Jojo Sarpong	202-586-6691 jojo.sarpong@hq.doe.gov
Local Privacy Act Officer	Brooke Dickson	202-287-5786 Brooke.Dickson@hq.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Daniel Mensah, Information System Security Officer (ISSO)	443-805-0579 daniel.mensah@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Person Completing this Document	Daniel Mensah, Information System Security Officer (ISSO)	443-805-0579 daniel.mensah@hq.doe.gov
Purpose of Information System or IT Project	The Innovation Community Center (ICC) Google Cloud Broker Platform Services (GCBPS) is a Department of Energy (DOE) Office of the Chief Information Officer (OCIO) secure cloud services broker that supports the missions of the ICC and the broader Department of Energy Offices and Labs. Specifically, it provides the ICC and other HQ, lab, or office entities rapid access to the Google Cloud Platform (GCP) to develop, test, operate, and maintain applications leveraging Google Cloud Platform FedRAMP Moderate services. The ICC GCBPS will serve as a broker to GCP, managing privileged accounts (Identity, Credentials, Access Management, and Role Based Access Control), ensuring the use of FedRAMP Moderate services in contintental US regions, maintaining perimeter security, and providing consumption based billing, enabling customers to focus on provisioning and protecting cloud services in support of developing, maintaining, and operating systems. GCBPS facilitates the creation of secure enclaves for new applications and provides access as appropriate to each enclave through role-based access controls. As a broker to Google Cloud, GCBPS allows customers to inherit benefits of GCP security controls addressed in its ATO as well as the ICC Broker ATO including billing architecture, security services, and mapping of user roles and corresponding boundaries within the enclave; this prevents each customer from having to build these application support structures manually for each new application within the cloud. Accordingly, customers will be charged based on their consumption through a chargeback model, decreasing their time to market and offsetting some costs to a shared services pool. This enables customers to focus more on development, delivery, and operations of their applications and less on establishing a secure cloud foundation, navigating the complexities of hybrid-poly-cloud network operations and security, onboarding, and maintaining a billing architecture. The only PII collected by or maintained in GCBPS includes basic contact information (i.e., name, DOE email address, and telephone (optional)) used by Identity and Access Management (IAM) for the security and administration of the system. As use of the system is currently limited to a handful of DOE personnel, PII is obtained directly and consensually through coordination with customer offices. Should use of the system expand, this PIA will be updated accordingly.	
Type of Information Collected or Maintained by the System:	☐ SSN ☐ Medical & Health Information ☐ Financial Information	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐ Clearance Information ☐ Biometric Information ☐ Mother's Maiden Name ☐ DoB, Place of Birth ☐ Employment Information ☐ Criminal History ☒ Name, Phone, Address • First Name • Last Name • DOE Email Address • [OPTIONAL] Phone Number ☐ 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.*	PII exists on 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

MODULE I – PRIVACY NEEDS ASSESSMENT

	☒ Federal Employees ☒ 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?	• 42 U.S.C. § 7101 et seq. • 5 U.S.C. § 552a • 10 CFR § 1008
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)?**	Access to GCBPS is “opt-in” by customer request, at which time they’ll have the opportunity to decline to provide information. Should an individual decline to provide information, they may not be granted access to the system.

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 GCBPS 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?**	Should PII within GCBPS 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 GCBPS (i.e., contact information used for administrative and security purposes (Identity and Access Management)) would have a limited privacy impact, as the PII is limited to low sensitivity basic contact information. Also, GCBPS is currently used by only a small number of DOE personnel and therefore contains the PII of a small number of individuals. Finally, PII is obtained consensually through direct coordination with customer offices. This PIA does not consider the impact of PII maintained in applications hosted within the Google Cloud, each of which requires its own PIA. DOE will conduct additional PIAs for applications added to the GCBPS that include PII or have other privacy impacts.
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.**	Identity Adminstrators and Super Administrators with role based access may retrieve basic information by unique identifier (i.e., individual name, role, and system name) for the administration and security of the system.

MODULE II – PII SYSTEMS & PROJECTS	
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*.**	No. Maintenance of information about an individual is not enough to trigger the SORN requirements of the Privacy Act, although it is enough to warrant a PIA. To trigger the SORN requirements of the Privacy Act, information must actually be retrieved by a personal identifier in practice for a purpose beyond the administration of a system. GCBPS has limited, role-based retrieval of limited PII purely for the administration of the system itself not including investigatory or substantive use of PII; as such, it does not require a SORN. As applications are added to the Cloud, DOE will identify the applicable SORNs in PIAs conducted on each particular application involving PII.
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?	As use of the system is currently limited to a handful of DOE personnel, IM-50 will be coordinating directly with customer offices to obtain PII manually and consensually.
9. Will the information system derive new or meta data about an individual from the information collected?	GCBPS will not derive new or meta data about individuals beyond the information contained in audit logs for the security and administration of the system itself.
10. Are the data elements described in detail and documented?	Yes. Data elements are described in Google system support documents.
DATA USE	
11. How will the PII be used?	The PII will be used for the administration and security of the system itself including security alerts related to suspicious login activity.

MODULE II – PII SYSTEMS & PROJECTS	
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?**	Audit log information will be used to generate alerts of suspicious behavior to maintain the security and integrity of the system.
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?	Audit log reports for the security and integrity of the system.
15. What will be the use of these reports?	Audit log reports will be used to generate alerts of suspicious behavior to maintain the security and integrity of the system.
16. Who will have access to these reports?	Identity Adminstrators and Super Administrators with role based access.
MONITORING	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	No. Audit log information will be tied to user accounts and will not provide the ability to locate individuals.
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?	The system does not provide the capability to monitor individuals. Moreover, technical and administrative controls protect the information in the system.
DATA MANAGEMENT & MAINTENANCE	

MODULE II – PII SYSTEMS & PROJECTS	
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.	IM-50 will be coordinating with customer offices to obtain accurate information directly and consensually.
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. The information system is operated at one site.
RECORDS MANAGEMENT	
22. Identify the record(s).	Audit logs, credentials, access management records.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	• GRS 3.2, items 030/031 - system access records • GRS 3.2, item 010 – system and data security records • GRS 3.1, items 010 & 011 - information technology development records • GRS 6.3, item 020 – enterprise architecture records
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 Wellington Burton Records Liaison Official (RLO) and IM-52 301-903-8502 wellington.burton@hq.doe.gov Anthony Carigo RLO IM-53 301-903-8332 anthony.carigo@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?	Security controls have been implemented and processes are in place to ensure that controls are operating effectively to mitigate the risk of GCP being compromised. Google as well as the GCP CBPS System Owner have implemented baseline security controls including Access Controls (AC), Identification and Authentication controls(IA) appropriate to its FIPS categorization in accordance with the Senior DOE Management PCSP and DOE Directives.
26. Who will have access to PII data?	Identity Administrators and Super Administrators
27. How is access to PII data determined?	According to role based job functions.
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?	System Owner.
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	(Print Name) Jojo Sarpong Digitally signed by Jojo Sarpong Date: 2021.04.23 14:41:21 -04'00' (Signature)	
Local Privacy Act Officer	(Print Name) Brooke J. Dickson Digitally signed by Brooke J. Dickson Date: 2021.04.23 13:08:59 -04'00' (Signature)	
Ken Hunt **Chief Privacy Officer**	(Print Name) WILLIAM HUNT Digitally signed by WILLIAM HUNT Date: 2021.04.23 13:04:20 -04'00' (Signature)	