U.S. Small Business Administration
409 3rd Street, S.W.
Washington, DC 20416

Office of the Chief Information Officer

Enterprise Azure Enclave

Privacy Impact Assessment

January 13, 2021

System Owner
Terrence Hudgen
Senior Advisor
Office of the Chief Information Officer
Terrence.Hudgen@sba.gov

Reviewing Official
Keith A. Bluestein
Senior Agency Official for Privacy
Chief Information Officer
Office of the Chief Information Officer
Privacyofficer@sba.gov

This is a Controlled Unclassified Document

I. System Description/General Information

Microsoft Azure is a multi-tenant cloud computing-based subscription service offering from Microsoft that is operational and in production at SBA. Cloud computing has been defined by National Institute of Standards and Technology (NIST) as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction. SBA's Enterprise Azure Enclave utilizes Microsoft's Azure Commercial Cloud Platform as a Service (PaaS) offering and Microsoft's O365 offering (including Exchange, SharePoint, Teams, etc.) to provide an environment for the management and deployment of SBA's Platform services and O365 services. Access to this environment is governed by SBA's on-premise Active Directory via Azure's Active Directory Federation Service (ADFS).
It is important to note that several applications might have been implemented using Azure PaaS services, however these applications may not be within the boundary of EAE and will be managed within their own system boundary.

The EAE is the GSS that serves the enterprise by providing office automation capabilities such as file sharing, directory services, remote access, application hosting, resource provisioning, and document management. The information in the system is about employees. Information about individual members of the public may vary based upon an application captured within the boundary of the system. Information contained in the system uses First Name, Middle Initial, and Last Name combination for simple identification and authentication purposes but does not otherwise collect information about individuals. However, the EAE provides various Platform based services and security controls to the agency as an enterprise, including backup services, application hosting, remote access, and file sharing. EAE is not a first point of collection for PII but utilizes such data from Infrastructure Services system. It is important to note that PII might be maintained within applications such as SharePoint and Exchange, but this is managed by the various SBA offices and related systems.

The EAE is the GSS that serves the enterprise by providing office automation capabilities such as file sharing, directory services, remote access, application hosting, resource provisioning, and document management.

The legal authority supporting the purchase and development of EAE are Small Business Act, Public Law (PL) 85-536 and Federal Information Technology Acquisition Reform Act (FITARA) Pub. L. No. 11 3- 291.

II. System Data

The categories of individuals covered in the system are SBA users. This may vary based on applications captured within the boundary of the system. Sources of the information in the system include Infrastructure Services system and underlying O365 components.
EAE does not directly collect information about individuals. It is incumbent upon the original source systems to validate the data for completeness, accuracy, and current information.

III. Data Attributes

The use of the data is relevant and necessary for the purpose for which the system is being designed. The EAE supports the enterprise by providing office automation capabilities such as file sharing, directory services, application hosting, remote access, and document management. The EAE will not derive any new data or create previously unavailable data about an individual through aggregation from the information collected. Data is usually retrieved by name within the hosted application however, the information retrieved is not necessarily about that individual, therefore a system of records does not exist for the EAE.

IV. Maintenance and Administrative Controls

The EAE has operations in Microsoft Azure FedRAMP approved locations (located within the Continental United States). Cloud systems have the feature or being location agnostic and system settings can be replicated in any site. Currently SBA uses the East location.
The retention period for the supported agency IT systems are governed by the individual Program Offices. The EAE retains all data in accordance with National Archives and Records Administration (NARA) regulations. Data disposition is governed by the SBA Cybersecurity and Privacy Policy (SOP 90 47 5). The system does not use any technologies that may affect public/employee privacy such as monitoring software, Caller-ID, etc.

V. Data Access

Authorized agency users have access to the system based on their specific roles or responsibility: Access to specific EAE file shares is governed by the requesting Program Offices and enforced through Discretionary Access Control Lists (DACLs) and the related originating systems. All users must complete annual cybersecurity and privacy awareness training. In addition, data is

encrypted at rest and in transit. Privacy Act clauses are incorporated into the EAE contracts.

Although the EAE does not directly collect information about individuals, because the EAE provides cloud-based IT infrastructure for the agency, it is assumed that Program Offices routinely generate and store reports from other agency IT systems in EAE repositories. In addition, the EAE provides recovery capabilities to agency IT systems, which may also contain information about individuals.
Senior Agency Official for Privacy (SAOP), Chief Information Security Officer (CISO) System Owner, Information System Security Officer, and System Administrators are responsible for protecting the privacy rights of the pubic and employees affected by any interface.

VI. Privacy Impact Analysis

There is minimal risk related to data type in which the sensitivity of the EAE data elements is mitigated as non-sensitive information for authentication purposes is the general information regarding employees. Risk related to the information is used as intended and the type of information collected.is mitigated in the same fashion. Revelation of EAE data would not have a significant impact to employees. Disclosure of EAE data would not adversely affect any particular vulnerable population.

Privacy risks are mitigated through access control, auditing, secure application design and monitoring, encryption, authentication, and boundary protection. Regarding the relevance of data over time, the aging of data is the responsibility of the source application. Lastly, mitigation is also through education via annual Cybersecurity Awareness and Privacy Training.