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

Office of Capital Access

Restaurant Revitalization Fund (RRF) Platform

Privacy Impact Assessment

March 15, 2024

Document Information

Template Owner Details	
Name	[redacted]
Contact Number	[redacted]
E-mail Address	[redacted]

Privacy Impact Assessment (PIA) Approval Page

The following individuals have approved this document:

1) **System Owner**

SHERYL MCCONVILLE Digitally signed by SHERYL MCCONVILLE Date: 2024.04.22 14:38:28 -04'00'

_____(Signature) _____(Date)

Name: Sheri McConville
Title: Deputy Director
Office of Capital Access

2) **Senior Agency Official for Privacy. Please note the Alt SAOP may sign on SAOP's behalf.**

KELVIN MOORE Digitally signed by KELVIN MOORE Date: 2024.04.25 08:12:00 -04'00'

_____ (Signature) _____(Date)

Name: Stephen Kucharski
Title: Chief Information Officer (Acting) and
Senior Agency Official for Privacy
Office of the Chief Information Officer

A. CONTACT INFORMATION

1) **Who is the person completing this document?** Nirish Namilae
Technical Lead / ISSO
Office of Capital Access
Nirish.Namilae@sba.gov

2) **Who is the Information System Security Manager?**
Maurice Turner, Chief Security Policy and Compliance Branch
Office of the Chief Information Officer
Maurice.Turner@sba.gov

Who is the Senior Advisor who reviewed this document?

Stephen Kucharski, Senior Agency Official for Privacy (SAOP)
Office of the Chief Information Officer
Stephen.Kucharski@sba.gov

3) **Who is the Privacy Reviewing Official on behalf of SAOP?**

LaWanda Burnette
Chief Privacy /Officer
Office of the Chief Information Officer
LaWanda.Burnette@sba.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION

The US Small Business Administration (SBA) requires the infrastructure and services to enable a scalable grant application workflow and process to support 250k+ United States restaurants which potentially will be applying for funding.

The RRF system enables users to apply for grants to the SBA through an Application Programming Interface (API) and by an automated upload portal designed to provide robust automation, routing and review capability with specific financial services domain level features allowing the organization to route loan origination approvals, grant applications, forgiveness processing, or other related booking and reviewing processing.
The technology has native support for ACH processing, schedule creation, Profile and User Management, API access, and can scale to support up to 25,000 concurrent users and millions of RRF grant applications with supporting documentation.

This platform has the key components required to support the SBA's Restaurant Revitalization Fund program in Support of the American Rescue Plan Act. The platform is provided in a Cloud-Hosted environment, using a highly elastic AWS native and secure framework in FEDRAMP certified AWS GOV Cloud

1) **Does this system contain any information about individuals? If yes, explain**. (Please list the PII variables and suggest validating via database schema if uncertain of what's being captured).

Yes, this system contains grant application information as collected from individual applicants by the RRF application interface. The information collected about individuals can include the borrower's social security number/Employer Identification Number (EIN), banking information, name, and address as well as other data elements required for a RRF grants.

a. **Is the information about individual members of the public?**

   Yes, information is collected on members of the public that apply for SBA RRF grants.

b. **Is the information about employees? (**If specific categories of employees please indicate)

   Employee information is NOT requested unless it is the applicant themselves.

2) **What is the purpose of the system/application?**

The U.S. Small Business Administration (SBA) awarded funding through the Restaurant Revitalization Program to restaurants, bars, and other similar places of business that serve food or drink. Since the program has grant program ended, the current purpose of this program is to provide support audits and post award litigation of grants to eligible entities that suffered revenue losses related to the COVID-19 pandemic.

On March 11, 2021, the American Rescue Plan Act (ARPA) became public law (P.L. 117-2). Section 5003 established the Restaurant Revitalization Fund (Fund), and appropriated $28.6 billion for SBA to award funds.

Given the intent of the American Rescue Plan Act (ARPA) to provide expeditious relief to the restaurant industry during these urgent circumstances, through broad accessibility to grants. RRFP automates application intake, verification, and approval services as required by the ARPA.

3) **Is the system in the development process?**

No, system is in production.

4) **How will the technology investment (new or updated) affect existing privacy processes?**

The investment doesn't impact existing privacy processes.

5) **What legal authority authorizes the purchase or development of this system/application? (**Statute, Executive Orders, etc.)

Public Law 85-536, 15 U.S.C 631 et seq. (Small Business Act, all provisions relating to loan programs, Public Law 85-699 as amended 15 U.S.C. 661 et seq (Small Business Investment Act of 1958, all provisions relating to loan programs), and American Rescue Plan Act (ARPA) public law (P.L. 117-2). Section 5003.

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	Sensitivity of data elements is mitigated using access control, encryption at rest and in-transit, auditing, and monitoring controls.
Context of the Data	RRFP collects data about principals including bank ACH information on grant applications.
Revelation of Private Information	The maximum extent to which private information could be disclosed is the last four digits of the SSN or address, which is mitigated through access enforcement, encryption at rest and in-transit, auditing, and monitoring controls.
Impact on Vulnerable Populations	RRPF doesn't collect vulnerable population data. No impact to vulnerable populations.
Relevance of the Data Over Time	All collected data will remain relevant and disposed of following the Agency retention policy

C. SYSTEM DATA

1) What categories of individuals are covered in the system?

Borrowers and principals of RRF grants are tracked in this system.

2) What are the sources of the information in the system? (Including an informational data flow would be a great opportunity here).

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.)

For the current scope of the application, no additional data is collected from the individuals or a third party.

b. What Federal agencies are providing data for use in the system?
Other Federal agencies, IRS, Treasury, may provide data for validation and/or authentication of applicant provided information. No data is collected from any other Federal Agency.

c. What Tribal, State and local agencies are providing data for use in the system?

Tribal, State, and local agencies do not provide data for RRFP.

d. From what other third-party sources will data be collected?

No new data from third-party sources is being collected for the current purposes of the application.

e. What information will be collected from the employee and the public?

No new data from public is being collected for the current purposes of the application.

3) Accuracy, Timeliness, and Reliability

a. How is data collected from sources other than SBA records verified for accuracy?

Not applicable since no new data is being collected.

b. How is data checked for completeness?

Not applicable since no new data is being collected.

c. Is the data current?

Yes.

d. Are the data elements described in detail and documented?

Yes. They are described in the data dictionary

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	Sensitivity of data elements is mitigated using access control, encryption at rest and in-transit, auditing, and monitoring controls.
Context of the Data	RRFP collects data about principals including bank ACH information on grant applications.
Revelation of Private Information	The maximum extent to which private information could be disclosed is the SSN or address, which is mitigated through access enforcement, encryption at rest and in-transit, auditing, and monitoring controls.
Impact on Vulnerable Populations	RRPF doesn't collect vulnerable population data.
Relevance of the Data Over Time	All collected data will remain relevant and disposed of following the Agency retention policy

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 used to manage the RRF grant process as defined in the American Rescue Plan Act (ARPA) public law (P.L. 117-2). Section 5003.

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, the system will not derive new data nor will it create previously unavailable data.

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?**

   N/A

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?**

   N/A

7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? If process is not be 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.**

   Data can be retrieved by the loan/grant number and/or social security number/EIN

9) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

   Reports can be produced on the records of individuals to respond to inquiries which comply with FOIA and Privacy Act requirements. Access is restricted to Program Officials with the "need to know" and to public inquiries where the specific data complies with FOIA and Privacy Act guidelines.

Controlled Unclassified Information

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 individuals can grant consent.

Not applicable since no new data is being collected from individuals.

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

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	Sensitivity of data elements is mitigated using access control, encryption at rest and in-transit, auditing, and monitoring controls.
Context of the Data	RRFP collects data about principals including bank ACH information on grant applications.
Revelation of Private Information	The maximum extent to which private information could be disclosed is the SSN or address, which is mitigated through access enforcement, encryption at rest and in-transit, auditing, and monitoring controls.
Impact on Vulnerable Populations	RRPF doesn't collect vulnerable population data.
Relevance of the Data Over Time	SSNs are considered relevant during a person's lifetime. EINs are considered relevant during a business' lifetime.

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?

RRFP is hosted on a government cloud solution that follows General Schedule and SBA retention policy. The cloud provider maintains a backup system and operates in a geo-diverse setup specific to SBA policies.

2) What are the retention periods of data in this system?

Records are maintained in accordance with latest edition SBA Standard Operating Procedure (SOP) series 00 41, schedules Records Management Records and Agency Accountability Records.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

Records maintained as part of the General Records Schedules (GRS) are disposed of in accordance with applicable SBA policies.

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.

N/A

7) What kinds of information are collected as a function of the monitoring of individuals?

N/A

8) **What controls will be used to prevent unauthorized monitoring?**

Risks to unauthorized monitoring of privacy data were identified and broken into three major categories, with associated mitigating strategies identified in the table below.

Potential Risk	**Mitigating Strategy**
Loss of data confidentiality	Access control
Loss of data integrity	Incremental and full backups
Loss of data availability	Contingency Planning

9) Under which Privacy Act systems of records notice (SORN) does the system operate? Provide number and name.

The SORN are SBA 20 and 21

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

N/A

F. DATA ACCESS

1) Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, tribes, other)

RRFP data is accessed by SBA personnel that support RRF grant application process. Data can be accessed by contractors, system administrators, and developers who support the system.

SBA's Restaurant Partners or SBA's Point-of-Sale (POS) Restaurant Partners can access the applications originated by them via APIs. Applicants can access their application data.

2) **How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**

Access to data is determined by Agency Security Roles and Procedures/Controls. Access is limited by control assignment of a responsibility profile to all users. 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. The servicing centers have documented procedures and controls to ensure that employees have access to perform assigned duties.

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**

Access is limited by controlled assignment of a responsibility profile to all users. 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.

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**)

SBA has implemented security roles and procedures to prevent misuse of information. Access is limited by control assignment of a responsibility profile to all users. 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. System audit trails can be used to document suspicious or irregular log-ons and navigation of the system. Agency network log-on procedures mandate a posted Warning Banner be viewed and acknowledged prior to entry. SBA Privacy Act of System Records
SBA 20 and SBA 21 define routine uses of this information and serve as control by defining acceptable uses. Access to information is limited to only those with a need to know the information.

Mandatory information security and privacy training is required by all employees to include contractors in accordance with agency policy. This training also includes Rules of Behavior for employees and contractors working on behalf of SBA.

Each contractor must sign a non-disclosure agreement. In addition, the contract clauses are inserted in their contracts to address regulatory measures relating to security.

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 Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?**

Yes. Privacy Act clauses are in the contract.

6) **Do other systems share data or have access to the data in the system? If yes, explain.**

Other systems do not have ingress access to RRFP data.

Controlled Unclassified Information

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

Information collected by this agency will be protected by the agency's IT Security Infrastructure, the Chief Information Security Officer (CISO) and the Senior Agency Official for Privacy

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))?**

For the current purposes of the application no data is shared or transmitted to other agencies.

9) **How will the shared data be used by the other agency?**

NA

10) **What procedures are in place for assuring proper use of the shared data?**

NA

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

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	Sensitivity of data elements is mitigated using access control, encryption at rest and in-transit, auditing, and monitoring controls.
Context of the Data	RRFP collects data about principals including bank ACH information on grant applications.
Revelation of Private Information	The maximum extent to which private information could be disclosed is the SSN or address, which is mitigated through access enforcement, encryption at rest and in-transit, auditing, and monitoring controls.
Impact on Vulnerable Populations	RRPF doesn't collect vulnerable population data.
Relevance of the Data Over Time	SSNs are considered relevant during a person's lifetime. EINs are considered relevant during a business' lifetime.

Controlled Unclassified Information