

PRIVACY IMPACT ASSESSMENT

Once the Privacy Impact Assessment is completed and the signature approval page is signed, please submit an electronic copy and hard copy with original signatures of the PIA to the SBA Senior Advisor to the Chief Privacy Officer in the Information Privacy Office of the OCIO.

Name of System/Application: SBA CENTRAL SERVICING AGENT/FISCAL TRANSFER AGENT SECONDARY MARKET SYSTEM (CSA/FTA)

Program Office: Office of Financial Assistance

A. CONTACT INFORMATION

1) Who is the person completing this document?

John Wade, Office of Financial Assistance, (202) 205-3647, john.wade@sba.gov

2) Who is the system owner?

Grady Hedgespeth, Office of Financial Assistance, (202) 205-7562, grady.hedgespeth@sba.gov

3) Who is the system manager for this system or application?

John Wade, Office of Financial Assistance, (202) 205-3647, john.wade@sba.gov

4) Who is the IT Security Manager who reviewed this document?

Ja'Nelle DeVore, Chief Information Security Officer, SBA Office of the CIO, (202) 205-7103, JaNelle.DeVore@sba.gov

5) Who is the Senior Advisor who reviewed this document?

Ethel Matthews, Senior Advisor to the Chief Information Officer, SBA Office of the CIO, 202-205-7173, Ethel.Matthews@sba.gov

6) Who is the Reviewing Official?

Paul Christy, Chief Information Officer, SBA Office of the CIO, 202-205-6708, Paul.Christy@sba.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION

1) Does this system contain any information about individuals? If yes, explain.

Yes. We are required to collect a taxpayer identification number (TIN) by the Internal Revenue Service (IRS) for each investor in loans sold into the secondary market or in pools of secondary market loans. If an individual is an investor, the TIN is the person's social security number.

a. Is the information about individual members of the public?

YES. When the individual becomes an investor in a loan or a pool, then that information collected would be about an individual member of the public.

b. Is the information about employees?

No.

2) What is the purpose of the system/application?

The CSA/FTA system enables a third party contractor to collect and distribute payments, fees and loan status information on SBA pooled investment vehicles.

The CSA/FTA systems:

1. Process and track SBA Program 7(a) loans sold into the secondary market, both pooled and non-pooled. The system analyzes and recomputes loan payments received and computes the payments to be made to investors and the SBA. The system includes various subsystems and applications including FLAGS, PSUOnline, Customer Service Online, eGreenbook, Factor Pages, Loan List, Settlement Express, and 1502 Connection;
2. Track SBA loans issued under the 503/504 programs. The system performs loan payment processing and computes the payments to be made to investors and the SBA. The system maintains a history of the 503/504 program loans and is used to fund the loans via an ACH transaction. In addition, the system handles the settlement and pooling of the individual debentures, processing the incoming payments for the Trustee and disbursing the funds to the proper participants and managing and reporting this data to SBA for the life of the product. The system includes a CDC Online application that provides portfolio information to each CDC, and a 503 ARRA- FMLP application designed to monitor pool formation and payment history associated with the SBA First Mortgage Loan Pool (FMLP) program.

3) Is the system in the development process?

No

4) How will the technology investment (new or updated) affect existing privacy processes?

There will be no impact on existing privacy processes.

5) What legal authority authorizes the purchase or development of this system/application?

- The American Recovery and Reinvestment Act of 2009 (PL 111-5).
- 15 U.S.C. § 634(b) (6), 44 U.S.C. § 3101.
- Privacy Act of 1974, 5 U.S.C. 552a and related statutes (Electronic Communications Privacy Act of 1986; Computer Matching and Privacy Protection Act of 1988).
- Paperwork Reduction Act of 1995; 44 U.S.C. 3501.
- Government Paperwork Elimination Act of 1998.
- Federal Records Act of 1950 and National Archives and Records Administration (NARA) implementing regulating at 36 C.F.R. 1220 and 41 C.S.R. 201-22.
- The Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Systems." OMB Circular A-130 implements a number of Federal laws relating to

information resources ID (for example, the Paperwork Reduction Act, the Clinger-Cohen Act; and the Government Performance and Results Act).

- Additional program definition is detailed in 13 C.F.R., Part 123.

6) Privacy Impact Analysis: What privacy risks were identified and describe how they were mitigated for security and access controls?

The level of privacy risk has been identified as low given the limited amount of privacy information that is collected and maintained on the system. Investors in SBA guaranteed loans or pools of those loans are primarily institutions and not individuals.

RISK: Unauthorized persons outside of CSA/FTA gain access to PII information.

MITIGATION:

- The CSA/FTA System runs in a segregated physical and logical environment.
- Servers and other hardware used to run the system is located in a separate locked cage within secured data centers.
- Networks on which the system runs are separated from other networks by firewalls.
- Transmission of data between the Internet host and the Bank of New York Mellon data centers is encrypted.
- Access to the applications and data is on a “need to know” basis. User access to the network and applications requires a user id and a complex password, which periodically expires in compliance with NIST requirements.

RISK: Unauthorized persons within the CSA/FTA gain access to PII information.

MITIGATION:

- Access to the applications and data is on a “need to know” basis. User access to the network and applications requires a user id and a complex password, which periodically expires in compliance with NIST requirements.

C. SYSTEM DATA

1) What categories of individuals are covered in the system?

Individuals who are investors in loan or pools of loans guaranteed by SBA.

Borrowers

Lenders

Broker/dealers and/or pool assemblers/originators

2) What are the sources of the information in the system?

The sources of information are from the SBA, Lenders, Community Development Companies (CDC), broker/dealers and/or pool assemblers and pool originators.

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

Individuals do not provide information to Colson. The sources of the data regarding individual investors are from broker/dealers and/or pool originators.

b. What Federal agencies are providing data for use in the system?

The SBA is the only Federal Agency providing data for use in the system.

c. What Tribal, State and local agencies are providing data for use in the system?

None.

d. From what other third party sources will data be collected?

None.

e. What information will be collected from the employee and the public?

Investor information including name, address, financial data and EIN or SSN will be collected from the general public by broker/dealers and/or pool originators.

3) Accuracy, Timeliness, and Reliability

a. How is data collected from sources other than SBA records verified for accuracy?

Data is collected by manual submission of documents to Colson. It is compared against existing loan information in the CSA/FTA system obtained from SBA and verified against that data for accuracy. Loan sale information provided by broker/dealers is sent to Colson and compared with 7(a) loan portfolio information captured by SBA and sent to Colson at the beginning of each month. Licensed CDCs will notify a centralized debenture pool aggregator under contract with the SBA of their intention to close a related 504 note and of their need for funds to disburse at closing. All CDCs are required to provide a unique CDC identification number on submitted debenture requests. It will also be checked against the information on the physical loan certificates. The data may also be compared against information in the SBA's databases. Reconciliation of discrepant information pertaining to the same data element is performed prior to loan or debenture sales settlement.

b. How is data checked for completeness?

Data that is submitted either online or through other means is verified using edit checks that are built into the system. Each submission is checked for completeness before an entry will be accepted and processed by the system.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

SBA supplies a current data file of loan numbers and borrower names to the contractor on a monthly basis.

d. Are the data elements described in detail and documented?

No. The data elements of the CSA/FTA system are provided by investors when there is a request for purchase of Guranteed Interest Certificates or Pooled Interest certificates.

4) Privacy Impact Analysis: Discuss what privacy risks were identified and how they were mitigated for the types of information collected?

RISK: Unauthorized persons gain access to PII information.

MITIGATION: Access to the CSA/FTA system and its data is on a “need to know” basis. User access to these systems requires a user id and a complex password, which periodically expires in compliance with NIST requirements. The networks are monitored continuously for possible intrusions/hackers.

D. DATA ATTRIBUTES

1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes. In order to confirm the tax identity of an individual, the Issuers, CDC’s, broker/dealers and/or pool originators are required to report information regarding the investors, some of whom may be individuals.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

No. Non-institutional investor information is collected and maintained by the Issuers, CDC’s, broker/dealers or pool originators. There is no aggregation of data nor is data formally derived by the CSA/FTA system.

3) Will the new data be placed in the individual’s record?

N/A

4) Can the system make determinations about employees or members of the public that would not be possible without the new data?

N/A

5) How is the new data verified for relevance, timeliness and accuracy?

Data is collected by manual submission of documents to Colson. It is compared against existing loan information in the CSA/FTA system obtained from SBA and verified against that data for accuracy. Reconciliation of discrepant information pertaining to the same data element is performed prior to loan or debenture sales settlement.

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

The data is stored on a segregated network and the physical hardware is located within a locked cage in secure data centers. Access to the data is on a “need to know” basis and all access is assigned from a least privilege status. Other controls regarding user access and password protection are in place. There is limited access to batch processes, including those for posting and payout. System operators have the access rights to initiate batch print processes only. The majority of the batch processes is automated and are executed by scheduling programs.

SOP 90-47.2 identifies responsibilities for securing access to the SBA’s IT resources and Agency policy regarding implementation of minimum security controls. The SBA’s Secure Baseline Configuration Standards provide detailed guidance for administrators in configuring access controls. Account access is reviewed using the access control system by the DISO/DSA every 4 months to determine if the account access is still required. If an individual’s account is inactive for 85 days, the account owner will be notified. At 90 days, the account is disabled and removed, at which point, documentation pertaining to the account’s creation and use, is updated to reflect its removal.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? If process is not consolidated please state, “N/A”.

N/A

8) How will the data be retrieved? Does a personal identifier retrieve the data?

Information used for tax reporting to the IRS and for IRS Form 1099 distribution which is sent to individuals is retrieved and prepared electronically and arranged by the taxpayer id. All manual data retrieval is accomplished using non-PII information.

9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

Only reports relating to interest earned can be produced on individuals. These reports are used by the Help Desk to assist investors. Access to individual data for Help Desk assistance is provided to staff subject to access rights controls. Interest earned reports are also sent electronically to the IRS as required by IRS Regulation and IRS Form 1099s are sent to the investors for tax filing purposes.

10) What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required authorized uses), and how individuals can grant consent.

All investors in SBA loans sold into the secondary market and pools of SBA guaranteed loans are required to submit their taxpayer name and taxpayer identification. There are no options as this is required by IRS regulation.

11) Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is used as intended.

The system relies upon the Bank of New York Mellon Wide Area Network (WAN) to display the warning banner. The users must logon to the BNYM segregated network for SBA, where the warning banner is displayed. The system use notification message or banner is displayed after a user logs into a system component of the CSA/FTA system. Role based access controls are in place for individuals to perform specific duties according to their job functions. In the event that these individuals access system functions other than what is intended for their assigned duties, their access controls are limited. Access to the individuals TIN is not paired with any other personally identifiable information. The closed nature of the system design does not allow for transmission of the PII information out on the Internet.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

The production databases are located in a single site. Replication between the production site and the contingency site ensures that the data is consistent between the two sites, with a potential loss of 3 minutes or less.

2) What are the retention periods of data in this system?

It will be retained indefinitely, unless instructed otherwise by the SBA.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

At this time, electronic data is retained indefinitely. Reports containing data are stored in a secured facility and are retained until such time that the SBA calls for their destruction. The procedures are kept in multiple locations, including the Colson Operations area in New York.

4) Is the system using technologies in ways that the SBA has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No

5) How does the use of this technology affect public/employee privacy?

N/A.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

Yes. Role based access controls are in place for individuals to perform specific duties according to their job functions. In the event that these individuals access system functions other than what is intended for their assigned duties, their access controls are limited..

7) What kinds of information are collected as a function of the monitoring of individuals?

Identifiers (e.g., userids) and permissions associated with an access administrator will not be granted access to applications, files, databases, directories, or systems other than the security administration functions for which the user is authorized. The CSA/FTA system automatically audits all account creation, modification, disabling, and termination actions. All individuals

associated with these actions are notified. Time stamps provide evidence that these actions occurred

8) What controls will be used to prevent unauthorized monitoring?

Audit records are maintained and reviewed on a regular basis. Intrusion detection/prevention software is used to prevent unauthorized access, along with strong password requirements and recertification procedures. Access is restricted on a “need to know” basis.

9) Under which Privacy Act systems of records notice (SORN) does the system operate? Provide number and name.

Privacy Act systems of records notice SBA 21 Loan Systems

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision?

N/A

F. DATA ACCESS

a. Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, tribes, other)

All Colson employees with roles and responsibilities associated with the SBA secondary market will have access to the data in the system. The database administrators and the system administrators will have access to the data. Personnel in the Colson Operations groups who have responsibility for servicing the SBA products in their job description will have access to the appropriate data through the application only.

b. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Access is determined by job function. Job function templates have been designed as the criteria and procedures for granting access. Controls and responsibilities are identified in the system rules of behavior.

c. Will users have access to all data on the system or will the user’s access be restricted? Explain.

Access is restricted based upon the person’s job description and a “need to know.”

d. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please processes and training materials)

All Colson employees are required to attest to the Bank of New York Mellon Code of Conduct annually which defines data sensitivity, including data belonging to clients, the policies surrounding the use of data and penalties for not complying with those policies. PII Awareness Training is also given to all employees of the Bank. In addition, Colson employees are required to complete security awareness training from the SBA and from BNYM. User access recertification procedures ensure that employees have the appropriate access for their job

function. Controls and responsibilities are identified in the system rules of behavior that each user is required to complete.

e. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

Yes, Contractors were involved in development, maintenance and delivery of the CSA/FTA production system. Privacy Act clauses have been included in the contract.

f. Do other systems share data or have access to the data in the system? If yes, explain.

Yes. There are subsystem applications operated by the CSA/FTA that provide loan and pool level payment information that is provided to investors for purchase and sale transactions. Additional subsystems utilize payment information to construct transcripts of account and other program management reports for SBA.

g. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

Pursuant to the existing contracts for service, Colson Services Corp. designates an individual who serves as System Security Officer. The responsibilities included in the designation are the protection of privacy rights of the public and employees.

h. How will the shared data be used by the other agency?

Interest earned reports are sent by Colson electronically to the IRS as required by IRS Regulation

i. What procedures are in place for assuring proper use of the shared data?

Safe-guarding procedures are mandated by IRS and are in place to insure shared data is protected. No shared information provided by Colson to the IRS is released to the public.

j. Privacy Impact Analysis: Discuss what privacy risks were identified and how they were mitigated for information shared internal and external.

RISK: Disclosure of PII by Colson employees.

MITIGATION: Each person granted access to system data is required annually to certify their completion of coursework on Computer Security Awareness Training. Colson and Bank of New York Mellon employees are given PII Awareness Training while SBA personnel receive additional training on information privacy through the Freedom of Information Act training that is required each year. Role based access controls are in place for individuals to perform specific duties according to their job functions. In the event that these individuals access system functions other than what is intended for their assigned duties, their access controls are limited.

Privacy Impact Assessment PIA Approval Page

The Following Officials Have Approved this Document:

1) System Owner

_____ (Signature) _____ (Date)

Name: Grady B. Hedgespeth

Title: Director, Office of Financial Assistance

2) Project Manager

_____ (Signature) _____ (Date)

Name: John M. Wade

Title: Financial Analyst – System Owner Representative

3) IT Security Manager

_____ (Signature) _____ (Date)

Name: Ja’Nelle DeVore

Title: Chief Information Security Officer

4) Chief Privacy Officer

_____ (Signature) _____ (Date)


Name:

Title:

Privacy Impact Assessment PIA Approval Page

The Following Officials Have Approved this Document:

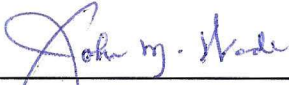
1) System Owner

 (Signature) 3.23.2011 (Date)

Name: Grady B. Hedgespeth

Title: Director, Office of Financial Assistance

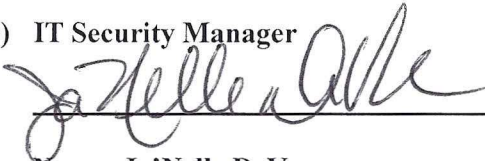
2) Project Manager

 (Signature) 3.23.2011 (Date)

Name: John M. Wade

Title: Financial Analyst – System Owner Representative

3) IT Security Manager

 (Signature) 3-23-11 (Date)

Name: Ja'Nelle DeVore

Title: Chief Information Security Officer

4) Chief Privacy Officer

 (Signature) 3.23.2011 (Date)

Name:

Title: