Small Business Administration

Small Business Administration
Information Systems Security Program

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

06/28/2020

U.S. Small Business Administration
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
1.1	06-25-2021	Nirish Namilae	Added additional financial instruments

Table of Contents

1 VENDOR CONTACT INFORMATION

Each vendor 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

2 TYPES OF FINANCIAL INSTRUMENTS

Please identify the financial instrument that you will service and originate.

__7a __504 __Microloans __CA__Bonds _X_ Grants __Disaster

3 PROCESS

The process for software vendors using CAFS APIs to request access to test is listed below.

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 lender/vendor system.
2. The lender/vendor will be sent the ISA vendor 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 will be set up with a location id in PIMS test with the required agreements. The vendor will also receive the Integration Guide.
5. The lender/vendor will also receive an authentication code.

6. The lender/vendor will be required to attend and onboarding session before they are given the XSDs.
7. After the onboarding session,
    a. The lender/vendor will receive a vendor id to test the APIs.
    b. The lender/vendor will receive instructions to create a partner account in test.
8. The lender/vendor will be required to test the following one or more scenarios as applicable:
    a. For Loan Origination, originate a sole prop loan with an SSN
    b. For Loan Origination, originate a sole prop loan with an EIN
    c. For Loan Servicing, cancel a loan using servicing.
    d. For 1502 reporting, submit sample 1502 reporting data
    e. For 1502 data retrieval, request sold loan status, rate information
9. The lender/vendor will send the loan numbers of the scenarios to CAFSTEST mailbox.
10. After review, the lender/vendor will be moved to production.
11. In production, the lender/vendor will send the lender location and NOT the location id provided for test. The lender/vendor will also send an authentication code.

4 INTERCONNECTION STATEMENT OF REQUIREMENTS

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

5 SYSTEM SECURITY CONSIDERATIONS

The interconnection between CAFS, owned by SBA OCA and **VENDOR** is a two-way communication path via web service, secureFTP or any other technology approved by Office of Capital Access. The purpose of the interconnection is for **VENDOR** to retrieve and deliver financial instrument origination and servicing data to CAFS.

Vendors 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."

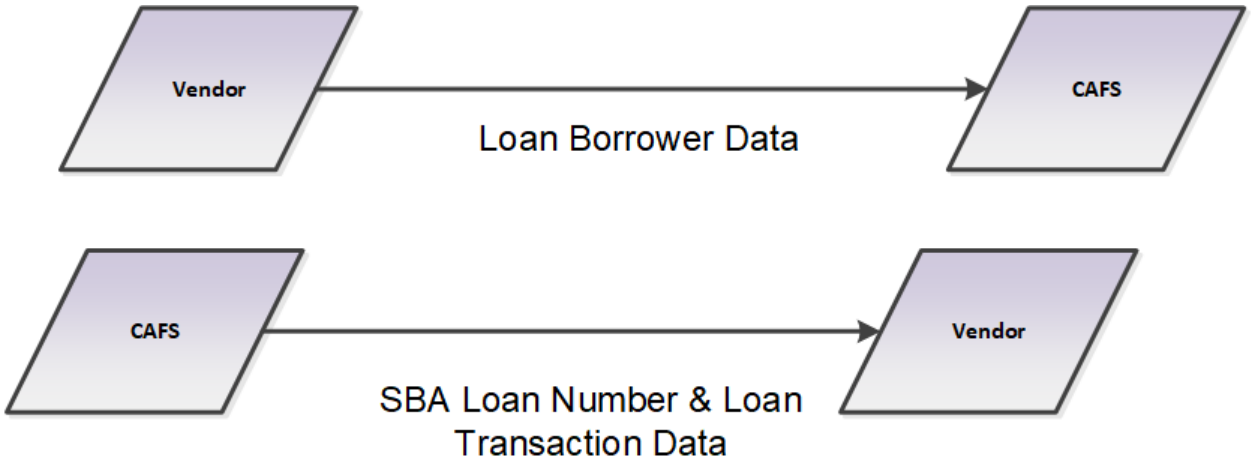
An SOE is a standard operating environment, or a specific computer operating system and collection of software that an IT department defines as a standard build which collects live data.

Assumptions:

- **VENDOR** will access system test at www.catweb2.sba.gov and SOE/production at www.caweb.sba.gov
- **VENDOR** is responsible for annually certifying that they comply with FISMA, Sarbanes Oxley, and NIST
- **VENDOR** is responsible for protecting production data.
- **VENDOR** 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** will only use the system to call OrigScore for an SBA loan.
- **VENDOR** will not use system to system accounts.
- **VENDOR** will not use robotic process automation or bulk processing.
- **VENDOR understands that the data in test is only segregated by VENDOR. Clients will see each other's data.**
- **VENDOR** will receive a vendor location id for test**. VENDOR** must use the lender location id for production.
- **VENDOR** will not share their id with another vendor.

5.1 System Description

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



5.2 Data and Security Controls

CAFS and **VENDOR** exchange data via a web service, SecureFTP or other technology approved by Office of Capital Access. CAFS web services use the "RSA 2048 bits" encryption method. Also, the web services rely on SHA256 with RSA to validate that the data received from a web service is not corrupted. SHA256 with RSA 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 SHA256 with RSA tells us that the web service incorporates a very strong validation that the bi-directional data received was not corrupted.

5.3 Services Offered

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

5.4 Data Sensitivity

VENDOR and CAFS exchange loan borrower data.

For test, the vendor 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

5.5 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.

5.6 Information Exchange Security

The information exchanged between **VENDOR** and CAFS requires the lender using the vendor solution has a valid CLS account.

5.7 Trusted Behavior Expectations / Rules of Behavior (ROB)

The lender, vendor, 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.

5.8 Incident Reporting

Upon discovering an incident involving PII, the vendor and lender/vendor 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

5.9 Security Parameters

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

5.9.1 Hardware Requirements

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

5.9.2 Software Requirements

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

5.10 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 5-1: System Sensitivity Levels

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

5.11 Audit Trails Responsibilities

SBA OCA and **VENDOR** 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.

5.12 Training and Awareness

The information is exchanged via a web service, SecureFTP or other technology approved by CAFS.There is no training required to access the web service.

5.13 Specific Equipment Restrictions

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

5.14 Connectivity

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

5.15 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:

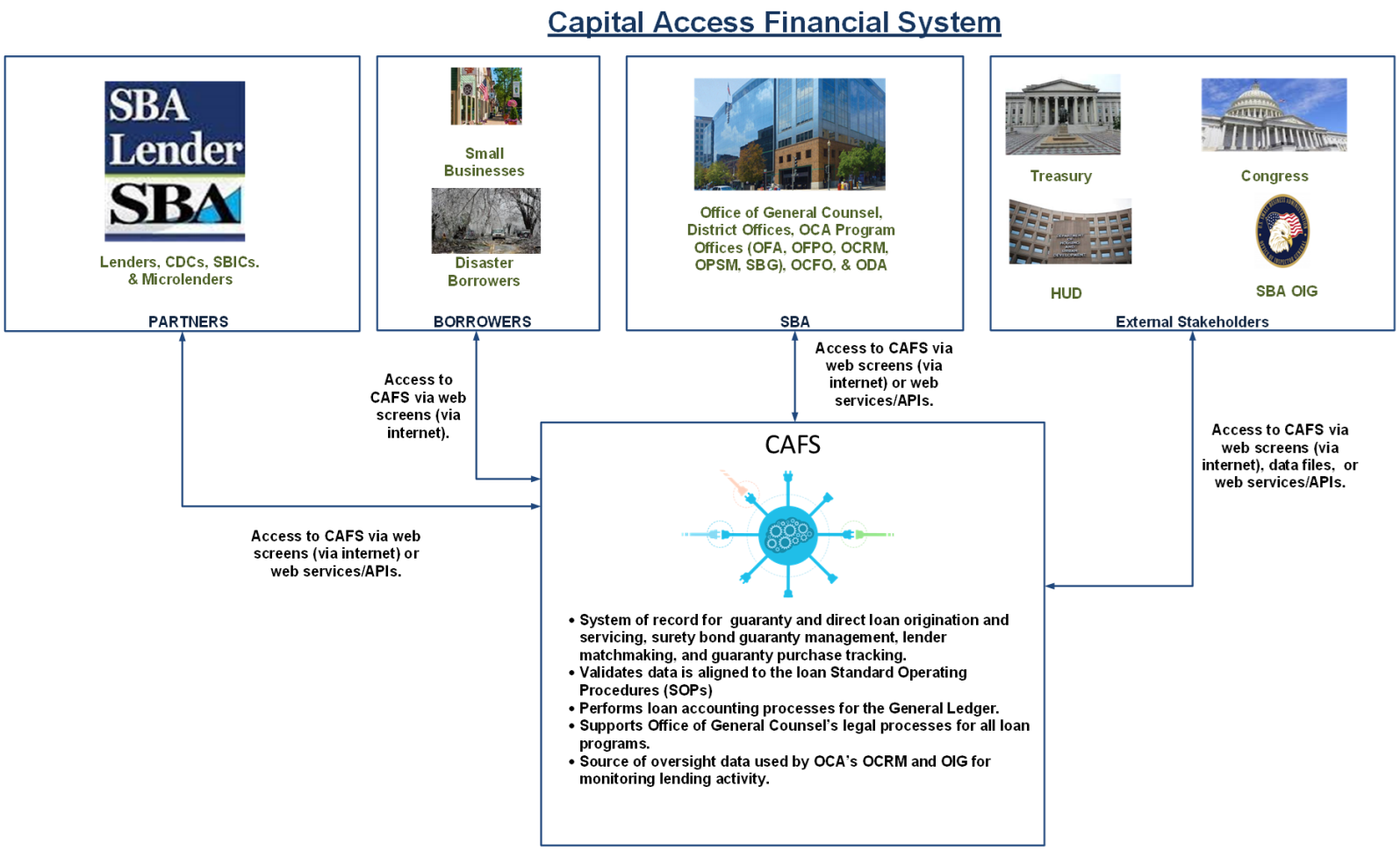
- Federal Information Security Management Act (FISMA) as part of the E-Government Act of 2002
- Office of the Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources
- NIST Special Publications, including NIST SP 800-47, Security Guide for Interconnecting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

5.16 Escalation Procedure

If there are issues with the web service, the lender/vendor authorizing official should follow the escalation procedure(s) to contact Sheri McConville, Ronald Whalen, and Steve Kucharski.

6 NETWORK TOPOLOGY DRAWING

The network topology is in the diagram below.



7 KEY DATES

ISA Completed		
Set up in test		
Testing Completed		
Moved to Production		

8 SIGNATORY AUTHORITY

This ISA is valid for one year 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 at least annually, or whenever a significant change occurs.

OCA Authorizing Official

_____

Steve Kucharski

_____

Director Office of Performance and Systems Management

_____

(Signature) (Date)

VENDOR Authorizing Official

_____

TBD

_____

TBD

_____

(Signature) (Date)