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

Office of Capital Access

Direct Loan Closing Platform Privacy Impact Assessment November 10, 2021

System Owner
Sheri McConville
Deputy Director, OPSM
Office of Capital Access
Sheri.McConville@sba.gov

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

This is a Controlled Unclassified Document

I. System Description/General Information

The Small Business Administration (SBA) requires the infrastructure and services to enable a application workflow and process to support Loan Closing process for the Coronavirus 19 Economic Injury Disaster Loan (COVID EIDL). The Summit Technology Group (STG) core application, Direct Loan Closing Platform (DLCP), is a Software as a Service (SaaS) solution. It is a multiuser, transaction-based application suite that enables the document management and processing of complex financial transaction. This platform has the key components required to support the solution. The platform is provided in a Cloud-Hosted environment, using a highly elastic Amazon Web Services (AWS) native and secure framework in the Federal Risk and Authorization Management Program (FEDRAMP) certified AWS Gov Cloud.

The provider web interface is a multiuser, web-based application. It is designed to support up to streamline loan closing process so that funds reach millions of eligible COVID EIDL loan applicants in a timely manner. The system enables Processing and Disbursement Center (PDC) attorneys to initiate closing process by uploading the completed closing package. Third-party Closers upload the executed closing documents to the system. System uses an Application Programming Interface (API) interface to confirm the filings of the closing documents in appropriate jurisdiction. Funds are then disbursed to borrowers using the API interface with SBA Capital Access Financial System. The user community reviewing the closing process could be a third-party Closer/Scheduler, PDC attorneys, paralegal staff or the Office of Capital Access (OCA) government user audience. Access to the platform and related APIs will only be provided after a full sandbox validation and production promotion process and validating all security access requirements.

The application also provides reporting interfaces as additional service offerings. These interfaces allow PDC and OCA government user to monitor basic statistics of their business and resolve simple questions and exceptions.

DLCP purpose is to provide Loan Closing support to eligible entities that have applied for COVID EIDL loan and in turn expedite the loan disbursements. The new module is added to an existing platform that was already in production.

DLCP is covered under System of Records Notices SBA 20 and SBA 21 which are posted in the Federal Register and on the agency’s webpage.

The legal authorities which supports this system are Privacy Act of 1974, as amended, 5 U.S.C. Sec. 552a, 5 U.S.C. 552a(b), 15 U.S.C. 634(b)(6), 44 U.S.C. 3101, Debt Collection Act of 1982, Authority of 44 U.S.C. 2904 and 2906, Federal Information Security Modernization Act of 2014 (FISMA), Intelligence, counterintelligence activities as defined by 50 U.S.C. 3003(3), 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), The Economic Aid to Hard-Hit Small Businesses, Nonprofits and Venues Act, P.L. 116-260 , Public Law 116-123, 134 Stat. 146, 147 (Coronavirus Preparedness and Response Supplemental Act), Public Law 116-136 (CARES Act), Public Law 116-260 (Economic Aid Act) and Public law 117-2 (American Rescue Plan Act (ARPA)).

II. System Data

This system contains loan application information that is collected by vendors and individual applicant. The information collected about individuals can include the borrower's social security number/Employer Identification Number (EIN), banking information, name, race, ethnicity, gender and address. The data elements are described in detail and documented in our project documentation and information workflow diagrams.
The categories of individuals covered in the system are borrowers and principals of COVID EIDL are tracked in this system. Information is not collected directly from the borrower but is based on the COVID EIDL loan application. PDC attorneys use the information to create closing package in DLCP. Third party Closers upload executed closing documents and update closing related fee values. PDC attorneys review the final package and make any corrections needed to fix validation checks before loan is marked for disbursement. No other federal agency data is used in the system as input. Tribal, State and local agencies do not provide data for DLCP.

Data in the system is current and checked for completeness. PDC conducts automatic and manual reviews on the document package received by DLCP. DLCP will rely on SBA Attorneys/paralegal staff and PDC personnel for reviewing the data during the Loan Closing verification process to ensure the data is complete.

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 is collected to manage the COVID EIDL loan closing process.

The system will not create or derive new data. The existing data can be retrieved by the loan/grant number and/or social security number/EIN.

A variety of reports are produced from system dashboards to monitor the process of the program. No current routine reports at the individual level are being produced. 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.

Any individual wanting to decline providing information would do so with the source system and declination would have an impact on the loan process.

IV. Maintenance and Administrative Controls

DLCP is hosted on a government cloud solution where the cloud provider maintains a backup system and operates in a geo-diverse setup in accordance to National Institute of Standards and Technology.

The retention period and disposition of data for DLCP 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.

DLCP does not employ any use of technologies to affect public/employee privacy. The system is not used to identify, locate, or monitor individuals.

V. Data Access

DLCP data is accessed by SBA personnel and third-party Closer/Schedulers hat support the closing process., Data can be accessed by SBA contractors who support operation the system.

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.

Access is controlled by assignment of a responsibility profile to all users. Third-party Closer are only allowed to only view loan related information. They are allowed to upload the executed closing packages and add various fees collected as part of the closing process. PDC attorneys and staff are allowed to review loan data and perform updates on loan financial data to bring the record into compliance

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.

DLCP 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. Third-party Closer are only allowed to only view and update closing fee information for loans assigned to them. Access to data is only by inputting the identifying loan number of tax id. PDC attorneys reviewing the closing documents can update loan financial fields. 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 notice 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 privacy and security.

Third-party Closers can upload executed closing documents to the DLCP system. These users can review loan related information but only input closing fee related details in addition to the closing documents.
DLCP data is not shared with other agencies.

VI. Privacy Impact Analysis

There is a risk related to data type in which the sensitivity of the DLCP 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. Revelation of DLCP data could have a significant revelation impact to employees during a person's lifetime. Disclosure of DLCP data would not adversely affect any particular vulnerable population.

Privacy risks are mitigated through access control, auditing, secure application design and monitoring, encryption at rest and in transit, and authentication. Mitigation also includes limiting content and ensuring collection is comparable to its' collection from the source system; ensuring collection follows statutory authority to collect, incremental and full backups, data integrity checks and monitoring controls. Lastly, mitigation is also through education via annual Cybersecurity Awareness and Privacy Training.