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

Office of Government Contracting and Business Development

Certify.sba.gov
Privacy Impact Assessment
September 26, 2023

System Owner
Hilary Cronin
Director of Technology Solutions
Office of Government Contracting Business Development
Hilary.Cronin@sba.gov

Reviewing Official
Stephen Kucharski
Senior Agency Official for Privacy
Acting, Chief Information Officer
Office of the Chief Information Officer
Privacy@sba.gov

I. System Description/General Information

Certify.sba.gov (Certify) is a platform of resources in supporting Small Business Administration's (SBA) mission with aiding government contracting to small business. Its primary component is a custom developed application which includes an interface for small businesses to manage their applications for various contracting support programs, as well as interfaces for SBA staff and other government support staff. The primary function of Certify is to provide SBA with flexible applications to suit the changing needs of the SBA. The legal authority which authorizes the purchase or development of this system/application is "The Small Business Act of 1953, Public Law 85-536, as amended."

Certify is an existing system that is fully operational in production. The last update included veteran-owned small business (VOSB) application; update nor change will not create any new privacy risks. The technological investment does not affect the existing privacy process. Certify includes information about individual members of the public to include applicants and program participants in SBA's 8(a) Business Development program, Mentor Protege Program, Women-owned Small Business Federal Contracting Program, HUBZone Program, and VOSB Federal Contracting Program, personal, business, veteran status and financial information is collected. Certify does not include any information about employees.

II. System Data

The categories of individuals covered in the system are individuals who are business owners, designated employees, and applicable family members such as a spouse of the business owner. The information is primarily collected by individual applicants or designees. Some information is also collected by the website SAM.gov. The U.S. General Service Administration provides business profile data for applicant firms. Information collection consists of: Name, address, telephone number, financial assets, debts, business name, business ownership information, tax information which may include social security tax numbers/tax identification number/employer identification number, and work locations. The forms used for collections are SBA forms: 1010-NHO, 1010-CDC, 1010-ANC, 1010B-AIT, 1010-Representative/Business, 1790-(Outside Assistance), FS-240 Consular Report of Birth Abroad of a Citizen of the United States, and 1010-C 8(a) Business Plan.

Sam.gov data is verified and reviewed for completeness. Individual applicants are required to verify the information from within their profiles. Documents uploaded to the system are reviewed individually by SBA employees.

III. Data Attributes

The use of the data is relevant and necessary for the purpose for which the system is being designed. The system will not drive new data or create previously unavailable data about an individual. No new data will be placed in the individual's record and the system can't make determinations about employees or members of the public that would not be possible without new data. Data is not being consolidated, no reports published on individuals, and "opt-out" options are governed by the collecting Information Technology systems. The system is indexed by the individual firm record may be retrieved by the Data Universal Numbering System (DUNS), Unique Entity Identifier (UEI) or firm name.

IV. Maintenance and Administrative Controls

Certify is facilitated through the Amazon Web Services (AWS) infrastructure, which is available in the AWS East and West zones. All Certify data are replicated in both zones. Certify data are retained for a period of 6 years and 3 months. Originating source supplemental documents, such as WOSB, will be archived based on a General Schedule of Records in accordance to Records Management policy, currently under revision. WOSB applicants are no longer able to append documents via Certify. Regarding disposition, Certify user and administrator guides from the Cloud Service Provider include the procedures for the disposal of records. Records found to be of more than seven years old and no longer part of an active application will be designated for disposal. Additional procedures for disposing data are executed in accordance with NIST SP 800-88 as amended.

Certify monitors the access attempts and failures, logins, submittals, review, edits, and other user activity are collected and remain reviewable records. Role-based access controls and least privilege, auditing, encryption of data in transit and at rest, Cybersecurity Awareness Training for SBA employees, contractors acting on behalf of SBA, partners, etc.

V. Data Access

Authorized agency users have access to associated with their specific roles or responsibility. Contractor staff supporting application processing have access to only the cases assigned to them. Contractors are involved with the design and development of the system and Privacy Act contract clauses are in their contract along with requirement for compliance to Federal Information Security Modernization Act security requirements.
System Operational and Maintenance staff have privileged user access after

successfully obtaining appropriate investigation and clearance for this level of access. Access to the data is determined by Certify account management procedure that governs access based on job description and role. Role based permissions and privileges follow the principle of "least privilege". All users when entering the system agree to the Certify terms and conditions in that the agreement procedure is configurable by SBA to establish intervals, (e.g., each log-in, daily, monthly, annually, etc.)

Other systems do no share data or have access to the data in Certify. Other agencies share data or have access to the data in this system to public data. WOSB firms no longer self-certify and store the related document in Certify where Contracting Officers can access them. The shared data will be used to assess the status of an application and determine its suitability for their requirements for SBA. To assure proper use of the shared data, procedures and policies are in place for the protection of the shared information which includes, this Pia document, system Information Security Agreement, and Memorandum of Understanding along with all supporting System Security Policy procedures. The associated system of records notice for this IT System is SBA 30,, Certify which can be found on our agency's website and the Federal Register's website. Information System Security Officer, Office of the Chief Information Officer's AWS platform administrators, system administrators, the Chief Privacy Officer and the Senior Agency Officials for Privacy are responsible for protecting the privacy rights of the public and employees affected by the interface.

VI. Privacy Impact Analysis

There is a risk related to data type in which the sensitivity of the Certify data elements increases the risk for inadvertent disclosure which is susceptible to identity theft. Some data provides significant information about individuals and businesses to include private and corporate information. Disclosure of Certify data does not increase any impact on vulnerable populations.

Privacy risks are mitigated through access control, auditing, secure application design and monitoring. Access controls restrict visibility to the individual owner and businesses. Encryption of data in transit, incremental and full backups, data integrity checks, data redundancy, and Contingency Planning mitigate the risk of confidentiality, integrity, and availability. Time diminishes the risk slightly as much of the information is intended to be updates on an annual basis however, tax records have longer life value where risks can persist over time; encryption and access control mitigates. Mitigation also through education, Cybersecurity Awareness and Privacy Training.