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

Office of Hearings and Appeals
FOIAXpress
Privacy Impact Assessment

Date: September 2022

System Owner:
Oreoluwa Fashola
Branch Chief, Freedom of Information and Privacy Ac
Office of Hearings and Appeals
OreoluwaFashola@sba.gov

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

Approver:
Stephen Kucharski Acting Chief Information Officer and
Senior Agency Official for Privacy (SOAP)
Office of the Chief Information Officer
Stephen.Kucharski@sba.gov

I. System Description/General Information

The Freedom of Information Act (FOIA), 5 U.S.C. § 552 and Privacy Act of 1974, 5 U.S.C. § 552a, as amended authorizes SBA to provide means for the public to submit requests and obtain records of its activities, to ensure openness and transparency in all government agencies. A request where an individual or organization is seeking only records about him/herself are generally considered a Privacy Act request, while an individual or organization is seeking information about other individuals or SBA business operations is generally considered a FOIA request. SBA uses the same process for submitting both Privacy Act requests and FOIA requests. FOIAXpress will be the primary internal tool used by SBA to help facilitate the release of information to the public via FOIA and Privacy Act requests. FOIAXpress is a third-party vendor-created tracking and management software that will support SBA in administering the entire lifecycle of FOIA and Privacy Act requests. FOIAXpress is cloud base and FEDRamp approved.

Office of Hearing and Appeals (OHA) is publishing this Privacy Impact Assessment (PIA) to assess the uses of FOIAXpress and to document a new Public Access Link (PAL) add-on between it and the Federal service, Login.gov, which is owned and operated by the General Services Administration (GSA). The FOIAXpress Public Access Link (PAL) is a secure public-facing web portal that leverages Login.gov to provide the public with a single access point for requestors to create individual accounts, submit requests, access requested records and communicate with SBA about the status of a request. SBA is leveraging this new connection to implement the Office of Management and Budget (OMB) Memorandum (M)-21-04, Modernizing Access to and Consent of Disclosure of Records Subject to the Privacy Act (Nov. 12, 2020),which instructs federal agencies to "accept remote identity-proofing and authentication for the purpose of allowing an individual to request access to their records or to provide prior written consent authorizing disclosure of their records under the Privacy Act." With this connection, SBA can leverage the remote identity verification services conducted by Login.gov. Login.gov provides the same function to other Federal agencies who choose to utilize it, helping consolidate the identity verification process across Federal services and platforms.

II. System Data

SBA will utilize FOIAXpress to receive and process FOIA/Privacy Act requests, communicate with requestors about their request, provide status updates for requests, keep track of payment information for requests that are charged a fee, provide access to requests (if the file is too large for email), close and archive requests. FOIAXpress will also be integrated with Pay.gov, which is a web-based platform maintained by the U.S. Department of the Treasury, Bureau of the Fiscal Service, this done as way for requesters to pay fees associated with processing their request. Additionally, FOIA requests that are received via facsimile, postal mail, or email, will be entered manually by OHA Freedom of Information/Privacy Act staff. SBA staff will also use FOIAXpress to summarize and gather similar/frequent requests, for future distribution to the public. As part of receiving and processing requests, the personally identifiable information (PII) of requestors and the SBA processing the request is maintained in it as well. The system contains contact information about individuals of the public which could be perceived as PII. SBA

employee may also submit a FOIA/Privacy Act requests outside of duty hours and via personal email address, facsimile, or physical mail which is processed from a public request perspective. Collections of PII such as name, mailing address, email address and telephone numbers which data elements are described in detail and documented via database schema. No sensitive PII, such as social security numbers will be collected. However, responsive records may consist of additional information based on the individual's request which may consist of loan documents, in which these documents are captured in another Privacy Impact Assessment based upon their original source system.

SBA FOIAXpress is in production and there's no major technology investments at this time to affect existing privacy processes. SBA FOIAXpress is covered by the system of records, SBA 14, "Freedom of Information and Privacy Act Records."

SBA categories or individuals categorized that are covered under FOIAXpress consists of SBA Staff, designated FOIA point of contacts in the field, headquarters, program office, district offices, loan centers, and FOIA/PA requestors – individuals. Note: Organizations/media are perceived as individuals per statute.

Source of the information in the system is taken from the requesting individuals or their representative or data entered by staff for request received by postal mail, email, or facsimile. Additional collect from third party sources: Pay.gov or PAL. Other than that, no other federal agencies, tribal, state, or local agencies are providing data to the system.

Individuals making requests about themselves must use the Department of Justice (DOJ) Certification of Identity form. All other requests are redacted. Requests also go through a quality assurance check for completeness and because of the nature or requests, information may become dated over time.

III. Data Attributes

The use of the data is both relevant and necessary for the purpose of the FOIA/PA application for which the system is designed. The system is indexed and retrieved by name or tracking number. Statistical data is used to produce the annual report submitted to the DOJ. To process requests, the individual must provide voluntary information.

Data will be imported from the previous FOIA case management system, FOIAonline and no new data will be created. The same access control for FOIAXpress will be levied against the imported information. The data collected will be hosted in a FedRAMP moderate facility, and access to the servers is on a need-to-know basis by cleared staff.

IV. Maintenance and Administrative Controls

FOIAXpress will be maintained at a single site location. Records maintained in FOIAXpress are retained and disposed of in accordance with records' retention schedules approved by the National archives and Records Administration (NARA). Records maintained as part of the

General Records Schedules (GRS) are disposed of accordingly to policy.

V. Data Access

SBA FOIAXpress can be accessed by SBA staff, SBA contractors, to include headquarters, field staff, and loan centers that are designated access with the "right to know" and FOIA/Privacy Act requestors submitting a request for SBA records.

User Access is provisioned through a request from a supervisor by email. Access to the data is determined by individual's role and responsibility. Access is limited by control of defined categories for user profiles established for all users. Each profile comes with a predetermined set of capabilities, limiting functionality and data that may be viewed, as necessary to perform duties of the user. Access is limited by control of authenticated users, through their profile, which limits possible activities. Education of SBA staff regarding the Privacy Act rules and prohibitions on the dissemination or use of non-public information is recognized as mandatory and is ongoing. All Agency employees must take the Cyber Security Awareness Training (CSAT) with Privacy module and are required to sign the "Rules of Behavior". System audit trails can be used to document suspicious or irregular logons and navigation of the system. Agency network log-on procedures mandate a posted Privacy notice be viewed and acknowledged prior to entry. SBA Privacy Act System of Records SBA 14 defines routine uses of this information and serves as a control by defining acceptable uses. Limiting access to sensitive information to only those with a need to know is the primary control.

Contractors are involved in the design and development of FOIAXpress. Privacy Act clauses are in the contracts that protect Privacy Act and other sensitive data. Non-Disclosure Agreements are also signed.

The Public Access Link (PAL) is a secure public-facing web portal that leverages Login.gov to provide the public with a single access point for requestors to create individual accounts, submit requests, access requested records and communicate with SBA about the status of a request. Additionally, FOIAXpress secure integration with pay.gov, which allows payment of fees for the processing of requests.

VI. Privacy Impact Analysis

There are risks related to disclosure of individuals' privacy. Risks to the type of data, assurance the information is used as intended, safeguard unauthorized monitoring of privacy data, and protect information shared internal and external. The sensitivity of the FOIAXpress data elements increases the risk for inadvertent disclosure which is susceptible to identity theft. Some data provides significant information which could adversely affect individuals but not specifically to impact vulnerable populations. Privacy risks are mitigated through access control, auditing, secure application design and monitoring, encryption, and authentication. Mitigation also includes 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, and data redundancy. 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. Data remains historically accurate over time. Lastly, mitigation is also through education via annual Cybersecurity Awareness and Privacy Training.