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

# Office of Disaster Recovery and Resilience (ODR&R)

# Shuttered Venue Operators Grant System
# Privacy Impact Assessment

**November 24, 2024**

Revised June 2025

| Template Owner Details | |
|---|---|
| Name | Michael Post Chief Information Security Officer (Acting) |
| Contact Number | (202) 205-3645 |
| E-mail Address | Michael.Post@sba.gov |

**Privacy Impact Assessment (PIA) Approval Page**

The following individuals have approved this document:

**System Owner (SO)**

MICHAEL YEAGER Digitally signed by MICHAEL YEAGER Date: 2025.06.12 13:39:46 -04'00' **(Signature & Date)**

Michael A. Yeager, Director, Data Analytics & Information Technology
Data Analytics & Information Technology (DAIT)
Michael.Yaegar@sba.gov

**Chief Information Officer (CIO) (Alternate DCIO or CISO may sign)**

MICHAEL POST Digitally signed by MICHAEL POST Date: 2025.07.01 09:26:02 -04'00' **(Signature & Date)**

Hartley M. Caldwell IV, Chief Information Officer,
Office of the Chief Information Officer
Hartley.Caldwell@sba.gov



Controlled Unclassified Information

## A. CONTACT INFORMATION

1) **Who is the person completing this document?**
Timothy S. Baughman, Information System Security Officer/IT Project Manager
Office of Disaster Data Analytics & IT (DR&R)
Timothy.baughman@sba.gov

1) **Who is the Information Systems Security Manager?**
Michael Post, Chief Information Security Officer (CISO) (Acting),
Office of the Chief Information Officer
Michael.Post@sba.gov

2) **Who is the Senior Advisor who reviewed this document?**
Hartley M. Caldwell IV, Chief Information Officer,
Office of the Chief Information Officer
Hartley.Caldwell@sba.gov

3) **Who is the Reviewing Official on behalf of SAOP?**
Michael Post, Chief Privacy Officer (CPO) (Acting),
Office of the Chief Information Officer
Michael.Post@sba.gov

## B. SYSTEM APPLICATION/GENERAL INFORMATION

The U.S. Small Business Administration (SBA) Office of Disaster Recovery and Resilience (ODR&R) oversees the Shuttered Venue Operators Grant (SVOG), which coordinates grants under the Economic Aid to Hard-Hit Small Businesses, Nonprofits, and Venues Act, as amended by the American Rescue Plan Act. The program includes over $16 billion in grants to shuttered venues, to be administered by SBA's Office of Disaster Assistance. The SVOG information system, does not take any new applications currently and was used to process COVID-19 Grant applications from shuttered venues impacted by the financial challenges of the coronavirus pandemic.
The SVOG information system, a cloud-based Salesforce Software System implemented by ODR&R, processes the COVID-19 Disaster Grant for venues affected by the financial challenges of the pandemic. The mission of the SVOG program is to support the ongoing operations of eligible live venues and operators, including live venue promoters, theatrical producers, talent representatives, live performing arts organizations, museums, and motion picture theaters during the uncertain economic conditions caused by COVID-19.

**Note:** SVOG is no longer accepting new applications. However, the SVOG portal remains open for all active applicants and awardees https://www.svograntportal.sba.gov/s/.

1) **Does this system contain any information about individuals? If yes, explain**.
The Shuttered Venue Operators Grant System (SVOG) contains personally identifiable information (PII) necessary for processing grant applications, including Social Security Number (SSN), Automatic Clearing House (ACH) details, 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, business email address, Employer Identification Number (EIN), DUNS number (before 2022), System for Award Management (SAM.gov) UEI

number, insurance policy number, grant numbers, and handwritten signatures. This data is collected to verify eligibility and process grant applications.

**a. Is the information about individual members of the public?**
Yes. The applicants who applied for the grant.

**b. Is the information about employees? (Yes/No)**
No, all information pertains to Grantees and their designated POCs.

2) **What is the purpose of the system/application?**
The SVOG information system is used to process COVID Disaster Grant applications from shuttered venues impacted by the financial challenges of the coronavirus pandemic, serving a unique purpose for carrying out the mission.

**3) Is the system in the development process? (Yes/No)**
No.

**4) How will the technology investment (new or updated) affect existing privacy processes?**
SVOG is a Government Cloud-based + Hyper force development effort and will not affect the privacy process.

*5)* **What legal authority authorizes the purchase or development of this system/application? (**Statute, Executive Orders, etc.)
The Shuttered Venue Operators Grant (SVOG) program is Section 324 of the Economic Aid to Hard-Hit Small Businesses, Nonprofits and Venues Act (Economic Aid Act),
Small Business Act [Public Law 85–536]

**6) Privacy Impact Analysis: What privacy risks were identified and describe how they were mitigated for security and access controls.**
Office of Management and Budget (OMB) Memorandum 17-12 (M-17-12) identifies risks of disclosure of individuals' privacy data in five major areas. The table below identifies those risk areas and the mitigating strategies for each.

| Potential Risk | Mitigating Strategies |
|---|---|
| Sensitivity of Data Elements | The sensitivity of data elements is mitigated using access control, auditing, monitoring, authentication, encryption, and boundary protection. |
| Context of the Data | Context of data elements is mitigated using access control, auditing, monitoring, authentication, encryption, and boundary protection. |
| Revelation of Private Information | Revelation would have a significant negative impact by exposure to proprietary information. Mitigated through the use of access control, auditing, monitoring, authentication, and boundary protection. |
| Impact on Vulnerable Populations | This system does not specifically track or document vulnerable populations. Grants were awarded solely based on the application, qualifications, and specific needs of the applicant. While any data exposure would impact grantees, we do not have statistics on vulnerable populations because we did not grant based on those |



Controlled Unclassified Information

| | |
|---|---|
| | criteria. We did not give preference to any vulnerable organizations or populations. |
| Relevance of the Data Over Time | Data are kept current and remain relevant over time. Mitigation includes maintaining role-based access controls, data integrity, data validation, and auditing to ensure data is current and relevant. The system protects grantee-provided data. We have a document auditing history. User-level monitoring and audits are also conducted. Internal controls are used to revalidate data. OIG and OGC also conduct reviews. Even after grants are closed, grantees can still access their files in a view-only mode. We strive to maintain a "rule of two" for reviews and approvals to ensure data integrity. We constantly monitor data, assess its validity, and track changes through audit histories. Data is protected throughout the process. Changes are tracked, and original data is preserved. Access is role-based to prevent any single individual from controlling an entire file's progress. |

## C. SYSTEM DATA

1) **What categories of individuals are covered in the system?**
Small businesses, nonprofits, and venues impacted by COVID-19 that applied for the SVOG program, including their owners, executives, and designated points of contact.

2) **What are the sources of the information in the system?** (Including an informational data flow would be a great opportunity here.)
The system contains applicant-supplied data as well as third-party information lookups based on that data obtained for validation and verification reasons. The individual, as the applicant/grantee, is required to create a SAM.gov account as the source of the information. Systems provide validation information and records of transactions that are directly linked to the grantee records. SBA system: E-Tran, Joint Administrative Accounting Management System (JAAMS), Payroll Protection Program (PPP), Capital Access Financial System (CAFS), Federal Awardee Performance and Integrity Information System (FAPIIS), LexisNexis searches, Restaurant Revitalization Fund Grant (RRF), Treasury (DNP/ IRS (4506T)), SEC (for verification if publicly traded), and state-specific business registration entities.

   a. **Is the source of the information from the individual, or is it taken from another source? If not directly from the individual, then what other source?** (Please be specific to include form numbers where applicable.)
   The primary source of information is the individual applicant, who submits their information via the SVOG portal. The system also collects validation data from third-party systems, including IRS, Treasury (Do-Not-Pay system), SAM.gov, LexisNexis, SBA's E-Tran, JAAMS, CAFS, and FAPIIS.

   b. **What Federal agencies are providing data for use in the system?**
   The system receives data from the IRS, Treasury's Do-Not-Pay (DNP) system, SBA's E-Tran, and JAAMS, as well as other federal databases, including FAPIIS and SEC (for verifying publicly traded companies).



Controlled Unclassified Information

**c. What Tribal, State, and local agencies are providing data for use in the system?**
Not Applicable

**d. From what other third-party sources will data be collected?**
The SVOG system manually collects and verifies data from third-party sources, including SAM.gov, FAPIIS, LexisNexis, Restaurant Revitalization Fund Grant (RRF), Treasury (DNP/IRS 4506T), SEC (for publicly traded businesses), and state business registration entities.

**e. What information will be collected from the employee and the public?**
The applicant provides personally identifiable information (PII) and business-related data necessary for grant eligibility and processing. This includes Social Security Numbers (SSN), Automatic Clearing House details, date of birth, name, income, driver's license or state/federal ID information, business addresses, assets, telephone numbers, tax returns, Employer Identification Number (EIN), DUNS number, System for Award Management (SAM.gov) UEI number, insurance policy numbers, and grant numbers.

**3) Accuracy, Timeliness, and Reliability**

**a. How is data collected from sources other than SBA records verified for accuracy?**
Data obtained from applicants is checked against other sources for completeness and fraud prevention. Staff manually reviews third-party information, validating key data and personal information to ensure compliance and verify the identity of the person and business. All grantees were required to use a SAM.gov account to validate their identity. Applicants had to provide specific information, including a copy of their driver's license or identification card. This information is reviewed and validated by multiple people.

- Data verification includes cross-referencing applicant-provided information with third-party databases such as IRS (4506T), SAM.gov, DNP, and LexisNexis for fraud prevention. The SVOG Grant Management Specialist (GMS) and Supervisors validate and review data integrity and completeness before approval.

**b. How is data checked for completeness?**
Application forms on the SVOG portal have required fields as applicable as well as field-level validation. Internal process flows require validation checks with third-party systems before approval and screenshots of the resulting information to be captured within the Salesforce system, which is reviewed by GMS and the Supervisor.
Applications are required to complete multiple forms within the SVOG portal, requiring mandatory fields and submission of required documents. The SVOG system utilized data validation checks to ensure that data was present and was of acceptable format. The final data verification is the staff manually reviewing the grantee-provided information and the required documents for completeness and, if there was a lack of data, would request the information from the grantee by use of a system-managed and monitored "action item." These required fields and documents were reviewed by the Grant Management Specialists (GMS) and Supervisors.
As the grant was moved through the processing and decision-making processes, if additional requirements were identified, the processor would request additional.



Controlled Unclassified Information

Information as needed. All requests are captured within the system, either as file uploads, completed fields, emails from the grantee, or staff-generated documents that have been uploaded to the record.

**c. Is the data current? (Yes/No)**
The data is current at the time of its being originally entered into the system, and additional information is requested as required.

**d. Are the data elements described in detail and documented? (Yes/No)**

Yes, this is described in the data dictionary, along with the SVOG Architectural Diagrams and SVOG High-Level Solution Design, as documented in the SVOG SSP.

**4) Privacy Impact Analysis: Discuss what privacy risks were identified and how they were mitigated for the types of information collected.**

Office of Management and Budget (OMB) Memorandum 17-12 (M-17-12) identifies risks of disclosure of individuals' privacy data in five major areas. The table below identifies those risk areas and the mitigating strategies for each.

| Potential Risk | Mitigating Strategies |
|---|---|
| Sensitivity of Data Elements | The sensitivity of data elements is mitigated through the use of access control, auditing, monitoring, authentication, encryption, and boundary protection. |
| Context of the Data | Context of data elements is mitigated through the use of access control, auditing, monitoring, authentication, encryption, and boundary protection. |
| Revelation of Private Information | Revelation would have a significant negative impact and is mitigated through the use of access control, auditing, monitoring, authentication, and boundary protection. |
| Impact on Vulnerable Populations | Disclosure of data would adversely affect individuals, but this would not be focused on any vulnerable population. |
| Relevance of the Data Over Time | Data are kept current and remain relevant over time. Mitigation includes access control, auditing, monitoring, authentication, encryption, and boundary protection. |

## D. DATA ATTRIBUTES

**1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**
Yes, the data collected is necessary to process grants and determine eligibility for SVOG in compliance with the Economic Aid Act.



Controlled Unclassified Information

2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**
No

3) **Will the new data be placed in the individual's record?**
N/A

4) **Can the system make determinations about employees or members of the public that would not be possible without the new data?**
No

5) **How is the new data verified for relevance, timeliness, and accuracy?**
N/A

6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**
Not Applicable because the system collects information but does not consolidate the information.

7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? If the process is not consolidated, please state "N/A."**
N/A

8) **How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**
Records are retrieved by the name of the individual, business name, application number, grant number, and Data Universal Numbering System. The data is mainly retrieved via a business name or grant application number. Also, use a business name in combination with a unique identifier such as EIN, DUNS number, and SAM.gov UEI number.

9) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**
Ad hoc Reports are currently limited to being generated by request as needed. Reports may include approved grant details such as Grantee Name, Business Address, Venue Type, Award Date, and Total Awarded Grant Amount.

10) **What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how can individuals grant consent?**
Applicants provide consent by submitting their information in the grant application. Consent is implied for required processing, but individuals may request access, correction, or contest records through FOIA and Privacy Act procedures.



Controlled Unclassified Information

**Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is used as intended.**

OMB Memorandum 17-12 (M-17-12) identifies risks of disclosure of individuals' privacy data in five major areas. Details regarding the mitigation strategies of each associated risk are answered in Section B, response 6 of this PIA.

Office of Management and Budget (OMB) Memorandum 17-12 (M-17-12) identifies risks of disclosure of individuals' privacy data in five major areas. The table below identifies those risk areas and the mitigating strategies for each.

| Potential Risk | Mitigating Strategies |
|---|---|
| Sensitivity of Data Elements | The sensitivity of data elements is mitigated using access control, auditing, monitoring, authentication, encryption, and boundary protection. |
| Context of the Data | Context of data elements is mitigated using access control, auditing, monitoring, authentication, encryption, and boundary protection. |
| Revelation of Private Information | Revelation would have a significant negative impact and is mitigated through the use of access control, auditing, monitoring, authentication, and boundary protection. |
| Impact on Vulnerable Populations | Disclosure of data would adversely affect individuals, but this would not be focused on any vulnerable population. |
| Relevance of the Data Over Time | Data are kept current and remain relevant over time. Mitigation includes access control, auditing, monitoring, authentication, encryption, and boundary protection. |

## E. MAINTENANCE AND ADMINISTRATIVE CONTROLS

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**
The data is stored within a government-level encrypted Amazon Web Service (AWS) and uses a government-level Salesforce (GovCloud+ Hyper force) cloud environment to interface with and update data accordingly. Having and maintaining a centralized location for secure data housing and validation enables grantees and staff to enter information and data, and it ensures proper data validation if completed.

2) **What are the retention periods of data in this system?**
Grantees must maintain SVOG award files for four years following the initial award Notice of Award (NOA) issuance for employment-related records and three years for all other records, per SBA Records Management Policy.
The system is hosted on a secured AWS Cloud environment with backups. SVOG follows Data Retention policies and routinely reviews all forms of compliance with the agency,



Controlled Unclassified Information

3) **What are the procedures for the disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**
Data disposal follows SBA Records and Information Management SOP 00-41-03 and NARA General Records Schedule guidelines. Disposal includes secure deletion and de-identification of sensitive data.

4) **Is the system using technologies in ways that the SBA has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**
No

5) **How does the use of this technology affect public/employee privacy?**
N/A

6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**
No

7) **What kinds of information are collected as a function of the monitoring of individuals?**
No monitoring of individuals is conducted.

8) **What controls will be used to prevent unauthorized monitoring?**
Access is controlled through User IDs, password controls, multi-factor authentication, role-based access, and auditing of security-related events.
Strong encryption (data in transit and at rest), auditing of security-related events, and contractual agreements.

9) **Under which Privacy Act systems of records notice (SORN) does the system operate? Provide the number and name.**
System of Records Notice (SORN) SBA-20:

10) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision?**
Yes.

**F. DATA ACCESS**

1) **Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, tribes, and others)**
Agency officials, SBA contractors, regulators, and experts engaged by the SBA will have access to the data in the system, limited by role-based access control. Includes system administrators, and system access is granted on a need-to-know basis in compliance with the Privacy Act of 1974 and SBA security policies.

2) **How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**
Access to the data is determined by the individual's role and responsibility. Access is limited 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 information system have been published.



Controlled Unclassified Information

3) **Will users have access to all data on the system, or will the users' access be restricted? Explain.**
Role-based Access Controls are restricted based on the level of system responsibility assigned to specific users by their managers and approved by the SVOGS Information System Security Officer, the Contracting Officer (in case the user is not an employee), and/or the System Owner. System end-users are Grantees and members of the public. Their access is limited to only the SVOG public-facing portal, and they can only access their data, records, and grant status. This is ensured by the enforcement of Multi-Factor Authentication (MFA).

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials.**)
Access is limited by control of User IDs, password controls, and the assignment of a Responsibility profile to all User IDs, effectively limiting the data objects and fields they can access. In addition to this, record-level security is enabled using access control settings, role hierarchies, and defined user roles that limit access to sensitive information to only those with a need to know. Everyone must take Cyber Security Awareness training with the Privacy module.

5) **Are contractors involved with the design and development of the system, and will they be involved with the maintenance of the system**? **If yes, were Security and Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?**
Yes. Security and Privacy Act clauses are in each respective contract for the contractors that are involved in the design, development, and maintenance of the SVOGS information system.
FAR 52.224-1 Privacy Act Notification (Apr 1984)
FAR 52.224-2 Privacy Act (Apr 1984)
Yes. The contractors, as outlined in FAR 52.224-1 Privacy Act Notification (Apr 1984) and FAR 52.224-2 Privacy Act (Apr 1984), must comply with these regulations in all aspects of support and development. Contractors are also required to ensure that the system, data, and all access comply with the Federal Risk and Authorization Management Program (FedRAMP), the National Institute of Standards and Technology (NIST), and the Federal Information Security Management Act (FISMA) requirements.

6) **Do other systems share data or have access to the data in the system? If yes, explain.**
The SVOG system shares data with third-party validation sources such as Treasury DNP and IRS (4506T) through one-time automation data requests/downloads and manual efforts. The system currently does not exchange data with ETRAN. JAAMS transactions are recorded manually. To comply with Data Retention policies, SVOG Data is exported to an SBA-controlled data warehouse (AWS), and security is used to limit visibility in reporting capabilities. SVOG publicly reports using two different methods. The first is to publish approved grants using the SVOG data | U.S. Small Business Administration site. The second method is by submitting updates to the Treasury Do Not Pay (DNP) system, which is performed through a secure DNP website. Through the Salesforce system, data is collected, and reports are generated for internal staff and management, and where appropriate and upon approved request, for other governmental agencies, but no user information is provided. The reports are for a broad overview of the program. SVOG will respond to FOIA, Litigation, and OIG requests. There is no direct access to this data by the requestors. All reports/records are manually collected and provided via a secure link. SVOG continues to work with approved third-party systems to streamline our data-sharing process.

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**



Controlled Unclassified Information

System Owner, Information System Security Officer, system administrators, and Senior Agency Official for Privacy (SAOP)

8) **Will other agencies share data or have access to the data in this system via transferred or transmitted (Federal, State, and Local Other (e.g., Tribal))?**
Data is shared with Department of Treasury – Fiscal Service for the purpose of mitigating fraud via Do Not Pay Program.

9) **How will the shared data be used by the other agency?**
Data is shared with the Treasury DNP and IRS through a transmission process, but there is no direct connection to the SVOG data itself.

10) **What procedures are in place for ensuring proper use of the shared data?**
IRS uses shared data for tax compliance audits, and law enforcement agencies may access data for fraud investigations.
The agency MOU between SBA and treasury provides guidelines on how the data is to be used, and then we talk about shared data for tax compliance and Treasury DNP uses for the agency and program. We did find that MOU did include SVOG data to the Treasury and EMP.
Treasury DNP is authorized and governed by the Payment Integrity Information Act of 2019 (PIIA) and Office of Management and Budget (OMB) memoranda and circulars.

11) **Privacy Impact Analysis: Discuss what privacy risks were identified and how they were mitigated for information shared internally and externally.**

Office of Management and Budget (OMB) Memorandum 17-12 (M-17-12) identifies risks of disclosure of individuals' privacy data in five major areas. The table below identifies those risk areas and the mitigating strategies for each.

| Potential Risk | Mitigating Strategies |
|---|---|
| Sensitivity of Data Elements | The sensitivity of data elements is mitigated using access control, auditing, monitoring, authentication, encryption, and boundary protection. |
| Context of the Data | Context of data elements is mitigated using access control, auditing, monitoring, authentication, encryption, and boundary protection. |
| Revelation of Private Information | Revelation would have a significant negative impact and is mitigated through the use of access control, auditing, monitoring, authentication, and boundary protection. |
| Impact on Vulnerable Populations | Disclosure of data would adversely affect individuals, but this would not be focused on any vulnerable population. |
| Relevance of the Data Over Time | Data are kept current and remain relevant over time. Mitigation includes access control, auditing, monitoring, authentication, encryption, and boundary protection. |



Controlled Unclassified Information