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

Office of Capital Access

Capital Access Financial System
Privacy Impact Assessment
January 22, 2021

System Owner
Ronald Whalen
Director, Systems Operation Division
Office of Capital Access
Ronald.Whalen@sba.gov

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

I. System Description/General Information

The Small Business Administration (SBA) provides access to capital for tens of thousands of small businesses and disaster victims each year. SBA's $905+ billion loan portfolio plays an important role in the small business economy. Capital Access Financial System (CAFS) is an Operations & Maintenance (O&M) investment that supports the SBA's Guaranty Loan Programs (7(a), Payroll Protection/CARES Act, and 504), Surety Bond Guaranty Programs, Direct Loans (EIDL/Disaster/Microloans), and the credit risk management processes.

CAFS supports SBA's guaranty and Disaster loan programs' full loan life cycle, which includes lender/borrower matchmaking, origination, servicing, and post servicing. CAFS also supports the surety guaranty bond program. CAFS includes a front-end thin client, back end batch processes, and web services to integrate with third party vendors.

The SBA provides direct loans and loan guarantees for small businesses, entrepreneurs, and individuals through several capital access programs.

- The 7(a) program provides loan guarantees to help qualified small businesses obtain conventional financing through commercial lending institutions,
- The CARES Act/Payroll Protection Program (PPP) provides loans to businesses impacted by the COVID-19 pandemic.
- The 504 loan program provides long-term, fixed-rate financing for small firms to acquire physical assets through certified development companies,
- The small business investment company program licenses venture capital firms to offer financing to small firms,
- The microloan program provides very small loans to entrepreneurs needing special technical assistance, and
- The disaster loan program assists businesses as well as homeowners in the wake of physical disasters.
- The SBA also provides surety bond guarantees for small businesses.

CAFS is the system of record for the services and products listed above .and posted in the Federal Register and agency webpage under System of Records Notices SBA 20 and SBA 21.

The legal authority which supports this system is 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).

II. System Data

The categories of individuals covered in the system are applicants, principals, and guarantors of SBA loan and guaranty products. Sources of the information

is obtained by SBA partner, lenders, and investors who electronically send the information to SBA.

Information on disaster loan applicants is gathered from Disaster centers. Disaster personnel enter the information into Disaster Credit Management System (DCMS), which sends the information to CAFS. Furthermore, the Surety bond information is gathered from business owners.

Treasury provides updates to the system for payments made on charge off or delinquent loans. Treasury also provides Do Not Pay data to the system. The Do Not Pay data identifies borrowers who may not be eligible for Federal funding.

Housing and Urban Development (HUD) provides information for applicants that are currently in default or foreclosure or have had a claim paid by the reporting agency in the last three years.

Tribal, state, and local agencies are not providing data for use in the system.

SBA collects information from the credit bureaus, Lexis-Nexis, and Dun & Bradstreet on loan applicants. SBA collects information about lenders from Acuity.

Applicants of SBA loan products provide information to SBA on their financial/credit history, social security numbers, name, and address.

All CAFS account holders provide their name, phone number, email address, and work address upon registration.

The sources of data for CAFS include Treasury, HUD, credit bureaus, Lexis Nexis, Dun & Bradstreet, and Acuity. Various mechanisms are used for validation, depending on the source which may include: applicant verification, loan history information, public data sources, DUNS number, lending partners, adverse action list from other federal agencies, etc.

SBA conducts a periodic physical review of the loan folder. During the review, the information in the loan folder is validated against information in CAFS.

When the loan servicing center charges off a loan, the center personnel have a checklist to compare the file data with CAFS.

III. Data Attributes

The use of the data is relevant and necessary for the purpose for which the system is being designed. Only the minimum data necessary to manage SBA's loan and surety products that directly link the Agency's mission.

The data is current and described in detail in the data dictionary. No new data

will be derived or created.

Data can be retrieved by the licensing number, loan number, tax identification number/social security number, and/or loan application number.

A variety of reports can be developed as needed. Reports can be produced on the records of individuals to respond to inquiries which comply with FOIA and Privacy Act requirements. Access is restricted based to those with the "need to know" and to public inquiries where the specific data complies with FOIA and Privacy Act guidelines.

IV. Maintenance and Administrative Controls

CAFS data transactions are designed to adhere to the atomicity, consistency, isolation, and durability principles. Atomicity is adhered to by requiring a transaction is completely saved or not saved at all. In the event that a connection is lost, the database is rolled back to the state prior to the transaction initiation. Consistency is adhered to by enforcing data integrity. If a transaction impacts the integrity, the database validations report an error. In the event of an error, the data may be saved but the transaction is aborted. Isolation is maintained by requiring transactions to occur in a serially which requires that transactions are queued to prevent multiple transactions on a single record. Durability is maintained by having real time back up to ensure that data is maintained in the event of a system failure.

The retention period and disposition of data for CAFS is in accordance with NARA standards and SBA Standard Operating Procedures (SOP) "Records Management Program: SOP 0041, latest rendition. It is also conveyed in system of records notices SBA 20 and SBA 21.

CAFS does not employ any use of technologies to affect public/employee privacy. CAFS tracks financial information for members of the public who apply for SBA loan and bond products. SBA does not sell or share information with 3rd party organizations unless it is required to do so in the originating and/or servicing of the product. The system is not used to identify, locate, or monitor individuals.

V. Data Access

CAFS data is accessed by SBA personnel that support the loan and bond processes. Data can be accessed by contractors, system administrators, and developers who support the system. Also, Lenders and investors can access their loan data. Authorized agency users have access to the system based on their specific roles or responsibility.

Access to data is determined by user type as well as assigned roles. 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 CAFS to perform assigned duties. 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.

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 Privacy access and monitor notice be viewed and acknowledged prior to system 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.

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.

CAFS shares data with other systems securely and in compliance with policy. The systems include the Denver Finance Center System (DFCS), Disaster Credit Management System (DCMS), Financial Transfer Agent (FTA), Central Servicing Agent (CSA), Mainframe, United States Treasury Department, Housing and Urban Development (HUD), Credit Alert Interactive Voice Response System (CAIVRS), and Credit Bureaus for various reasons to include computer matching.

SBA has a Computer Matching Agreement with HUD and Treasury that is reviewed annually. Treasury and HUD are provided a copy of problem loans. Treasury uses the information to place borrowers on the Do Not Pay list. HUD

adds the information to their multi-agency database of persons that have problem with government loans.

VI. Privacy Impact Analysis

There is a risk related to data type in which the sensitivity of the CAFS data elements increases the risk for inadvertent disclosure which is susceptible to identity theft. There is also risk ensuring that the information is used as intended and the type of information collected. Some data provides significant information about individuals has context with regard to individual's finances and business tax purposes. Revelation of CAFS data could have a significant revelation impact to employees and external entities. Disclosure of CAFS data would not significantly lose relevance over time. Disclosure of CAFS data would not adversely affect any particular vulnerable population.

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.