

PRIVACY IMPACT ASSESSMENT (PIA)

Name of System/Application: Customer Service Center
Telecommunication System (CSCTCS)

Program Office: Office of Disaster Assistance, Buffalo Customer Service
Center

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

A. CONTACT INFORMATION

1) Who is the person completing this document?

Thomas J. Guido
Information Technology Supervisor
SBA Office of Disaster Assistance
Buffalo Customer Service Center
716-843-4101, ext.1313
Thomas.guido@sba.gov

Kristin D. Hughes
Program Analyst
SBA Office of Disaster Assistance
Buffalo Customer Service Center
716-843-4101, ext. 1584
Kristin.hughes@sba.gov

2) Who is the system owner?

James E. Rivera
Associate Administrator for Disaster Assistance
SBA Office of Disaster Assistance
(202) 205-6734
James.Rivera@sba.gov

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

Thomas J. Guido
Information Technology Supervisor
SBA Office of Disaster Assistance
Buffalo Customer Service Center
716-843-4101, ext.1313
Thomas.guido@sba.gov

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

Ronald L. Koop
Information Security Officer
SBA Office of Disaster Assistance
Buffalo Customer Service Center
716-843-4101, ext. 1321
Ronald.koop@sba.gov

5) Who is the Privacy Officer who reviewed this document?

Ethel Matthews
Senior Advisor to the Chief Privacy Officer
Office of the Chief Information Officer
202-205-7173
Ethel.matthews@sba.gov

6) Who is the Reviewing Official?

Robert B. Naylor
Chief Information Officer/Chief Privacy Officer
Office of the Chief Information Officer
202-205-6708
Robert.naylor@sba.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION

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

Yes, the CSCTCS does contain information about individuals. Information regarding the applicant/borrower is gathered to verify Personally Identifiable Information (PII) on all incoming telephone calls prior to release of any information regarding a disaster application/loan. Customer Service Representatives (CSRs) are required to confirm the identity of a caller and assure the requestor is entitled to the information being sought. The PII is then documented within the CSCTCS for Customer Service Center (CSC) production and quality assurance measures.

Information regarding CSC staff is also documented within the CSCTCS, such as name, address, telephone number(s), and Social Security Number (SSN). This documentation is necessary in order capture and monitor staffing levels within the office.

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

Yes

b. Is the information about employees?

Yes

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

The CSCTCS is comprised of two sub networks in the Buffalo CSC. The SBA data subnet encompasses the Microsoft Windows servers, networking devices, and the desktop computing platform. The devices on this network are maintained by SBA OCIO and CSC IT personnel. The Voice Phone subnet comprises the telephone communication and management system maintained by the CSC IT/Telecommunication Specialists. Additional vendor support is provided by Avaya and Avaya Business Partners.

3) Is the system in the development process?

No

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

Existing privacy issues will not be affected by the CSCTCS since all data is housed within the system. Access controls are in place for staff that have administrative and supervisory rights to the system.

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

15 U.S.C. § 634(b)(6), 44 U.S.C. § 3101

Section 7(b)(1) of the Small Business Act, as amended, authorizes the Agency's Physical Disaster Loan Program. SBA can make loans to eligible victims of declared disasters as defined by the Small Business Act.

Section 7(b)(2) of the Small Business Act, as amended, authorizes the Agency's Economic Injury Disaster Loan (EIDL) Program. SBA can make loans to eligible non-farm small businesses and eligible small agricultural cooperatives located in a disaster area that suffered substantial economic injury as a result of the disaster.

Privacy Act of 1974, 5 USC 552a and related statutes (Electronic Communications Privacy Act of 1986; Computer Matching and Privacy Production Act of 1988)

The Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Systems"

OMB Memorandum M-06-15 issued May 15, 2006

OMB Memorandum M-06-16 issued June 22, 2006

The Federal Information Security Management Act of 2002 (FISMA)

Additional program definition is detailed in Title 13 of the Code of Federal Regulations (13 CFR), Part 123

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

PII issues were identified early in the development of the CSCTCS and measures are in place for security and access control. Specifically the use of

names and SSNs to verify applicants/borrowers inquiring about disaster applications/loans and personnel documentation regarding CSC employees.

All data collected is housed within the CSCTCS. Access controls are in place for staff that have administrative and supervisory rights.

C. SYSTEM DATA

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

Information regarding the disaster loan applicant/borrower is gathered to verify PII on all incoming telephone calls prior to release of any information regarding a disaster application/loan. CSRs are required to positively confirm the identity of a caller and assure the requestor is entitled to the information being sought before any specific file/loan information can be released or discussed.

Information regarding CSC staff includes personal information such as address, telephone number(s), and SSN/EIN.

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

Disaster Credit Management System (DCMS)
Federal Emergency Management Agency (FEMA)
National Emergency Management System (NEMIS)
SBA Electronic Loan Application (ELA)
SBA Personnel and Administrative Support (PASC)

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?

The source of the applicant/borrower information is the individual on the telephone in compliance with federal PII. This information is then verified against data in the DCMS or FEMA's NEMIS programs.

If the caller has registered to use the SBA's ELA located on the web at <https://disasterloan.sba.gov/ela/> the CSR will use the CSR ELA Portal (<https://employee.disasterloan.sba.gov/elaemployee>) to verify PII prior to assistance.

Staff information is gathered from the employee and Personnel Departments in the CSC and PASC office located in Herndon, VA.

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

N/A

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

N/A

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

N/A

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

Information to be collected from applicant/borrower:

- Name
- SSN (or Employer Identification Number [EIN] for businesses) or
- Date of Birth
- Address or Telephone number(s)

Information to be collected from the employee:

- Name
- Address
- SSN
- Telephone number(s)
- Employment appointment dates

3) Accuracy, Timeliness, and Reliability

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

The only source outside of SBA of applicant/borrower data utilized to verify PII is FEMA's NEMIS system if the disaster in question is a Presidential declaration. However, there is no outside source if the disaster is an agency declaration. Data collected from CSC staff is provided by the employee.

b. How is data checked for completeness?

The CSC relies on the data stored in the DCMS and NEMIS systems to be up-to-date and accurate. Data documented in CSCTCS is for PII purposes to verify the identity of the caller.

CSC employee data on the CSCTCS is verified against information gathered by the CSC Human Resource Department at time of employment in-processing.

c. Is the data current

Yes, data is current.

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

No, not at this time.

4) Privacy Impact Analysis:

All data collected is housed within the CSCTCS with controls in place that allow staff with administrative rights access.

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 be compliant with federal PII requirements, the CSR's must confirm and document with whom they are speaking with on the telephone or responding to via email. Employee data is retained for federal employment purposes and to effectively manage production workload.

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, the system will not derive new data or create previously unavailable data.

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?

No

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

N/A

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

All data collected is housed within the CSCTCS. Access controls are in place to allow staff with administrative rights to access the data.

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

N/A

- 8) **How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

Yes, a personal identifier will retrieve the data in that it can only be accessed by CSC staff with administrative and/or supervisory rights to the CSCTCS. Rights to the data are given by IT department security officer.

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

CSCTCS Application	Report Name	Use	Access
Call Monitoring QA	Team Compliance Detail Report	Internal for quality assurance monitoring purposes	CSC Director, CSC Deputy Director, CSC supervisors, floor supervisor, QA staff, and IT personnel
Call Monitoring QA	Compliance Summary Report	Internal for quality assurance monitoring purposes	CSC Director, CSC Deputy Director, CSC supervisors, floor supervisor, QA staff, and IT personnel
Call Monitoring QA	Call Rating Trends Report (Monthly)	Internal for quality assurance monitoring purposes	CSC Director, CSC Deputy Director, CSC supervisors, floor supervisor, QA staff, and IT personnel
Call Monitoring QA	Agent Compliance Detail Report	Internal for quality assurance monitoring purposes	CSC Director, CSC Deputy Director, CSC supervisors, floor supervisor, QA staff, and IT personnel

Call Monitoring QA	Agent Monitoring Report	Internal for quality assurance monitoring purposes	CSC Supervisors, floor supervisor, team leads, program assistants, and IT personnel
Call Monitoring QA	Agent Scorecard Report	Internal for quality assurance monitoring purposes	CSC Supervisors, floor supervisor, team leads, program assistants, and IT personnel
Call Monitoring QA	Call Rating Trends	Internal for quality assurance monitoring purposes	CSC Supervisors, floor supervisor, team leads, program assistants, and IT personnel
Call Monitoring QA	Exception Report	Internal for quality assurance monitoring purposes	CSC Supervisors, floor supervisor, team leads, program assistants, and IT personnel
Call Monitoring Team Leader	Team Monitoring Report	Internal for quality assurance, training, and monthly ratings purposes	CSC supervisors, floor supervisor, team leads, program assistants, and IT personnel
Call Monitoring Team Leader	Agent Compliance Report	Internal for quality assurance, training, and monthly ratings purposes	CSC supervisors, floor supervisor, team leads, program assistants, and IT personnel
Call Monitoring Team Leader	Team Compliance Report	Internal for quality assurance, training, and monthly ratings purposes	CSC supervisors, floor supervisor, team leads, program assistants, and IT personnel
Call Monitoring Team Leader	Exception Report	Internal for quality assurance, training, and monthly ratings purposes	CSC supervisors, floor supervisor, team leads, program assistants, and IT personnel
Staffing Report	Staffing Report	Administration of CSC staffing levels and operations	CSC Human Resource personnel and IT personnel

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 or authorized uses), and how individuals can grant consent.

In order to comply with federal PII, all incoming telephone inquiries from applicants/borrowers must provide this in order to receive any information regarding SBA applications/loans. The caller is advised by the CSR that by

refusing to give this information, they will not receive any information regarding the application/loan.

Employees must provide the requested information in order to be employed with the federal government.

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

Before a user is granted access to the CSCTCS, they must complete and sign the Computer Access Clearance/Security Form (SBA Form 1228) and Disaster Assistance System Access Security Request (SBA Form 2161). Employees receive a copy of SBA Procedural Notice 9000-1400 (Computer Security Rules of Behavior). Failure to comply with these policies (SOP 90-47.2) will result in penalties outlined in SOP 37-52.2 (Discipline and Adverse Actions).

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 CSCTCS operates from a single site and utilizes a fireproof safe within a magnetic locked storage room that only authorized IT personnel and Executive Management have access. Safe key is locked in a storage box within the LAN room which is also magnetic lock protected. When daily tapes are not in use, the remaining backup tapes are stored within the safe. The CSC only houses one week's worth of backup storage on-site. Three weeks worth of backup storage is located at an off-site location provided by Iron Mountain, Buffalo, NY location. Only authorized members of the IT staff are designated to interact with Iron Mountain to exchange tape containers.

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

Data from the CSCTCS is maintained for a period of 4-weeks. At such time, the tape media is overwritten with the most current backup. As stated above, CSC rotates tape media on a 4-week schedule.

- 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?**

The CSC is currently not keeping media past the 4-week period and Backup Exec reports are deleted from the server after that 4-week period. There would be no PII contained within the backup logs. These procedures are documented within the IT department handbook.

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

All incoming calls into the CSC display the complete telephone number on the telephone console. Incoming calls to CSR's are recorded using Witness Voice Recording System (eQuality) for future monitoring by the Quality Assurance and Training (QA) department. CSR's are also monitored in real time by CSC team leaders for accuracy and quality purposes.

A recorded announcement at the beginning of incoming calls advises that the telephone conversation may be monitored and or recorded for quality assurance.

- 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, the CSCTCS has a workstation recording software package, eQuality that can record both voice and screen video capture. The voice portion of the application is currently in production and recordings are being held on the network for 60 days for monitoring and quality assurance purposes. All recordings are deleted after this time period.

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

Currently, CSC management, supervisors, team leaders, and members of QA document the PII supplied by the applicant/borrower in the Quality Assurance Monitoring application.

The CSCTCS is currently in the process of the initial Certification and Accreditation (C&A).

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

Only designated management, supervisors, team leaders, members of QA, and designated IT staff have access to the monitoring of telephone calls. Access is granted by the CSC Information Security Officer.

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

SBA Privacy Act System of Record Number 20

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

No system modification is anticipated.

F. DATA ACCESS

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

The system will be accessed by authorized CSC personnel acting in their official capacity and certified contractors under confidentiality agreements while engaged in system development and maintenance. The following is a list of potential users who may have access

- Center Director
- Center Deputy Director
- CSC Human Resource Department staff
- CSC Administration Department staff
- Customer Service Supervisors
- CSC Floor Supervisor
- CSC Team Leaders
- Customer Service Representatives
- CSC Information Technology Department staff
- Headquarter staff of Office of Disaster Assistance
- SBA Office of Chief Information Officer

- 2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**

Access to the data is determined by staff member's official duties and responsibilities. Depending on disaster activity (increase or decrease), any CSC personnel may change job responsibilities; i.e., CSR job duty to team lead responsibilities. When changing responsibilities an updated SBA Form 2161 must be completed and submitted to the IT department.

- 3) Will users have access to all data on the system or will the user's access be restricted? Explain.**

Access to pertinent information on the CCSTCS is strictly controlled by the CSC Information Security Officer on a need-to-know basis. Information access is layered by no access, read only, read/write, and system configuration determined by the status of CSC staff.

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

Upon employment at the CSC, all system users and contractors must complete the required SBA Computer Access Clearance and Security (Form 1228) and System Access Security Request (Form 2161). Access is then granted according to defined job duties and assignments. The system is closely monitored by CSC IT staff to ensure that unauthorized access to applications within the CSCTCS is not breached.

CSC-wide SBA Computer Security Awareness Training (CSAT) and Personally Identifiable Information (PII) yearly training are conducted by IT personnel.

- 5) 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?**

N/A

- 6) **Do other systems share data or have access to the data in the system? If yes, explain.**

No other systems have access to the CSCTCS.

- 7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

The CSC Information Security Officer

- 8) **Will other agencies share data or have access to the data in this system via transferred or transmitted (Federal, State, and Local, Other (e.g., Tribal))?**

Data in the CSCTCS will not be shared with any other agency nor will any agency have access to it.

- 9) **How will the shared data be used by the other agency?**

N/A

- 10) **What procedures are in place for assuring proper use of the shared data?**

N/A

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

Privacy risks have been identified on the CSCTCS' eQuality recording and Auto Dialer Express applications. eQuality is a "listen-only" incoming telephone-recording package used for quality assurance purposes. It is strictly controlled by the CSCTCS' CMS Administrator and the general user cannot edit or remove any portion of the recording.

The Auto Dialer Express application contains preprogrammed telephone numbers and names utilized for outbound dialing campaigns. CSC IT staff with CMS Administrator rights are the only staff with access to this application.

Privacy Impact Assessment PIA Approval Page

The Following Officials Have Approved this Document:

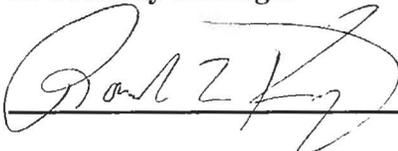
1) Project Manager

 (Signature) 2/17/10 (Date)

Name: Thomas J. Guido

Title: Information Technology Supervisor

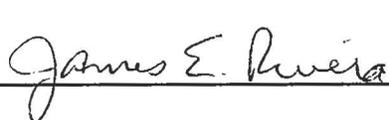
2) IT Security Manager

 (Signature) 2/17/10 (Date)

Name: Ronald L. Koop

Title: Information Security Officer

3) System Owner

 (Signature) 3/22/10 (Date)

Name: James E. Rivera

Title: Associate Administrator for Office of Disaster Assistance

4) Chief Privacy Officer

 (Signature) 4/15/10 (Date)

Name: Robert B. Naylor

Title: Chief Information Officer