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

Office of Disaster Assistance
Shuttered Venue Operators Grant System

Privacy Impact Assessment
March 10, 2021
modified April 19, 2021

System Owner
Barbara Carson
Deputy Associate Administrator
Office of Disaster Assistance
Barbara.Carson@sba.gov

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

This is a Controlled Unclassified Document

I. System Description/General Information

SBA provides disaster assistance through its Office of Disaster Assistance (ODA), which coordinates low-interest, long-term loans for damage caused by a declared disaster. In March 2020, as the Coronavirus (COVID-19) pandemic began spreading across the United States. The Shuttered Venue Operators Grant System (SVOGS) is a new cloud-based Software as a service (SaaS) system by Salesforce for the Office of Disaster Assistance (ODA). The system was established on behalf of the Shuttered Venue Operations Grant Program as part of Section 324 of the " Economic Aid to Hard-Hit Small Businesses, Nonprofits and Venues Act" signed into law on December 27, 2020. The statute calls for the SBA's Associate Administrator, ODA, to implement the billion dollars grant program. This represents the first grant program within ODA that must comply with applicable Uniform Guidance (2 CFR 200) requirements

SVOGS has a universal resource locator (URL) www.sba,gov/svog to allow a venue operator to demonstrate interest in this program. This URL catalogs business name, industry, email, city, states, and zip code. The SVOGS 1.0 contains personally identifiable information (PII) about individuals with user level data necessary for disposition of the Shuttered Venue Operators Grant applications. SVOGS does not contain information about SBA employees.

On April 18, 2021, the SVOGS was updated to include batch data matching with Treasury Department on behalf of the Do Not Pay (DNP) program. The data sharing and matching will not create any unmitigated privacy risks

II. System Data

The categories of individuals covered in the system are Small businesses and principals. Voluntary participation for collection as the application process obtains the applicant's intent to apply for financing and for their information to be used to that end. . Being a streamlined processing system, required information is generally the only one requested.

The information is primarily collected by individual applicants as well as other resources, such as SBA's E-Tran, Joint Administrative Accounting Management System (JAAMS), and Payroll Protection Program (PPP). Some information is also collected by the website SAM.gov, Treasury Department's Internal Revenue Service and Do Not Pay program. Information collected from individuals and various sources consists of: Social Security Numbers (SSN), Automatic Clearing House, date of birth, name, income, driver's license or state/federal identification information, business addresses, assets, telephone number, expenses, tax returns history, tax identification number, email address, Employer Identification Number

(EIN), DUNS number, insurance policy number, grant numbers, and handwritten signature.

Data obtained from the applicant has required fields for processing to ensure complete information is provided. The data is checked against other sources to include a representative double checking for completeness and fraud prevention check. A Grant Officer or Team Lead will ultimately use their knowledge and experience to make a final determination on accuracy. The data is current at the time of its being entered into the system or requested from third parties. The data elements collected are described in detail and documented.

III. Data Attributes

The use of the data is relevant and necessary for the purpose of the grant program for which the system is designed. The system is indexed mainly by the application or grant number and reports from the system are currently under review for development. 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.
The SVOGS 1.0 protects individuals' privacy data through access control, strong authentication, auditing, and monitoring. Also, the Reviewer of the information will sign a "Conflict of Interest Statement."

IV. Maintenance and Administrative Controls

The SVOGS is operating under the Privacy Act systems of records notice SBA 20. The system is hosted in a cloud environment with backups. The retention periods of data in this system are in compliance with SBA policy and the National Archives and Records Administration's General Schedule. The procedures for disposition of the records are applicable to the current Standards Operating Procedures of Records Management. Additional procedures for disposing data are executed in accordance with National Institute of Standards and Technology Special Publication 800-88, as amended

The system does not use any technologies in ways that SBA has not previously employed, for example, no monitoring software, caller -identification, etc. This system does not provide the capability to identify, locate, or monitor individuals in real time. designated for disposal.

V. Data Access

Agency officials and certified contractors will have access to the data in the

system. Access is limited to Agency officials acting in their official capacity, with a need to know, and certified contractors under confidentiality agreements while engaged in system development, modification, or maintenance. This may include users, managers, or system administrators. Privacy Act clauses are in each respective contract for the contractors that are involved in the design, development, and maintenance of the SVOGS 1.0 information system.

Access to the data is determined by the individual's role and responsibility. Access is restricted based upon the level of system responsibility assigned users by their managers and approved by the SVOGS Information System Security Officer, the Contracting Officer (in case the user is a not an employee) and the System Owner. System end-users are members of the public, and as disaster survivors, access is open for data entry of application submission.
Access is limited and restricted by control of User IDs, password controls, and the assignment of a "Responsibility Profile" to all user-ids. Each responsibility comes with a pre-determined set of privileges, limiting data that may be viewed to those screens and reports that are within the duties and needs of the user. User access policies and procedures for the SVOGS have been published. Also, everyone must take Cyber Security Awareness training which includes a Privacy module.

Data is routinely shared with other systems. The system provides the Treasury Department Tax Identification number, DUNS number, business or individual name for batch matching response file supporting Do Not Pay information. The system currently does not exchange data with ETRAN. Agreed upon data elements are transmitted as discrete packets sent over secure interfaces or approved technologies. Information System Security Officer, system administrators, and Senior Agency Official for Privacy are responsible for protecting the privacy rights of the public and employees affected by the interface.

Grant Reviewers will be provided access based upon access provisioning and permissions to include Power BI reports. For this purpose, sensitivity of the data elements, access control is monitored on a regular basis to ensure active members are added and removed as they are assigned. This will be done via our ticketing system to add/remove from security group.

VI. Privacy Impact Analysis

There are risks related to disclosure of individuals' privacy. Risks to the type of data, ensure information used as intended, safeguard unauthorized monitoring of privacy data, and protect information shared internal and external. The sensitivity of the SVOGS data elements increases the risk for inadvertent disclosure which is susceptible to identity theft. Some data provides significant information. Salesforce, ODA, and Office Chief Information Officer provides security and

privacy controls for safeguarding the handling of PII data in the SVOGS system.

Privacy risks are mitigated through access control, auditing, secure application design and monitoring, encryption, and authentication. Mitigation also includes limiting context regarding grant information and ensuring collection is comparable to its' collection; ensuring collection follows statutory authority to collect, encryption of data in transit and at rest; incremental and full backups, data integrity checks, data redundancy, and Contingency Planning.
Regarding the relevance of data, time diminishes the risk slightly as much of the information is intended would no longer be current or potentially applicable.
Lastly, mitigation is also through education via annual Cybersecurity Awareness and Privacy Training.