Small Business Administration

Small Business Administration

Information Systems Security Program

Capital Access Financial System (CAFS)
<Enter Vendor/Lender/Program Office Name Here> (Vendor/Lender/Program Office)
Interconnection Security Agreement (ISA)

Month/Day/Year

SBA

409 3rd ST, SW
Washington, DC 20024

Document Information

Template Revision History			
Version	**Date**	**Author**	**Changes / Comments**
1.0	05-07-2020	Timalyn Franklin	ISA
2.0	05-15-2021	Timalyn Franklin	Annual Update
3.0	06-25-2021	Nirish Namilae	Added financial instruments
4.0	09-08-2021	Timalyn Franklin	Added the Federal government language and added the APIs.
5.0	04-17-2024	Timalyn Franklin	Updated with test requirements.
6.0	08-01-2024	Timalyn Franklin	Update to include AES 256 requirement.
7.0	12-06-2024	Timalyn Franklin/Mohannad Yousef	Added Settlement Express API

Table of Contents

1 DISCLAIMER

All vendors must agree to the terms below and make sure that their clients understand the requirements for accessing a Federal system.

This is a U.S. Small Business Administration federal government computer system that is for official use only. This system is subject to monitoring and anyone using this system expressly consents to such monitoring. Individuals found performing unauthorized activities may be subject to disciplinary action including criminal prosecution.

2 VENDOR/LENDER/PROGRAM OFFICE CONTACT INFORMATION

Each vendor/lender/program office must provide two contacts in the table below.

Name	System Name	Business Address	URL	Contact Name	Contact Job Title	Contact Email Address	Contact Phone Number

3 TYPES OF LOAN & APIS

a. Is this a renewal for an existing ISA or a new ISA?
___New ___Renewal

b. Please identify the loans that you will service and originate.

__7a (select 7a for PPP) __504 __Microloans __Community Advantage

c. Please identify the APIs that you are requesting to use.

API	State Yes if you want to use the API
Origination	
Servicing	
1502	
Loan List	
Settlement Express	

4 ONBOARDING PROCESS (IF YOU ALREADY HAVE AN ISA, YOU CAN BYBPASS THIS STEP)

SBA only allows two test accounts per vendor/lender/program office. The two accounts must include point of contacts defined in section 2. The process to request access to test is listed below and based on the type of loans that you support.

4.1 7a Process

1. The vendor or lender can send an email to CAFSTEST@sba.gov with the following:
    a. Name, email address, and phone number of the lead in the loan division who will use the web service
    b. Name, email address, and phone number of the security officer who will be responsible for ensuring compliance with the security controls in the vendor/lender/program office system.
2. The lender/vendor will be sent the ISA vendor/lender/program office template for completion.
3. After the lender/vendor returns the signed ISA, the system owner will review and approve or reject the ISA.
4. If the ISA is approved, the vendor/lender/program office will be set up with a location id in PIMS test with the required agreements.
5. The vendor/lender/program office will also receive an authentication code.
6. The vendor/lender/program office will be required to attend and onboarding session before they are given the XSDs.
7. After the onboarding session,
    a. The lender will receive a vendor/lender/program office id to test the APIs.
    b. The lender/vendor will receive instructions to create a partner account in test.
8. The vendor/lender/program office will be required to test the following three scenarios:
    a. Originating a sole prop loan with an SSN
    b. Originating a sole prop loan with an EIN

   c. Canceling a loan using servicing.
   d. Send 1502 report on a loan.
   e. Request sold loan status via 1502.
9. The lender will send the loan numbers of the three scenarios to CAFSTEST@sba.gov.
10. After review, the lender will be moved to production.
11. In production, the lender will send the lender location and NOT the location id provided for test. The lender will also send an authentication code.

4.2 504 Process

1. The vendor or lender can send an email to CAFSTEST@sba.gov with the following:
   a. Name, email address, and phone number of the lead in the loan division who will use the web service
   b. Name, email address, and phone number of the security officer who will be responsible for ensuring compliance with the security controls in the vendor/lender/program office system.
2. The lender/vendor will be sent the ISA vendor/lender/program office template for completion.
3. After the lender/vendor/program office returns the signed ISA, the system owner will review and approve or reject the ISA.
4. If the ISA is approved, the vendor/lender/program office will be set up with a location id in PIMS test with the required agreements.
5. The vendor/lender/program office will also receive an authentication code.
6. The vendor/lender/program office will be required to attend and onboarding session before they are given the XSDs.
7. After the onboarding session,
   a. The vendor/lender/program, office will receive a vendor/lender/program office id to test the APIs.
   b. The lender/vendor/program office will receive instructions to create a partner account in test.
8. The vendor/lender/program office will be required to test the following three scenarios:
   a. Originating a sole prop loan with an SSN
   b. Originating a sole prop loan with an EIN
   c. Canceling a loan using servicing.
9. The lender will send the loan numbers of the three scenarios to CAFSTEST@sba.gov.
10. After review, the lender will be moved to production.
11. In production, the lender will send the lender location and NOT the location id provided for test. The lender will also send an authentication code.

4.3 Microloans & Community Advantage Process

SBA will onboard vendors with the program office.

4.4 Loan List API Process

1. The vendor or lender can send an email to CAFSTEST@sba.gov with the following:
    a. Name, email address, and phone number of the lead in the loan division who will use the web service
    b. Name, email address, and phone number of the security officer who will be responsible for ensuring compliance with the security controls in the vendor/lender/program office system.
2. The lender/vendor/program office will be sent the ISA vendor/lender/program office template for completion.
3. After the lender/vendor/program office returns the signed ISA, the system owner will review and approve or reject the ISA.
4. If the ISA is approved, the vendor/lender/program office will be set up with a location id in PIMS test with the required agreements.
5. The vendor/lender/program office will also receive an authentication code.
6. The vendor/lender/program office will be required to attend and onboarding session before they are given the XSDs.
7. After the onboarding session,
    a. The lender will receive a vendor/lender/program office id to test the APIs.
    b. The lender/vendor/program office will receive instructions to create a partner account in test.
8. The vendor/lender/program office will be required to show a test successfully calling the web service.
9. The lender will send the loan numbers of the three scenarios to CAFSTEST@sba.gov.
10. After review, the lender will be moved to production.
11. In production, the lender will send the lender location and NOT the location id provided for test. The lender will also send an authentication code.

4.5 Settlement Express API Process

1. The vendor can send an email to CAFSTEST@sba.gov with the following:
    a. Name, email address, and phone number of the lead in the loan division who will use the web service
    b. Name, email address, and phone number of the security officer who will be responsible for ensuring compliance with the security controls in the vendor/lender/program office system.
2. The vendor will be sent the ISA vendor/lender/program office template for completion.
3. After the vendor returns the signed ISA, the system owner will review and approve or reject the ISA.
4. If the ISA is approved, the vendor will be set up with a location id in PIMS test with the required agreements.
5. The vendor will also receive an authentication code.

6. The vendor will be required to attend and onboarding session before they are given the XSDs.
7. After the onboarding session,
    a. The vendor will receive a vendor id to test the APIs.
    b. The vendor will receive instructions to create a partner account in test.
8. The vendor will be required to show a test successfully calling the web service and be required to test the following two scenarios:
    a. Successfully submit the 1086/Note API
    b. Successfully submit the Confirm API
9. The vendor will send the loan numbers of the two scenarios to CAFSTEST@sba.gov.
10. After review, the vendor will be moved to production.
11. In production, the vendor will send the lender location and NOT the location id provided for test. The vendor will also send an authentication code.

5 INTERCONNECTION STATEMENT OF REQUIREMENTS

The requirements for interconnection between SBA OCA and **VENDOR/LENDER/PROGRAM OFFICE** are for the express purpose of exchanging data between CAFS owned by OCA OPSM and **VENDOR/LENDER/PROGRAM OFFICE data** owned by the lender submitting the data. **VENDOR/LENDER/PROGRAM OFFICE** requires the use of OCA's CAFS to originate and service loans for an SBA approved lender. This ISA is for the test environment (catweb2) and production (caweb).

6 SYSTEM SECURITY CONSIDERATIONS

The interconnection between CAFs, owned by SBA OCA and **VENDOR/LENDER/PROGRAM OFFICE** is a two-way communication path via web service. The purpose of the interconnection is for **VENDOR/LENDER/PROGRAM OFFICE** to deliver loan origination and servicing data to CAFS.

Approved vendors/lenders/program office have access to two environments—system test environment and standard operating environment (SOE)/production.

International Software Testing Qualifications Board (**ISTQB**) defines "system testing is a level of software testing where a complete and integrated software is tested. The purpose of this test is to evaluate the system's compliance with the specified requirements."

An SOE is a standard operating environment, or a specific computer operating system and collection of software that an IT department defines as a standard build which collects live data.

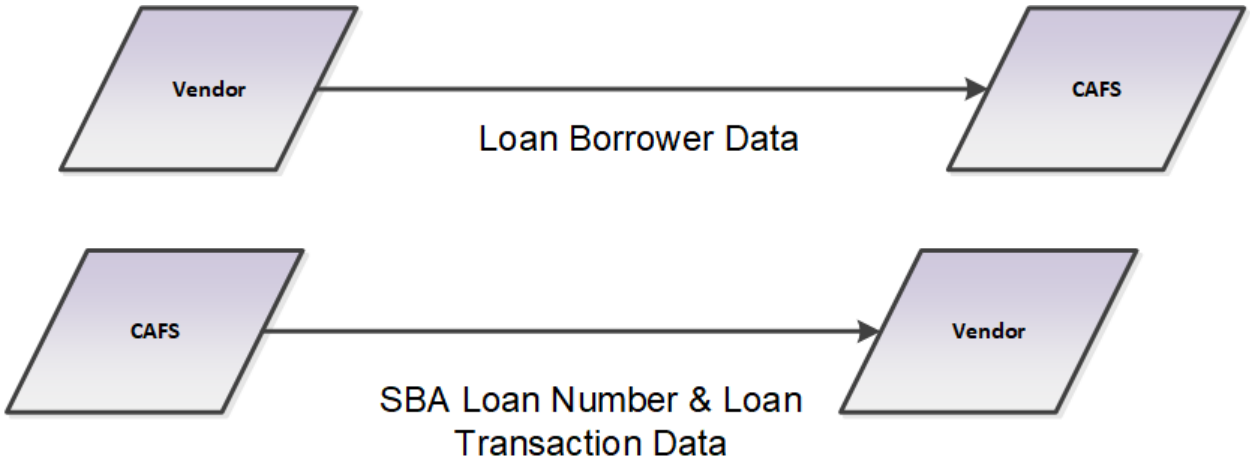
Assumptions:

- **VENDOR/LENDER/PROGRAM OFFICE** will access system test at catweb2.sba.gov and SOE/production at caweb@sba.gov .

- **VENDOR/LENDER/PROGRAM OFFICE** is responsible for annually certifying that they comply with FISMA, Sarbanes Oxley, and NIST.
- **VENDOR/LENDER/PROGRAM OFFICE** is responsible for protecting production data. ***The vendor/lender/program office is solely responsible for data breaches associated with the vendor's/lender's/program office's environment.***
- **VENDOR/LENDER/PROGRAM OFFICE** should never use test as a sandbox to QA or test production loans. **Test data should not be production data.** SBA is not responsible for the lender or vendor entering production data into the test environment. SBA doesn't provide or monitor test data. Test data should be mock data that cannot be used to identify a person.
- **VENDOR/LENDER/PROGRAM OFFICE** will only use the system to call OrigScore for an SBA loan.
- **VENDOR/LENDER/PROGRAM OFFICE** will not use system to system accounts.
- **VENDOR/LENDER/PROGRAM OFFICE** will not use robotic process automation or bulk processing.
- **VENDOR/LENDER/PROGRAM OFFICE understands that the data in test is only segregated by VENDOR/LENDER/PROGRAM OFFICE. Clients will see each other's data.**
- **VENDOR/LENDER/PROGRAM OFFICE** will receive a vendor location id for test.
- **VENDOR/LENDER/PROGRAM OFFICE** must use the lender location id for production.
- **VENDOR/LENDER/PROGRAM OFFICE** is responsible for ensuring that there is always a compliant ISA on file with SBA.
- **VENDOR/LENDER/PROGRAM OFFICE** will not share their id with another vendor.

6.1 System Description

The following diagram illustrates the flow of sources between OCA CAFS and **VENDOR/LENDER**. IP addresses are not included due to security mandates; however, this illustrates the path of data to and from CAFS.



6.2 Data and Security Controls

CAFS and **VENDOR/LENDER/PROGRAM OFFICE** exchange data via a web service. CAFS web services use AES256 encryption method to validate that the data received from a web service is not corrupted. AES 256 has a "signature algorithm" in the certificate which is embedded in the web service response. The "signature" that proves that the response is identical to whatever was sent from the server. The fact that our certificate uses AES 256 tells us that the web service incorporates a very strong validation that the bi-directional data received was not corrupted.

6.3 Services Offered

The connection is for the exchange of data only between the two systems.

6.4 Data Sensitivity

VENDOR/LENDER/PROGRAM OFFICE and CAFS exchange loan borrower data.

For test, the vendor/lender/program office should not provide any data that would be Sensitive-But-Unclassified (SBU.

For SOE/production Privacy Act data traverse this connection. Though the data classification is Sensitive-But-Unclassified (SBU), its sensitivity demands strong measures to provide a high level of confidence that is confidentiality, integrity, and availability are preserved

6.5 User Community

For test, the data is accessed by development team who has the authority to collect, enter, and/or process loan data.

For production/SOE, the data is accessed by the lender approved personnel who have the authority to collect, enter, and/or process loan data.

6.6 Information Exchange Security

The information exchanged between **VENDOR/LENDER/PROGRAM OFFICE** and CAFS requires the lender using the vendor/lender/program office solution has a valid CLS account.

6.7 Trusted Behavior Expectations / Rules of Behavior (ROB)

The lender, vendor/lender, and CAFS users are expected to protect data in accordance with the policies and standards of the Privacy Act, OMB A-130, NIST 800-53 (latest edition), and Sarbanes-Oxley Act of 2002.

6.8 Incident Reporting

Upon discovering an incident involving PII, the vendor and lender personnel must report it to SBA within an hour. The SBA must report the incident to the U.S Computer Emergency Readiness Team within one

hour of notification. The reportable incidents shall not distinguish between suspected and confirmed breaches.

All incidents must be reported to the

- SBA CIRT by emailing soc@sba.gov.
- CAFS System Owner, Ronald D. Whalen, Ronald.Whalen@sba.gov

6.9 Security Parameters

Data is exchanged using the latest secure connection protocol. SBA currently supports TLS 1.2 and 1.3.

6.9.1 Hardware Requirements

There are not any hardware requirements for the web service communication.

6.9.2 Software Requirements

There are not any software requirements for the web service communication.

6.10 Operational Security Mode

The table below lists the Federal Information Processing Standard (FIPS 199) security categorization for the SBA system(s) in Table 2-1.]

Table 6-1: System Sensitivity Levels

Security Objective	Level of Risk		
	High	Medium	Low
Confidentiality		X	
Integrity		X	
Availability		X	

6.11 Audit Trails Responsibilities

SBA OCA and **VENDOR/LENDER/PROGRAM OFFICE** are responsible for auditing application and user activities involving this interconnection. Activities that will be recorded include event type, date, and time of event, interconnecting system identification, success or failure of access attempts, and security actions taken by system administrators and security officers. Audit log records will be retained for one (1) year for production and one week for test.

6.12 Training and Awareness

The information is exchanged via a web service. There is not any training required to access the web service.

6.13 Specific Equipment Restrictions

The information is exchanged via a web service. There are not any equipment restrictions for the web service.

6.14 Connectivity

The web service required internet capability. **VENDOR/LENDER/PROGRAM OFFICE** must have the ability to call the web service via the internet and for CAFS to be accessible via the internet.

6.15 Security Documentation

The Executive and Legislative branches, Federal departments and agencies issue security policies, standards, and laws. This interconnection must comply with the following Federal requirements:

- Federal Information Security Management Act (FISMA) as part of the E-Government Act of 2002
- Office of the Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources
- NIST Special Publications, including NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems MODERATE CONTROLS

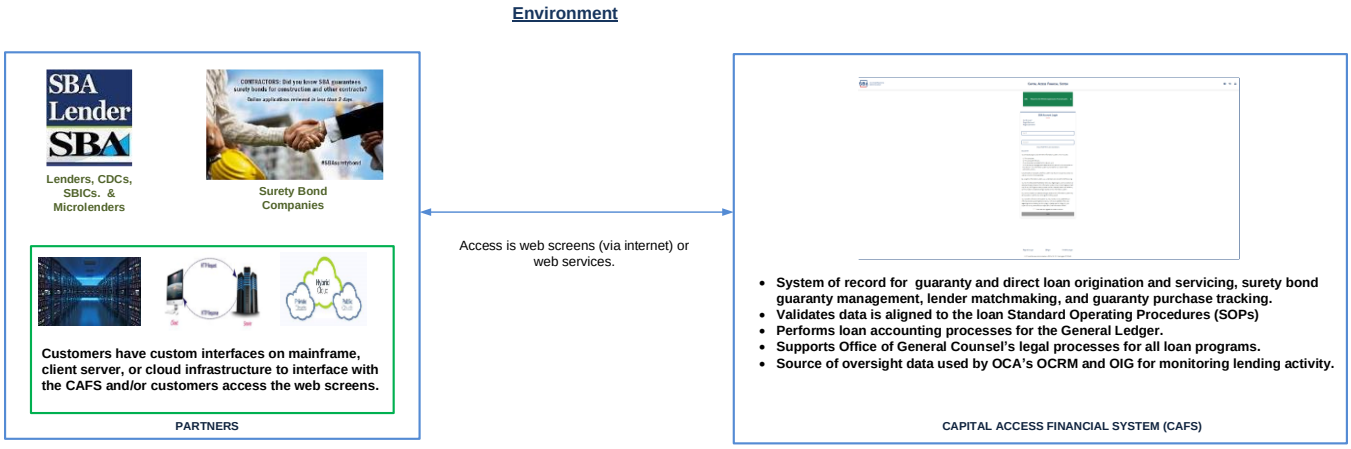
6.16 Escalation Procedure

If there are issues with the web service, the vendor/lender/program office authorizing official should contact cafstest@sba.gov.

Security issues incidents should be sent to CAFS@sba.gov..

7 NETWORK TOPOLOGY DRAWING

The network topology is in the diagram below.



8 SIGNATORY AUTHORITY

This ISA is valid for three years after the latest date on either signature below if the technology documented herein does not change or if there are no other intervening requirements for update. The security controls for this interconnection will be reviewed every three years, or whenever a significant change occurs.

VENDOR/LENDER/PROGRAM OFFICE Authorizing Official

_____

TBD

_____

TBD

_____

(Signature) (Date)